Breaking Intrusion Kill Chains with AWS

Reference Material

February 2019

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS's current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS's products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. AWS's responsibilities and liabilities to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Introduction

This reference document contains an example of how AWS services and functionality can be mapped to the intrusion kill chain model. Although this example mapping is comprehensive, it's not exhaustive. There are additional controls that are not included in the example mapping that you should identify and leverage as appropriate.

For information about how to use the mapping included in this document, see the Breaking Intrusion Kill Chains with AWS whitepaper.

Reconnaissance – Pre-Intrusion

This phase represents the work attackers do to research and select their targets, and understand their targets' digital footprints. This can include reconnaissance activities such as port scans and vulnerability scans of the targets' publicly accessible systems and of their supply chain partners.

Reconnaissance pre-intrusion activities occur prior to intrusion attempts. Examples include unusual API activity, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.

Control Objective – Detect

The objective of the *Detect* control in the *Reconnaissance Pre-Intrusion* phase is to "discover or discern the existence, presence, or fact of an intrusion into information systems."[1]

Control Names	Descriptions
Amazon GuardDuty (ID: Sec.Det.1)	This control detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.
Amazon GuardDuty Partners (ID: Sec.Det.2)	These controls are a complement to Amazon GuardDuty.

Control Names	Descriptions
AWS WAF, WAF Managed Rules + Automation (ID: Sec.Inf.2)	Malicious sources scan and probe Internet-facing web applications for vulnerabilities. They send a series of requests that generate HTTP 4xx error codes, and you can use this history to help identify and block malicious source IP addresses.
Amazon CloudWatch, CloudWatch Logs, CloudTrail + Insights, Reporting & Third Parties (ID: Sec.Det.6)	These controls help you to monitor, detect, visualize, receive notifications, and respond to changes in your AWS resources.
AWS Security Hub (ID: Sec.Det.3)	This control gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.
AWS Security Hub Partners (ID: Sec.Det.4)	AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.

Control Objective – Deny

The objective of the *Deny* control in the *Reconnaissance Pre-Intrusion* phase is to "prevent the adversary from accessing and using critical information, systems, and services."[1]

Control Names	Descriptions
Amazon Virtual Private Cloud (Amazon VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes (as a whitelist or blacklist of network reachable assets before Security Groups or NACLs).
AWS Identity and Access Management + AWS Organizations (ID: Sec.IAM.3)	In this context, attackers can't execute `<service>:Describe*` API calls without Allow permissions.
AWS Certificate Manager + Transport Layer Security (ID: Sec.DP.3)	Protecting data in transit denies attackers the ability to capture data in transit during the Reconnaissance phase, unless they are able to impersonate a legitimate endpoint.

Control Names	Descriptions
Network Infrastructure Solutions in the AWS Marketplace (ID: Sec.Inf.11)	Infrastructure solutions in the AWS Marketplace can help deny attackers access to data and infrastructure as they conduct reconnaissance.
AWS WAF, WAF Managed Rules + Automation (ID: Sec.Inf.2)	This control is a solution that leverages automation to quickly and easily configure AWS WAF rules that help block Scanners and Probes, Known Attacker Origins, and Bots and Scrapers solutions.
Amazon Virtual Private Cloud (Amazon VPC) VPN gateway / AWS Direct Connect (ID: Sec.Inf.5)	This control establishes private connectivity to multiple Amazon VPCs.

Control Objective – Disrupt

The objective of the *Disrupt* control in the *Reconnaissance Pre-Intrusion* phase is to "break or interrupt the flow of information." [1]

Control Names	Descriptions
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to block traffic associated with an attack.

Control Objective – Degrade

The objective of the *Degrade* control in the *Reconnaissance Pre-Intrusion* phase is to "reduce the effectiveness or efficiency of adversary command and control (C2) or communications systems, and information collection efforts or means."

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.

Control Objective – Deceive

The objective of the *Deceive* control in the *Reconnaissance Pre-Intrusion* phase is to "cause a person to believe what is not true. MILDEC [military deception] seeks to mislead adversary decision makers by manipulating their perception of reality."[1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.
AWS WAF + AWS Lambda (ID: Sec.IR.2)	These controls trap the endpoint to detect content scrapers and bad bots. When the endpoint is accessed, a function adds the source IP address to a block list.

Control Objective – Contain

The objective of the *Contain* control in the *Reconnaissance Pre-Intrusion* phase is "keeping something harmful under control or within limits." [1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.

Control Objective – Respond

The objective of the Respond control in the *Reconnaissance Pre-Intrusion* phase is to provide "capabilities that help to react quickly to an adversary's or others' IO attack or intrusion." [1]

Control Names	Descriptions
AWS WAF, WAF Managed Rules + Automation (ID: Sec.Inf.2)	Malicious sources scan and probe internet-facing web applications for vulnerabilities. They send a series of requests that generate HTTP 4xx error codes. You can use this history to help identify and block malicious source IP addresses.
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to block traffic associated with an attack.
Amazon GuardDuty Partners (ID: Sec.Det.2)	These controls are a complement to Amazon GuardDuty.
AWS Security Hub Partners (ID: Sec.Det.4)	AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.
Amazon CloudWatch Events & Alarms + Amazon SNS + SIEM Solutions (ID: Sec.Det.7)	These controls monitor, detect, visualize, receive notification about attacks, and respond to changes in your AWS resources.

Reconnaissance – Post-Intrusion

Activities in this phase occur after attacker's intrusion attempts have been successful. Attackers perform reconnaissance inside their victim's environment in an effort to build a map for themselves, which can then be referenced throughout the attack. These activities could include port scanning, ping sweeps, Windows Management Instrumentation (WMI) queries, and SNMP queries.

Control Objective – Detect

The objective of the *Detect* control in the *Reconnaissance Post-Intrusion* phase is to "discover or discern the existence, presence, or fact of an intrusion into information systems." [1]

Control Names	Descriptions
Amazon GuardDuty (ID: Sec.Det.1)	This control detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.
Amazon GuardDuty Partners (ID: Sec.Det.2)	These controls are a complement to Amazon GuardDuty.
Amazon CloudWatch, CloudWatch Logs, CloudTrail + Insights, Reporting & Third-Party Tools (ID: Sec.Det.6)	These controls monitor, detect, visualize, and receive notifications of attacks, and respond to changes in your AWS resources.
AWS Security Hub (ID: Sec.Det.3)	This control gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.
AWS Security Hub Partners (ID: Sec.Det.4)	AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.

Control Objective – Deny

The objective of the *Deny* control in the *Reconnaissance Post-Intrusion* phase is to "prevent the adversary from accessing and using critical information, systems, and services." [1]

Control Names	Descriptions
Amazon Virtual Private Cloud (Amazon VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
AWS Identity and Access Management + AWS Organizations (ID: Sec.IAM.3)	In this context, attackers can't execute `<service>:Describe*` API calls without Allow permissions.
AWS Certificate Manager + Transport Layer Security (ID: Sec.DP.3)	Protecting data in transit denies attackers the ability to capture data in transit during the Reconnaissance phase, unless they are able to impersonate a legitimate endpoint.
Network Infrastructure Solutions in the AWS Marketplace (ID: Sec.Inf.11)	Infrastructure solutions in the AWS Marketplace can help deny attackers access to data and infrastructure as they conduct reconnaissance.
Reverse Proxy Architecture (ID: Sec.Inf.12)	This control protects your servers from unwanted traffic.
AWS Cognito (ID: Sec.IAM.6)	This control provides temporary, limited-privilege AWS credentials to allow access to other AWS services.

Control Objective – Disrupt

The objective of the *Disrupt* control in the *Reconnaissance Post-Intrusion* phase is to "break or interrupt the flow of information." [1]

Control Names	Descriptions
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to block traffic associated with an attack.

Control Objective – Degrade

The objective of the *Degrade* control in the *Reconnaissance Post-Intrusion* phase is to "reduce the effectiveness or efficiency of adversary command and control (C2) or communications systems, and information collection efforts or means." [1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.

Control Objective – Deceive

The objective of the *Deceive* control in the *Reconnaissance Post-Intrusion* phase is to "cause a person to believe what is not true. MILDEC [military deception] seeks to mislead adversary decision makers by manipulating their perception of reality." [1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.
Amazon Virtual Private Cloud + Automation (ID: Sec.Inf.4)	These controls save the current security group of the host or instance, then isolate the host using restrictive ingress and egress security group rules.

Control Objective – Contain

The objective of the *Contain* control in the *Reconnaissance Post-Intrusion* phase is "keeping something harmful under control or within limits." [1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.
Amazon Virtual Private Cloud + Automation (ID: Sec.Inf.4)	These controls help contain compromised systems by using AWS Command Line Interface (CLI) or software development kits using predefined, restrictive security groups.

Control Objective – Respond

The objective of the *Respond* control in the *Reconnaissance Post-Intrusion* phase is to provide "capabilities that help to react quickly to an adversary's or others' IO attack or intrusion." [1]

Control Names	Descriptions
AWS WAF, WAF Managed Rules + Automation (ID: Sec.Inf.2)	Malicious sources scan and probe internet-facing web applications for vulnerabilities. They send a series of requests that generate HTTP 4xx error codes. You can use this history to help identify and block malicious source IP addresses.
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to block traffic associated with an attack.
Amazon GuardDuty Partners (ID: Sec.Det.2)	These controls are a complement to Amazon GuardDuty.
AWS Security Hub Partners (ID: Sec.Det.4)	AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.
Amazon CloudWatch Events & Alarms + Amazon SNS + SIEM Solutions (ID: Sec.Det.7)	These controls help you to monitor, detect, visualize, and receive notifications of attacks, so you can respond to changes in your AWS resources.

Weaponization

There are no products or services included for this phase because *Weaponization* typically occurs in secret, outside of the view of defenders. Subsequently, during this phase of the intrusion kill chain, products and services cannot detect, deny, disrupt, degrade, or complete any other objective.

Delivery

During the *Delivery* phase in the intrusion kill chain, attackers transmit their weapon to the intended victim. Some examples of delivery mechanisms include phishing emails, malicious email attachments, and drive-by download sites.

Control Objective – Detect

The objective of the *Detect* control in the *Delivery* phase is to "discover or discern the existence, presence, or fact of an intrusion into information systems." [1]

Control Names	Descriptions
Amazon GuardDuty (ID: Sec.Det.1)	Detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known bad IP address.
AWS WAF, WAF Managed Rules + Automation (ID: Sec.Inf.2)	Malicious sources scan and probe internet-facing web applications for vulnerabilities. They send a series of requests that generate HTTP 4xx error codes. You can use this history to help identify and block malicious source IP addresses.
AWS Shield (ID: Sec.Inf.14)	This control defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications.
Amazon VPC Flow Logs + Amazon CloudWatch Alarms (ID: Sec.Det.8)	These controls capture and monitor information about the IP traffic going to and from your Amazon VPC.

Control Objective – Deny

The objective of the *Deny* control in the *Delivery* phase is to "prevent the adversary from accessing and using critical information, systems, and services." [1]

Control Names	Descriptions
Amazon Virtual Private Cloud (VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
Amazon Virtual Private Cloud (Amazon VPC) VPN Gateway / AWS Direct Connect (ID: Sec.Inf.5)	These controls establish private connectivity to multiple Amazon VPCs.
Amazon EC2 Security Groups (ID: Sec.Inf.6)	This control is a virtual firewall that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Network Access Control Lists (ID: Sec.Inf.7)	This control is a virtual Access Control List that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
AWS Shield (ID: Sec.Inf.14)	This control defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications.
AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries (ID: Sec.IAM.2)	These controls implement strong, least-privilege and need-to-know security principles for both users and services that access your resources.
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies (ID: Sec.IAM.5)	These controls specify access privileges to objects and prevent the upload of that malicious objects into the bucket.

Control Names	Descriptions
AWS Cognito (ID: Sec.IAM.6)	This control provides temporary, limited-privilege AWS credentials to allow access to other AWS services.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux, FreeBSD – Hardening and Minimization (ID: Sec.Inf.22)	These controls disable or remove unused services and packages.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
Microsoft Windows Security Baselines (ID: Sec.Inf.27)	This control allows you to harden system and user configurations.
AWS Physical & Operational Security Policies & Processes (ID: Platform.5)	AWS data centers are secure by design and our controls make that possible. We spend countless hours considering potential threats and designing, implementing, and testing controls to ensure the systems, technology, and people we deploy counteract risks.

Control Objective – Disrupt

The objective of the *Disrupt* control in the *Delivery* phase is to "break or interrupt the flow of information." [1]

Control Names	Descriptions
Amazon Virtual Private Cloud (Amazon VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
Amazon EC2 Security Groups (ID: Sec.Inf.6)	This control is a virtual firewall that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Network Access Control Lists (ID: Sec.Inf.7)	This control is a virtual Access Control List that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
AWS Shield (ID: Sec.Inf.14)	This control defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	Rebuilt or refresh your environments periodically to make it more difficult for an attack payload to persist.

Control Objective – Degrade

The objective of the *Degrade* control in the *Delivery* phase is to "reduce the effectiveness or efficiency of adversary command and control (C2) or communications systems, and information collection efforts or means." [1]

Control Names	Descriptions
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to degrade or block traffic associated with an attack.
AWS Shield (ID: Sec.Inf.14)	This control defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications.
Load Balancing (ID: Sec.Inf.9)	With this control, before an attacker can consistently communicate with your resources, all the instances included in the load-balanced service need to be compromised by the attack. If one or more instances has not been compromised, the load balancer switches to an unaffected instance, which degrades the attack.
Immutable Infrastructure - Short-Lived Environments (ID: Ops.2)	Rebuilt or refresh your environments periodically to make it more difficult for an attack payload to persist.

Control Objective – Deceive

The objective of the *Deceive* control in the *Delivery* phase is to "cause a person to believe what is not true. MILDEC [military deception] seeks to mislead adversary decision makers by manipulating their perception of reality." [1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.
AWS WAF + AWS Lambda (ID: Sec.IR.2)	These controls trap endpoints to detect content scrapers and bad bots. When the endpoint is accessed a function adds the source IP address to a blocked list.

Control Objective – Contain

The objective of the *Contain* control in the *Delivery* phase is the "action of keeping something harmful under control or within limits." [1]

Control Names	Descriptions
AWS WAF (ID: Sec.Inf.1)	This control protects your network from common web exploits that could affect application availability, compromise security, or consume excessive resources.
Amazon Virtual Private Cloud (A**mazon** VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
Amazon EC2 Security Groups (ID: Sec.Inf.6)	This control is a virtual firewall that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Network Access Control Lists (ID: Sec.Inf.7)	This control is a virtual Access Control List that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.

Control Names	Descriptions
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
Linux cgroups, namespaces, SELinux (ID: Sec.Inf.28)	These controls enforce capability profiles, which prevent running processes from accessing files, network sockets, and other processes.
AWS Container and Abstract Services (ID: Platform.1)	These controls prevent access to underlying infrastructure by customers and threat actors, and segregate your service instances.
AWS Lambda, Amazon Simple Queue Service (SQS), AWS Step Functions (ID: Platform.2)	These services provide orchestration mechanisms for containment.
Hypervisor-Level Guest-to-Guest and Guest-to-Host Segregation (ID: Platform.4)	This control leverages the string isolation capabilities of the AWS hypervisor.

Control Objective – Respond

The objective of the *Respond* control in the *Delivery* phase is to provide "capabilities that help to react quickly to an adversary's or others' IO attack or intrusion." [1]

Control Names	Descriptions
AWS Systems Manager State Manager (ID: Sec.Inf.15)	This control helps you to define and maintain consistent OS configurations.
AWS Partner Offerings – File Integrity Monitoring (ID: Sec.Inf.30)	These controls help you to maintain the integrity of operating system and application files.
AWS WAF + AWS Lambda (ID: Sec.IR.2)	These controls trap endpoints to detect content scrapers and bad bots. When the endpoint is accessed, a function adds the source IP address to a blocked list.

Control Names	Descriptions
Third-Party WAF Integrations (ID: Sec.IR.3)	These controls are a complement to AWS WAF.
AWS Config Rules (ID: Sec.IR.5)	These rules are a configurable set of functions that trigger when an environment configuration change is registered.
Amazon CloudWatch Events + Lambda (ID: Sec.IR.6)	These controls are a configurable set of functions that trigger when an environment configuration change is registered.
AWS Managed Services (ID: Ops.3)	AWS Managed Services monitors the overall health of your infrastructure resources, and handles the daily activities of investigating and resolving alarms or incidents.

Control Objective – Restore

The objective of the *Restore* control in the *Delivery* phase is to "bring information and information systems back to their original state." [1]

Control Names	Descriptions
AWS Systems Manager State Manager (ID: Sec.Inf.15)	This control helps you to define and maintain consistent OS configurations.
CloudFormation + Service Catalog (ID: Ops.1)	These controls help you to provision your infrastructure in an automated and secure manner. The CloudFormation template file serves as the single source of truth for your cloud environment.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	Rebuilt or refresh your environments periodically to make it more difficult for an attack payload to persist.

Exploitation

In the *Exploitation* phase, after the weapon has been delivered to the target, the weapon tries to exploit the weakness it was designed for. This could be the exploitation of a vulnerability or misconfiguration in an operating system, web browser, or other application. An exploit can also be designed to trick people into making poor trust decisions, which is also known as *social engineering*. Another weakness that attackers typically try to exploit is weak, leaked, or stolen passwords.

Control Objective – Detect

The objective of the *Detect* control in the *Exploitation* phase is to "discover or discern the existence, presence, or fact of an intrusion into information systems." [1]

Control Names	Descriptions
Amazon GuardDuty (ID: Sec.Det.1)	This control detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.
AWS WAF, WAF Managed Rules + Automation (ID: Sec.Inf.2)	Malicious sources scan and probe internet-facing web applications for vulnerabilities. They send a series of requests that generate HTTP 4xx error codes. You can use this history to help identify and block malicious source IP addresses.
Amazon Virtual Private Cloud (A**mazon** VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
AWS Systems Manager State Manager, or Third-Party or OSS File Integrity Monitoring Solutions on Amazon EC2 (ID: Sec.Inf.16)	This control automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define.
AWS Config (ID: Sec.Det.5)	With this control, you can assess, audit, and evaluate the configurations of your AWS resources.

Control Names	Descriptions
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Partner Offerings – Anti-Malware Protection (ID: Sec.Inf.33)	These controls detect and block malicious payloads.
AWS Lambda Partners (ID: Sec.Inf.34)	These controls are a complement to the security properties of Lambda functions.
Container Partners – Security (ID: Sec.Inf.35)	These controls are a complement to the security properties of containers solutions.

Control Objective – Deny

The objective of the *Deny* control in the *Exploitation* phase is to "prevent the adversary from accessing and using critical information, systems, and services." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) Roles (ID: Sec.IAM.1)	These controls help deny or contain the blast radius of attacks.
Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies (ID: Sec.IAM.5)	These controls manage access to objects and prevent upload of malicious objects into the Amazon S3 bucket.
AWS Secrets Manager (ID: Sec.IAM.7)	This control protects the secrets needed to access your applications, services, and IT resources.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.

Control Names	Descriptions
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux, FreeBSD – Hardening and Minimization (ID: Sec.Inf.22)	These controls disable or remove unused services and packages.
Amazon EC2 – Linux, Windows, FreeBSD – Address Space Layout Randomization (ASLR) (ID: Sec.Inf.23)	ASLR is a technology that helps prevent shellcode from being successful.
Amazon EC2 – Linux, Windows, FreeBSD – Data Execution Prevention (DEP) (ID: Sec.Inf.24)	DEP is a memory safety feature that makes it more difficult for malware to run.
Amazon EC2 – Windows – User Account Control (UAC) (ID: Sec.Inf.25)	UACs make it more difficult for malware to install and run.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
Microsoft Windows Security Baselines (ID: Sec.Inf.27)	This control hardens system and user configurations.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.

Control Names	Descriptions
AWS Partner Offerings – Anti-Malware Protection (ID: Sec.Inf.33)	This control detects and blocks malicious payloads.
AWS Lambda Partners (ID: Sec.Inf.34)	This control is a complement to the security properties of Lambda functions.
Container Partners – Security (ID: Sec.Inf.35)	This control is a complement to the security properties of containers solutions.
Amazon Simple Email Service (ID: Platform.3)	This control prevents mail from known spammers, or containing malware, from entering the system.

Control Objective – Disrupt

The objective of the *Disrupt* control in the *Exploitation* phase is to "break or interrupt the flow of information." [1]

Control Names	Descriptions
AWS WAF, WAF Managed Rules + Automation (ID: Sec.Inf.2)	Malicious sources scan and probe internet-facing web applications for vulnerabilities. They send a series of requests that generate HTTP 4xx error codes. You can use this history to help identify and block malicious source IP addresses.
Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies (ID: Sec.IAM.5)	These controls manage access to objects and prevent uploads of malicious objects into the bucket.
AWS Secrets Manager (ID: Sec.IAM.7)	This control protects the secrets needed to access your applications, services, and IT resources.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.

Control Names	Descriptions
Amazon EC2 – Linux, Windows, FreeBSD – Address Space Layout Randomization (ASLR) (ID: Sec.Inf.23)	ASLR is a technology that helps prevent shellcode from being successful.
Amazon EC2 – Linux, Windows, FreeBSD – Data Execution Prevention (DEP) (ID: Sec.Inf.24)	DEP is a memory safety feature that makes it more difficult for malware to run.
Amazon EC2 – Windows – User Account Control (UAC) (ID: Sec.Inf.25)	UACs make it more difficult for malware to install and run.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Partner Offerings – Anti-Malware Protection (ID: Sec.Inf.33)	This control detects and blocks malicious payloads.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	This control rebuilds or refreshes environments periodically to make it more difficult for attack payloads to persist.

Control Objective – Degrade

The objective of the *Degrade* control in the *Exploitation* phase is to “reduce the effectiveness or efficiency of adversary command and control (C2) or communications systems, and information collection efforts or means.” [1]

Control Names	Descriptions
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to degrade or block traffic associated with an attack.
AWS WAF (ID: Sec.Inf.1)	This control protects you from common web exploits that could affect application availability, compromise security, or consume excessive resources.
Load Balancing (ID: Sec.Inf.9)	With this control, before an attacker can consistently communicate with your resources, all the instances included in the load-balanced service need to be compromised by the attack. If one or more instances has not been compromised, the load balancer switches to an unaffected instance, which degrades the attack.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

Control Objective – Deceive

The objective of the Deceive control in the Exploitation phase is to "cause a person to believe what is not true. MILDEC [military deception] seeks to mislead adversary decision makers by manipulating their perception of reality."[1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.
AWS WAF + AWS Lambda (ID: Sec.IR.2)	These controls trap endpoints to detect content scrapers and bad bots. When the endpoint is accessed, a function adds the source IP address to a blocked list.

Control Objective – Contain

The objective of the *Contain* control in the *Exploitation* phase is the "action of keeping something harmful under control or within limits." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) Roles (ID: Sec.IAM.1)	These controls help you to deny or contain the blast radius of attacks.
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.

Control Names	Descriptions
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux, FreeBSD – Hardening and Minimization (ID: Sec.Inf.22)	These controls disable or remove unused services and packages.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
Linux cgroups, namespaces, SELinux (ID: Sec.Inf.28)	These controls enforce capability profiles, which prevent running processes from accessing files, network sockets, and other processes.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Container and Abstract Services (ID: Platform.1)	These controls prevent access to underlying infrastructure by customers and threat actors, and segregate your service instances.
Hypervisor-Level Guest-To-Guest and Guest-To-Host Segregation (ID: Platform.4)	This control leverages the string isolation capabilities provided by the AWS hypervisor.

Control Objective – Respond

The objective of the *Respond* control in the *Exploitation* phase is to provide "Capabilities that help to react quickly to an adversary's or others' IO attack or intrusion." [1]

Control Names	Descriptions
Amazon GuardDuty Partners (ID: Sec.Det.2)	These controls are a complement to Amazon GuardDuty.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Partner Offerings – Behavioral Monitoring, Response Tools and Services (ID: Sec.Inf.36)	These controls provide insights into the threats in your environment.
AWS Managed Services (ID: Ops.3)	AWS Managed Services monitors the overall health of your infrastructure resources, and handles the daily activities of investigating and resolving alarms or incidents.

Control Objective – Restore

The objective of the Restore control in the Exploitation phase is to "bring information and information systems back to their original state." [1]

Control Names	Descriptions
AWS Auto Scaling (ID: Sec.Inf.10)	This control adjusts capacity to maintain steady, predictable performance.
AWS Systems Manager State Manager (ID: Sec.Inf.15)	This control helps you to define and maintain consistent OS configurations.
AWS Partner Offerings – File Integrity Monitoring (ID: Sec.Inf.30)	These controls help you to maintain the integrity of operating system and application files.
CloudFormation + Service Catalog (ID: Ops.1)	These controls help you to provision your infrastructure in an automated and secure manner. The CloudFormation template file serves as the single source of truth for your cloud environment.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

Installation

In the *Installation* phase, after vulnerabilities have been successfully exploited, many attackers will attempt to persist undetected in the environment as long as possible, in order to accomplish their objectives. In this phase, attackers will attempt to install tools that allow them to maintain remote access to the victim's environment.

Control Objective – Detect

The objective of the *Detect* control in the *Installation* phase is to "discover or discern the existence, presence, or fact of an intrusion into information systems." [1]

Control Names	Descriptions
Amazon GuardDuty (ID: Sec.Det.1)	This control detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.
Amazon CloudWatch, CloudWatch Logs, CloudTrail + Insights, Reporting & Third-Party Tools (ID: Sec.Det.6)	These controls monitor, detect, visualize, and receive notifications of attacks, and respond to changes in your AWS resources
AWS Security Hub (ID: Sec.Det.3)	This control gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.
AWS Security Hub Partners (ID: Sec.Det.4)	AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.
AWS Systems Manager State Manager, AWS Systems Manager Inventory, AWS Config (ID: Sec.Inf.17)	When new AWS assets are created, or if malware is installed with a regular package, the AWS System Manager Inventory identifies it and sends it to AWS Config for evaluation.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for containers.

Control Names	Descriptions
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Partner Offerings – Anti-Malware Protection (ID: Sec.Inf.33)	These controls detect and block malicious payloads.

Control Objective – Deny

The objective of the *Deny* control in the *Installation* phase is to "prevent the adversary from accessing and using critical information, systems, and services." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries (ID: Sec.IAM.2)	These controls provide strong, least-privilege and need-to-know security principles for both the users and services that can access your resources.
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies (ID: Sec.IAM.5)	These controls manage access to objects and prevent upload of malicious objects into the Amazon S3 bucket.
AWS Cognito (ID: Sec.IAM.6)	This control provides temporary, limited-privilege AWS credentials to allow access to other AWS services.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.

Control Names	Descriptions
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux, FreeBSD – Hardening and Minimization (ID: Sec.Inf.22)	These controls disable or remove unused services and packages.
Amazon EC2 – Windows – User Account Control (UAC) (ID: Sec.Inf.25)	UACs make it more difficult for malware to install and run.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
Amazon EC2 – Windows – Device Guard (ID: Sec.Inf.29)	This control specifies which binaries are authorized to run on your server.
AWS Partner Offerings – Anti-Malware Protection (ID: Sec.Inf.33)	These controls detect and block malicious payloads.

Control Objective – Disrupt

The objective of the *Disrupt* control in the *Installation* phase is to "break or interrupt the flow of information." [1]

Control Names	Descriptions
Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies (ID: Sec.IAM.5)	These controls manage access to objects and prevent upload of malicious objects into the Amazon S3 bucket.
AWS Systems Manager State Manager (ID: Sec.Inf.15)	This control helps you to define and maintain consistent OS configurations.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Windows – User Account Control (UAC) (ID: Sec.Inf.25)	UACs make it more difficult for malware to install and run.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
Amazon EC2 – Windows – Device Guard (ID: Sec.Inf.29)	This control specifies which binaries are authorized to run on your server.
AWS Partner Offerings – File Integrity Monitoring (ID: Sec.Inf.30)	This control helps to maintain the integrity of operating system and application files.

Control Names	Descriptions
AWS Partner Offerings – Anti-Malware Protection (ID: Sec.Inf.33)	These controls detect and block malicious payloads.

Control Objective – Degrade

The objective of the *Degrade* control in the *Installation* phase is to "reduce the effectiveness or efficiency of adversary command and control (C2) or communications systems, and information collection efforts or means." [1]

Control Names	Descriptions
Load Balancing (ID: Sec.Inf.9)	With this control, before an attacker can consistently communicate with your resources, all the instances included in the load-balanced service need to be compromised by the attack. If one or more instances has not been compromised, the load balancer switches to an unaffected instance, which degrades the attack.
AWS Systems Manager State Manager (ID: Sec.Inf.15)	This control helps you to define and maintain consistent OS configurations.
Amazon EC2 – Linux, FreeBSD – Hardening and Minimization (ID: Sec.Inf.22)	These controls disable or remove unused services and packages.
Amazon EC2 – Windows – Device Guard (ID: Sec.Inf.29)	This control specifies which binaries are authorized to run on your server.
AWS Partner Offerings – File Integrity Monitoring (ID: Sec.Inf.30)	This control helps to maintain the integrity of operating system and application files.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

Control Objective – Deceive

The objective of the *Deceive* control in the *Installation* phase is to "cause a person to believe what is not true. MILDEC [military deception] seeks to mislead adversary decision makers by manipulating their perception of reality."[1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys (ID: Sec.Inf.19)	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.

Control Objective– Contain

The objective of the *Contain* control in the *Installation* phase is the "action of keeping something harmful under control or within limits." [1]

Control Names	Descriptions
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.

Control Names	Descriptions
Linux cgroups, namespaces, SELinux (ID: Sec.Inf.28)	These controls enforce capability profiles, which prevent running processes from accessing files, network sockets, and other processes.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Container and Abstract Services (ID: Platform.1)	These controls prevent access to underlying infrastructure by customers and threat actors, and segregate your service instances.
Hypervisor-Level Guest-to-Guest and Guest-to-Host Segregation (ID: Platform.4)	This control leverages the string isolation capabilities of the AWS hypervisor.

Control Objective – Respond

The objective of the *Respond* control in the *Installation* phase is to provide "Capabilities that help to react quickly to an adversary's or others' IO attack or intrusion." [1]

Control Names	Descriptions
AWS Systems Manager State Manager (ID: Sec.Inf.15)	This control helps you to define and maintain consistent OS configurations.
AWS Systems Manager State Manager, or Third-Party or OSS File Integrity Monitoring Solutions on Amazon EC2 (ID: Sec.Inf.16)	This control automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define.

Control Names	Descriptions
AWS Systems Manager State Manager, AWS Systems Manager Inventory, AWS Config (ID: Sec.Inf.17)	When new AWS assets are created, or if malware is installed with a regular package, the AWS System Manager Inventory identifies it and sends it to AWS Config for evaluation.
AWS Partner Offerings – File Integrity Monitoring (ID: Sec.Inf.30)	This control helps to maintain the integrity of operating system and application files.

Control Objective – Restore

The objective of the *Restore* control in the *Installation* phase is to "bring information and information systems back to their original state." [1]

Control Names	Descriptions
AWS Auto Scaling (ID: Sec.Inf.10)	This control adjusts capacity to maintain steady, predictable performance.
AWS Systems Manager State Manager (ID: Sec.Inf.15)	This control helps you to define and maintain consistent OS configurations.
AWS Partner Offerings – File Integrity Monitoring (ID: Sec.Inf.30)	This control helps to maintain the integrity of operating system and application files.
CloudFormation + Service Catalog (ID: Ops.1)	These controls help you to provision your infrastructure in an automated and secure manner. The CloudFormation template file serves as the single source of truth for your cloud environment.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

Command and Control

In the *Command and Control* (C2) phase, attackers maintain illicit access to their victims' environments and can remotely control compromised infrastructure.

Control Objective – Detect

The objective of the *Detect* control in the *C2* phase is to "discover or discern the existence, presence, or fact of an intrusion into information systems." [1]

Control Names	Descriptions
Amazon GuardDuty (ID: Sec.Det.1)	This control detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.
Amazon CloudWatch, CloudWatch Logs, CloudTrail + Insights, Reporting & Third Parties (ID: Sec.Det.6)	These controls help you to monitor, detect, visualize, receive notifications, and respond to changes in your AWS resources.
AWS Security Hub (ID: Sec.Det.3)	This control gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.
AWS Security Hub Partners (ID: Sec.Det.4)	AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.
Outbound Proxy Partners (ID: Sec.Inf.8)	Because it is an intermediary for requests, this control can detect malicious traffic before it reaches your network.
AWS EC2 Forward Proxy Servers (ID: Sec.Inf.13)	Because it is in intermediary for requests, this control can detect malicious traffic before it reaches your network.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.

Control Objective – Deny

The objective of the *Deny* control in the *C2* phase is to "prevent the adversary from accessing and using critical information, systems, and services." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries (ID: Sec.IAM.2)	These controls provide strong, least-privilege and need-to-know security principles for both the users and services that can access your resources.
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
AWS Cognito (ID: Sec.IAM.6)	This control provides temporary, limited-privilege AWS credentials to allow access to other AWS services.
Amazon Virtual Private Cloud (VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
Amazon EC2 Security Groups (ID: Sec.Inf.6)	This control is a virtual firewall that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Network Access Control Lists (ID: Sec.Inf.7)	This control is a virtual Access Control List that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.

Control Objective – Disrupt

The objective of the *Disrupt* control in the *C2* phase is to "break or interrupt the flow of information." [1]

Control Names	Descriptions
Amazon Virtual Private Cloud (VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
Amazon EC2 Security Groups (ID: Sec.Inf.6)	This control is a virtual firewall that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Network Access Control Lists (ID: Sec.Inf.7)	This control is a virtual Access Control List that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to degrade or block traffic associated with an attack.
Amazon GuardDuty + AWS Lambda + AWS WAF, Security Groups, NACLs (ID: Sec.IR.4)	These controls detect attacks and modify security configurations to block traffic associated with an attack.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

Control Objective – Degrade

The objective of the *Degrade* control in the *C2* phase is to "reduce the effectiveness or efficiency of adversary command and control (C2) or communications systems, and information collection efforts or means." [1]

Control Names	Descriptions
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to degrade or block traffic associated with an attack.
Amazon GuardDuty + AWS Lambda + AWS WAF, Security Groups, NACLs (ID: Sec.IR.4)	These controls detect attacks and modify security configurations to block traffic associated with an attack.
–Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

Control Objective – Deceive

The objective of the *Deceive* control in the *C2* phase is to "cause a person to believe what is not true. MILDEC [military deception] seeks to mislead adversary decision makers by manipulating their perception of reality." [1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.

Control Objective – Contain

The objective of the *Contain* control in the *C2* phase is "keeping something harmful under control or within limits." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries (ID: Sec.IAM.2)	These controls provide strong, least-privilege and need-to-know security principles for both the users and services that can access your resources.
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
Amazon Virtual Private Cloud (VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
Amazon EC2 Security Groups (ID: Sec.Inf.6)	This control is a virtual firewall that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Network Access Control Lists (ID: Sec.Inf.7)	This control is a virtual Access Control List that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
AWS Lambda, Amazon Simple Queue Service (SQS), AWS Step Functions (ID: Platform.2)	These services provide orchestration mechanisms for containment.

Control Objective – Respond

The objective of the *Respond* control in the *C2* phase is to provide "Capabilities that help to react quickly to an adversary's or others' IO attack or intrusion." [1]

Control Names	Descriptions
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Partner Offerings – Behavioral Monitoring, Response Tools and Services (ID: Sec.Inf.36)	These controls provide insight into the threats in your environment.
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to block traffic associated with an attack.
AWS Managed Services (ID: Ops.3)	AWS Managed Services monitors the overall health of your infrastructure resources, and handles the daily activities of investigating and resolving alarms or incidents.

Control Objective – Restore

The objective of the *Restore* control in the *C2* phase is to "bring information and information systems back to their original state." [1]

Control Names	Descriptions
AWS Auto Scaling (ID: Sec.Inf.10)	This control adjusts capacity to maintain steady, predictable performance.
AWS Systems Manager State Manager (ID: Sec.Inf.15)	This control helps you to define and maintain consistent OS configurations.
AWS Partner Offerings – File Integrity Monitoring (ID: Sec.Inf.30)	This control helps to maintain the integrity of operating system and application files.
CloudFormation + Service Catalog (ID: Ops.1)	These controls help you to provision your infrastructure in an automated and secure manner. The CloudFormation template file serves as the single source of truth for your cloud environment.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.
AWS DR Solutions (ID: Ops.4)	These controls enable rapid recovery of your IT infrastructure and data.

Actions on Objectives

At in the *Actions* phase of the intrusion, the attackers are now in a position to achieve their objectives. Objectives can include data theft, compromising data integrity, destroying data and infrastructure, disrupting operations, and perpetrating attacks on other victims.

Control Objective – Detect

The objective of the *Detec*t control in the *Actions* phase is to "discover or discern the existence, presence, or fact of an intrusion into information systems." [1]

Control Names	Descriptions
Amazon GuardDuty (ID: Sec.Det.1)	This control detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.
Amazon CloudWatch, CloudWatch Logs, CloudTrail + Insights, Reporting & Third Parties (ID: Sec.Det.6)	These controls help you to monitor, detect, visualize, receive notifications, and respond to changes in your AWS resources.
AWS Security Hub (ID: Sec.Det.3)	This control gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.
AWS Security Hub Partners (ID: Sec.Det.4)	AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.
Outbound Proxy Partners (ID: Sec.Inf.8)	Because it is an intermediary for requests, this control can detect malicious traffic before it reaches your network.
AWS EC2 Forward Proxy Servers (ID: Sec.Inf.13)	Because it is in intermediary for requests, this control can detect malicious traffic before it reaches your network.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.

Control Names	Descriptions
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Partners Offerings – SQL Behavioral Analytics Proxies (ID: Sec.DP.4)	These controls detect unauthorized actions on SQL applications.

Control Objective – Deny

The objective of the *Deny* control in the *Actions* phase is to "prevent the adversary from accessing and using critical information, systems, and services." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries (ID: Sec.IAM.2)	These controls provide strong, least-privilege and need-to-know security principles for both the users and services that can access your resources.
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
AWS Cognito (ID: Sec.IAM.6)	This control provides temporary, limited-privilege AWS credentials to allow access to other AWS services.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.

Control Names	Descriptions
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Key Management Service (KMS) + AWS CloudHSM (ID: Sec.DP.1)	These controls prevent attackers from exfiltrating clear text data that has been encrypted.
AWS KMS Key Policies (ID: Sec.DP.2)	This control implements strong access control policies for encryption keys.

Control Objective – Disrupt

The objective of the *Disrupt* control in the *Actions* phase is to "break or interrupt the flow of information." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries (ID: Sec.IAM.2)	These controls provide strong, least-privilege and need-to-know security principles for both the users and services that can access your resources.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
–Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Config Rules (ID: Sec.IR.5)	These rules are a configurable set of functions that trigger when an environment configuration change is registered.
Immutable Infrastructure – Short-Lived Environments (ID: Ops.2)	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

Control Objective – Degrade

The objective of the *Degrade* control in the *Actions* phase is to "reduce the effectiveness or efficiency of adversary command and control (C2) or communications systems, and information collection efforts or means." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries (ID: Sec.IAM.2)	These controls provide strong, least-privilege and need-to-know security principles for both the users and services that can access your resources.
Load Balancing (ID: Sec.Inf.9)	With this control, before an attacker can consistently communicate with your resources, all the instances included in the load-balanced service need to be compromised by the attack. If one or more instances has not been compromised, the load balancer switches to an unaffected instance, which degrades the attack.
Amazon EC2 – Linux, SELinux – Mandatory Access Control (ID: Sec.Inf.20)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control (ID: Sec.Inf.21)	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) (ID: Sec.Inf.26)	This control implements least-privilege account profiles.
AWS Partners Offerings – SQL Behavioral Analytics Proxies (ID: Sec.DP.4)	These controls detect unauthorized actions on SQL applications

Control Objective – Deceive

The objective of the *Deceive* control in the *Actions* phase is to "cause a person to believe what is not true. MILDEC [military deception] seeks to mislead adversary decision makers by manipulating their perception of reality." [1]

Control Names	Descriptions
Honeypot and Honeynet Environments (ID: Sec.Inf.18)	These controls help to degrade, detect, and contain attacks.

Control Objective – Contain

The objective of the *Contain* control in the *Actions* phase is "keeping something harmful under control or within limits." [1]

Control Names	Descriptions
AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries (ID: Sec.IAM.2)	These controls provide strong, least-privilege and need-to-know security principles for both the users and services that can access your resources.
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts (ID: Sec.IAM.4)	These controls provide strong, least-privilege and need-to-know security principles for both users and services across a multi-account structure. You can control administrators privileges in child accounts.
Amazon Virtual Private Cloud (VPC) (ID: Sec.Inf.3)	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance. Amazon VPC Black Hole Routes operate as a whitelist or blacklist of network reachable assets, before Security Groups or NACLs.
Amazon EC2 Security Groups (ID: Sec.Inf.6)	This control is a virtual firewall that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.
Network Access Control Lists (ID: Sec.Inf.7)	This control is a virtual Access Control List that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.

Control Names	Descriptions
Linux cgroups, namespaces, SELinux (ID: Sec.Inf.28)	These controls enforce capability profiles, which prevent running processes from accessing files, network sockets, and other processes.
AWS Container and Abstract Services (ID: Platform.1)	These controls prevent access to underlying infrastructure by customers and threat actors, and segregate your service instances.
Hypervisor-Level Guest-to-Guest and Guest-to-Host Segregation (ID: Platform.4)	This control leverages the string isolation capabilities of the AWS hypervisor.

Control Objective – Respond

The objective of the *Respond* control in the *Actions* phase is to provide "Capabilities that help to react quickly to an adversary's or others' IO attack or intrusion." [1]

Control Names	Descriptions
Third-Party Security Tools for Containers (ID: Sec.Inf.31)	This control implements advanced security protection and behavioral security solutions for Containers.
Third-Party Security Tools for AWS Lambda Functions (ID: Sec.Inf.32)	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Partner Offerings – Behavioral Monitoring, Response Tools and Services (ID: Sec.Inf.36)	These controls provide insight into the threats in your environment.
Amazon GuardDuty + AWS Lambda (ID: Sec.IR.1)	These controls detect reconnaissance activities and modify security configurations to block traffic associated with an attack.
AWS Managed Services (ID: Ops.3)	AWS Managed Services monitors the overall health of your infrastructure resources, and handles the daily activities of investigating and resolving alarms or incidents.

Control Objective – Restore

The objective of the *Restore* control in the *Actions* phase is to "bring information and information systems back to their original state." [1]

Control Names	Descriptions
AWS Auto Scaling (ID: Sec.Inf.10)	This control adjusts capacity to maintain steady, predictable performance.
AWS Partner Offerings – File Integrity Monitoring (ID: Sec.Inf.30)	This control helps to maintain the integrity of operating system and application files.
CloudFormation + Service Catalog (ID: Ops.1)	These controls help you to provision your infrastructure in an automated and secure manner. The CloudFormation template file serves as the single source of truth for your cloud environment.
AWS DR Solutions (ID: Ops.4)	These controls enable rapid recovery of your IT infrastructure and data.

Control Name Descriptions

This section provides detailed descriptions of the controls used in the Intrusion Kill Chain, in the order they are presented in the phases. Intrusion Kill Chain implementations are likely to follow a category-based implementation.

For a list of these controls, ordered by category, and for recommendations on how to prioritize implementations, see the Prioritizing Control Implementations section.

Amazon GuardDuty

Amazon GuardDuty provides intelligent threat detection by collecting, analyzing, and correlating billions of events from AWS CloudTrail, Amazon VPC Flow Logs, and DNS Logs across all of your associated AWS accounts. Amazon GuardDuty cross-references those events with threat intelligence feeds from AWS's own Threat Intelligence team and third parties.

Amazon GuardDuty detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.
For more information, see https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types.html

Amazon GuardDuty Partners

Amazon GuardDuty APN Partner products are a complement to Amazon GuardDuty.

For more information, see https://aws.amazon.com/guardduty/resources/partners/

AWS WAF, WAF Managed Rules + Automation

AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.

For more information, see:

- https://aws.amazon.com/waf/
- https://docs.aws.amazon.com/solutions/latest/aws-waf-security-automations/capabilities.html

Scanners and Probes

Malicious sources scan and probe Internet-facing web applications for vulnerabilities. They send a series of requests that generate HTTP 4xx error codes, and you can use this history to help identify and block malicious source IP addresses. This solution creates an AWS Lambda function that automatically parses Amazon CloudFront or Application Load Balancer access logs, counts the number of bad requests from unique source IP addresses, and updates AWS WAF to block further scans from those addresses.

Known Attacker Origins (IP Reputation Lists)

A number of organizations maintain *IP address reputation lists*, which are lists of IP addresses operated by known attackers, such as spammers, malware distributors, and botnets. These services leverage the information in these reputation lists to help you block requests from malicious IP addresses.

Bots and Scrapers

Operators of publicly accessible web applications have to trust that the clients accessing their content identify themselves accurately, and that they will use services as intended. However, some automated clients, such as content scrapers or bad bots, misrepresent themselves to bypass restrictions. These services help you identify and block bad bots and scrapers.

AWS WAF Security Automations

The **IP-list parsing (F)** component is the IP Lists Parser AWS Lambda function, which reviews third-party IP address reputation lists hourly to find new IP address ranges to block. These lists include the Spamhaus *Don't Route Or Peer (DROP)* and *Extended Drop (EDROP)* lists, the Proofpoint *Emerging Threats* IP address list, and the Tor exit node list.

The **HTTP Flood Protection (G)** component configures a rate-based rule to protect against attacks that consist of a large number of requests from a particular IP address, such as a web-layer DDoS attack or a brute-force login attempt. The rate-based rule is automatically triggered when web requests from a client exceed a configurable threshold, which defines the maximum number of incoming requests allowed from a single IP address within a five-minute period. Once this threshold is breached, additional requests from the IP address are blocked until the request rate falls below the threshold.

Amazon CloudWatch, CloudWatch Logs, CloudTrail + Insights, Reporting & Third Parties

In addition to CloudWatch, CloudWatch Logs, CloudTrail, and reporting tools such as Elastic Search, and QuickSight, you can integrate with third-party tools such as Splunk, Trend Micro, and Alertlogic.

You can use **Amazon CloudWatch Logs** to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.

For more information, see https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

Amazon CloudWatch Logs Insights enable you to interactively search and analyze your log data in Amazon CloudWatch Logs. You can run queries to help you quickly and effectively respond to operational issues. If an issue occurs, you can use Amazon CloudWatch Logs Insights to identify potential causes and validate deployed fixes.

For more information, see https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AnalyzingLogData.html

When you create your AWS account, CloudTrail is automatically enabled. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view events in the CloudTrail console in the event history. From the event history, you can view, search, and download the past 90 days of activity in your AWS account. You can also create a CloudTrail trail to archive, analyze, and respond to changes in your AWS resources.

For more information, see https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html

AWS Security Hub

AWS Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts. With Security Hub, you now have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions.

For more information, see https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

A Security Hub *insight* is a collection of related findings defined by an aggregation statement and optional filters. An insight identifies a security area that requires attention and intervention. Security Hub offers several managed (default) insights that you cannot modify or delete. You can also create custom insights to track security issues that are unique to your AWS environment and usage.

For more information, see https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-insights.html

AWS Security Hub Partners

AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.

For more information, see https://aws.amazon.com/security-hub/partners/

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

Amazon VPC provides advanced security features, such as security groups and network access control lists, to enable inbound and outbound filtering at the instance level and subnet level. In addition, you can store data in Amazon S3 and restrict access so that it's only accessible from instances in your Amazon VPC. Optionally, you can choose to launch Dedicated Instances, which run on hardware dedicated to a single customer for additional isolation.

In this context, Amazon VPC can help prevent attackers from scanning network resources during reconnaissance.

For more information, see https://aws.amazon.com/vpc/

NAT Gateways

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.

For more information, see https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html

Amazon VPC Black Hole Routes

You can use Amazon VPC black hole routes as a whitelist or blacklist of network reachable assets before Security Groups or NACLs.

The state of a route appears in the route table (active | black hole). When the state is *black hole*, the route's target isn't available. For example, the specified gateway isn't attached to the VPC, or the specified NAT instance has been terminated.

For more information, see https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-route-tables.html

VPC Endpoints

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink, without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and other services does not leave the Amazon network.

For more information, see https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html

AWS PrivateLink

AWS PrivateLink is a purpose-built technology designed for customers to access AWS services in a highly available and scalable manner, while keeping all the network traffic within the AWS network. When you create endpoints for AWS services powered by PrivateLink, these service endpoints appear as Elastic Network Interface (ENI) with private IP addresses in your VPCs. PrivateLink makes it unnecessary to whitelist public IP addresses, or manage Internet connectivity using an Internet Gateway, Network Address Translation (NAT) devices, or firewall proxies to connect to AWS services. AWS services available on PrivateLink also support private connectivity over AWS Direct Connect, so applications in your own data centers can connect to AWS services through the Amazon private network using the service endpoints.

For more information, see https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html - what-is-privatelink

Amazon EC2 Security Groups

A security group is a virtual firewall that controls inbound and outbound traffic to your network resources and Amazon EC2 instance.

For more information, see https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

Network Access Control Lists

Similar to a firewall, Network Access Control Lists (NACLs) control traffic in and out of one or more subnets. To add an additional layer of security to your Amazon VPC, you can set up NACLs with rules similar to your security groups.

For more information, see https://docs.aws.amazon.com/AmazonAmazon VPC/latest/UserGuide/Amazon VPC_ACLs.html

AWS Identity and Access Management + AWS Organizations

AWS Identity and Access Management (AWS IAM) enables you to securely manage access to AWS services and resources. Using AWS IAM, you can create and manage AWS users and groups, and specify permissions to allow and deny their access to AWS resources.

For more information, see https://aws.amazon.com/iam/

AWS Certificate Manager + Transport Layer Security

Protecting data in transit denies attackers the ability to capture data in transit during Reconnaissance, unless they are able to impersonate a legitimate endpoint.

AWS Certificate Manager is a service that enables you to easily provision, manage, and deploy public and private Transport Layer Security (TLS) certificates for use with AWS services and your internal connected resources. TLS certificates are used to secure network communications and establish the identity of websites over the internet and resources on private networks.

For more information, see:

- https://aws.amazon.com/certificate-manager/
- https://aws.amazon.com/blogs/security/introducing-s2n-a-new-open-source-tls-implementation/
- https://aws.amazon.com/blogs/security/easier-certificate-validation-using-dns-with-aws-certificate-manager/
- https://aws.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-using-the-network-load-balancer-with-amazon-ecs/
- https://aws.amazon.com/blogs/aws/new-encryption-of-data-in-transit-for-amazon-efs/

Network Infrastructure Solutions in the AWS Marketplace

The infrastructure solutions in the AWS Marketplace can help deny attackers access to your data and infrastructure as they conduct reconnaissance.

For more information, see https://aws.amazon.com/marketplace/b/2649366011?Ref_=hmpg_categories_2649366011

Amazon Virtual Private Cloud VPN Gateway + AWS Direct Connect

An Amazon Virtual Private Cloud (Amazon VPC) VPN gateway connection creates a link between your data center (or network) and your Amazon VPC . A customer gateway is the anchor on your side of that connection, and can be a physical or software appliance. The anchor on the AWS side of the VPN connection is known as a virtual private gateway.

For more information, see https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html

You can use AWS Direct Connect to establish a private virtual interface from your on-premises network directly to your Amazon VPC. This interface provides you with a private, high-bandwidth network connection between your network and your Amazon VPC. With multiple virtual interfaces, you can establish private connectivity to multiple VPCs, while maintaining network isolation.

For more information, see https://aws.amazon.com/directconnect/

Amazon GuardDuty + AWS Lambda

Amazon GuardDuty gives you intelligent threat detection by collecting, analyzing, and correlating billions of events from AWS CloudTrail, Amazon VPC Flow Logs, and DNS Logs across all of your associated AWS accounts, and then cross-references them with threat intelligence feeds from AWS's Threat Intelligence team and third-party information.

Amazon GuardDuty detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known bad IP address.

For more information, see https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types.html

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. You can use AWS Lambda to run your code in response to events, such as when Amazon GuardDuty finds that a CloudWatch Event was triggered.

For example, the following blog post describes how to use AWS GuardDuty and AWS Web Application Firewall to automatically block suspicious hosts by triggering AWS Lambda responders: https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/

When an attack is detected by Amazon GuardDuty, AWS Lambda responders can be used to modify security configurations to block traffic associated with an attack in progress as well as isolate the potentially compromised environment.

This same approach, AWS GuardDuty > Amazon CloudWatch Events > AWS Lambda responders, can be used to disrupt other flows, as described in these hands-on exercise samples https://github.com/aws-samples/amazon-guardduty-hands-on

Honeypot and Honeynet Environments

Deception technology products present themselves as part of a legitimate infrastructure. When an attacker attempts to compromise the infrastructure, the deception technology helps to degrade, detect, and contain the attack, so your system recovers from attacks faster.

Deception technology products for honeypot or honeynet environments include third-party deception technology solutions, both commercial and open-source. Solutions include Guardicore, Attivo, Illusive, TopSpin, or TrapX. There are also numerous open-source solution honeypot and honeynet projects on GitHub and elsewhere.

For more information, see https://www.guardicore.com/wp-content/uploads/2017/03/Guardicore_SolBrief_Deception_1.pdf

Honeywords and Honeykeys

Planting false credentials makes attackers think they have something of value when they do not. When an attacker attempts to use stolen, false credentials, it helps your system to detect and contain the attacker, so your system recovers faster. The detected use of honeykeys and honeywords is always a true positive for intrusion attempts.

AWS WAF + AWS Lambda

AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.

For more information, see:

- https://aws.amazon.com/waf/
- https://docs.aws.amazon.com/solutions/latest/aws-waf-security-automations/architecture.html

Honeypot (A) for Bad Bots and Scrapers

This component automatically sets up a honeypot, which is a security mechanism intended to lure and deflect an attempted attack. The honeypot is a trap endpoint that you can insert in your website to detect inbound requests from content scrapers and bad bots. If a source gets access to the honeypot, the Access Handler AWS Lambda function intercepts and inspects the request to extract its IP address, and then add it to an AWS WAF block list.

Amazon CloudWatch Events & Alarms + Amazon SNS + SIEM Solutions

You can combine Amazon CloudWatch Events & Alarms with Amazon Simple Notification Service (SNS) and integrate them with security information and event management (SIEM) solutions like Splunk or AlertLogic.

Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams.

You can create a CloudWatch alarm that watches a single CloudWatch metric or the result of a math expression based on CloudWatch metrics. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over

a number of time periods. The action can be a notification sent to an Amazon SNS topic.

You can also add alarms to CloudWatch dashboards and monitor them visually or integrate with other SIEM solutions.

For more information, see:

- https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html
- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html
- https://splunkbase.splunk.com/app/3790/
- https://www.alertlogic.com/solutions/aws-vulnerability-scanning-and-assessment

Network Infrastructure Solutions in AWS Marketplace

The network infrastructure solutions that are available in the AWS Marketplace can help you deny access to the attackers attempting get your data and infiltrate your infrastructure as they conduct reconnaissance.

For more information, see https://aws.amazon.com/marketplace/b/2649366011?ref_=hmpg_categories_2649366011

AWS Cognito

Amazon Cognito provides solutions to control access to backend resources from your application. You can define roles and assign users to different roles so your application can access only the resources that are authorized for each user.

Amazon Cognito Identity Pools (Federated Identities)

Amazon Cognito identity pools (federated identities) enable you to create unique identities for your users and federate them with identity providers. With an identity pool, you can obtain temporary, limited-privilege AWS credentials to access other AWS services.

For more information, see https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-identity.html

Reverse Proxy Architecture

Reverse proxies are a powerful software architecture primitive for fetching resources from a server on behalf of a client. They serve a number of purposes, from protecting servers from unwanted traffic to offloading some of the heavy lifting of HTTP traffic processing.

For more information, see https://aws.amazon.com/blogs/compute/nginx-reverse-proxy-sidecar-container-on-amazon-ecs/

Amazon Virtual Private Cloud + Automation

With Amazon Virtual Private Cloud (Amazon VPC) Subnet Isolation, you can contain compromised systems by using AWS Command Line Interface (AWS CLI), or software development kits using predefined, restrictive security groups. You can save the current security group of the host or instance, and then isolate the host using restrictive ingress and egress security group rules.

For more information, see https://aws.amazon.com/blogs/publicsector/building-a-cloud-specific-incident-response-plan/

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic, inline mitigations that minimize application downtime and latency, so you don't have to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield: Standard and Advanced.

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

For more information, see https://aws.amazon.com/shield/

Amazon VPC Flow Logs + Amazon CloudWatch Alarms

Amazon VPC Flow Logs enables you to capture information about the IP traffic going to and from network interfaces in your Amazon VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs and Amazon S3, or another analytics tool. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.

For more information, see https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html

AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policies Boundaries

AWS Identity and Access Management (AWS IAM) enables you to manage access to AWS services and resources securely. Using AWS IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

For more information, see https://aws.amazon.com/iam/

You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions.

For more information, see https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

A permissions boundary is a managed policy in which you set the maximum permissions that an identity-based policy can grant to an IAM entity. When you set a permissions boundary for an entity, the entity can perform only the actions that are allowed by both its identity-based policies and its permissions boundaries.

For more information, see https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

AWS Identity and Access Management (AWS IAM) Roles

AWS Identity and Access Management (AWS IAM) Roles help deny or contain the blast radius of attacks. For example, you can use an IAM role to grant permissions to applications running on Amazon EC2 instances.

For more information, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

AWS Organizations + Service Control Policies (SCPs) + AWS Accounts

With AWS Organizations, you can create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts. SCPs put bounds around the permissions that AWS Identity and Access Management (AWS IAM) policies can grant to entities in an account, such as IAM users and roles. For example, IAM policies for an account in your organization cannot grant access to AWS Direct Connect if access is not also allowed by the SCP for the account. Entities can only use the services allowed by both the SCP and the IAM policy for the account.

For more information, see https://aws.amazon.com/organizations/

Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs enable you to restrict, at the account level of granularity, what services and actions are available to the users, groups, and roles in those accounts.

For more information, see https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies

A bucket policy is a resource-based AWS Identity and Access Management (AWS IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it.

With an Amazon S3 bucket policy, malicious objects that contain attacker payload can be prevented from directly being uploaded into the bucket. All objects must be uploaded through the application and subject to malware checks before they can be stored in an Amazon S3 bucket.

For more information, see https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-overview.html#access-control-resources-manage-permissions-basics

Amazon EC2 – Linux, SELinux – Mandatory Access Control

Mandatory Access Control can be configured as a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls for users (including root) and processes.

Amazon EC2 – FreeBSD, Trusted BSD – Mandatory Access Control

Mandatory Access Control for FreeBSD and Trusted BSD can be configured as a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls for users (including root) and processes.

Amazon EC2 – Linux, FreeBSD – Hardening and Minimization

Hardening and minimization make it difficult to exploit a vulnerability in a service by reducing the services that are running and removing or uninstalling unnecessary services.

Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC)

RBAC and DAC provide least-privilege account profiles mediated by root that control which users can get access to your resources.

Amazon EC2 – Windows – Device Guard

With Windows Device Guard for your Amazon EC2 instance, you can specify which binaries are authorized to run on your server, including user mode and kernel mode binaries, which enhances AppLocker functionality.

Microsoft Windows Security Baselines

A security baseline is a group of Microsoft-recommended configuration settings. You can use security baselines to:

- Set configuration settings. For example, you can use Group Policy to configure a device with the setting values specified in the baseline.
- Make sure that user and device configuration settings are compliant with the baseline.

For more information, see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines

AWS Physical & Operational Security Policies & Processes

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is AWS's number one priority, and while you can't visit our data centers or offices to see this protection firsthand, we provide several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations.

For more information about AWS compliance, see aws.amazon.com/compliance.

For more information about AWS security, see https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

For more information about AWS datacenters, see https://aws.amazon.com/compliance/data-center/controls/

Immutable Infrastructure – Short-Lived Environments

In the case of Amazon EC2, Containers, and especially AWS Lambda, short environment lifetimes (when compared to traditional datacenters) mean that an environment being targeted at time `t="now"` may not be the same as an environment being targeted in time `t="now+5 minutes"`. When environments are being rebuilt or refreshed every few minutes, it is a much more difficult task to make an attack payload persist.

When your production environment does not have privileges configured, including for the network infrastructure, there is nothing for attackers to modify and your environment is more resilient to attacks.

Load Balancing

With load balancing, before an attacker can consistently get access to your resources, all the instances included in the load-balanced service need to be compromised by the attack. If one or more instances has not been compromised, the load balancer switches to an unaffected instance, which degrades the attack.

For more information, see https://aws.amazon.com/elasticloadbalancing/

AWS Lambda, Amazon Simple Queue Service (SQS), AWS Step Functions

These services are orchestration mechanisms for containment.

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume—there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service, all with zero administration. Just upload your code and AWS Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

For more information, see https://aws.amazon.com/lambda/

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware, and empowers developers to focus on differentiating work. Using Amazon SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with Amazon SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

For more information, see https://aws.amazon.com/sqs/

AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. Using AWS Step Functions, you can design and run workflows that stitch together services such as AWS Lambda and Amazon ECS into feature-rich applications. Workflows are made up of a series of steps: the output of one step is the input for the next step.

For more information, see https://aws.amazon.com/step-functions/

AWS WAF

AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

For more information, see https://aws.amazon.com/waf/

AWS Container and Abstract Services

AWS Container and Abstract services prevent access to underlying infrastructure by both customers and threat actors, and segregate service instances while enabling customers to apply selective permissions to allow third parties to access them. This limits the scope and effect of any attack a threat actor could perpetrate using these services.

Linux cgroups, namespaces, SELinux

SELinux and the technologies that support it (including cgroups and namespaces) can enforce capability profiles that prevent running processes from accessing files, network sockets, and other processes, using Mandatory Access Control. This means that, even if a running process is compromised, it can be prevented from accessing other resources on the OS instance, or even doing things expected of regular Unix processes (such as forking copies of itself or reading world-read files).

Hypervisor-Level Guest-to-Guest and Guest-to-Host Segregation

The hypervisor for Amazon EC2 instances and other services is in-scope for PCI-DSS certification for separating different operating system instances from each other, and guest operating systems from itself. Hypervisor separation, and the additional technologies incorporated as modules into it (such as Security Groups), provide mechanisms to mitigate some risks of one compromised Amazon EC2 instance being used as a platform to compromise other instances.

AWS Systems Manager State Manager

AWS Systems Manager State Manager helps you define and maintain consistent OS configurations such as firewall settings and anti-malware definitions to comply with your policies. You can monitor the configuration of a large set of instances, specify a configuration policy for the instances, and automatically apply updates or configuration changes.

For more information, see https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-state.html

AWS Partner Offerings – File Integrity Monitoring

File integrity monitoring (FIM) and enforcement are controls that help maintain the integrity of operating system files and application files by verifying the current file state and a known good baseline of these files. Check features of products carefully for enforcement or reversion capabilities. For example, Trend Micro Deep Security, Tripwire are two partner offerings for FIM.

For more information, see https://aws.amazon.com/partners/

Third-Party WAF Integrations

Some examples of third-party tools that integrate with AWS WAF include Trend Micro, Imperva, and Alert Logic.

For more information about third-party integrations with AWS WAF, see https://aws.amazon.com/waf/partners/

AWS Config

AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With AWS Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

For more information, see:

- https://aws.amazon.com/blogs/aws/track-aws-with-config/
- https://aws.amazon.com/config/

AWS Config Rules

AWS Config Rules are a configurable and extensible set of Lambda functions (for which source code is available) that trigger when an environment configuration change is registered by the AWS Config service. If AWS Config Rules deem a configuration change to be undesirable, they can act to remediate it. In common with all other Lambda functions, AWS Config Rules can be assigned IAM Roles with permissions that enable them to make appropriate remedial API calls.

For more information, see https://aws.amazon.com/config/

Amazon CloudWatch Events + Lambda

Amazon CloudWatch Events occur when various states are detected (such as GuardDuty findings), and can be used to trigger Lambda functions in the same manner as AWS Config Rules. If the Lambda functions deem an event to be undesirable, they can act to remediate it, using IAM Roles with the correct permissions to allow them to make appropriate remedial API calls.

AWS Managed Services

AWS Managed Services monitors the overall health of your infrastructure resources, and handles the daily activities of investigating and resolving alarms or incidents. AWS Managed Services protects your information assets and helps keep your AWS infrastructure secure. With anti-malware protection, intrusion detection, and intrusion prevention systems, AWS Managed Services manages security policies per stack, and is able to quickly recognize and respond to any intrusion.

For more information, see https://aws.amazon.com/managed-services/

CloudFormation + Service Catalog

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation enables you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. This file serves as the single source of truth for your cloud environment.

AWS CloudFormation is available at no additional charge, and you pay only for the AWS resources needed to run your applications.

For more information, see https://aws.amazon.com/cloudformation/

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows you to centrally manage commonly deployed IT services, and helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

For more information, see https://aws.amazon.com/servicecatalog/

AWS Systems Manager State Manager, or Third-Party or OSS File Integrity Monitoring Solutions on Amazon EC2

AWS Systems Manager State Manager is a secure and scalable configuration management service that automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define.

For more information, see https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-state.html

For information about AWS Marketplace solutions, see https://aws.amazon.com/marketplace/search/results?x=0&y=0&searchTerms=file+integrity+monitoring&page=1&ref_=nav_search_box

Third-Party Security Tools for Containers

Some of the third-party security tools available for containers include Twistlock, Neuvector, Aqua, Alcide, and Trend Micro Deep Security Smart Check.

For example, the Alcide Cloud Native Security Platform provides a single view into, and unified security controls for distributed environments and cloud-native environments. It works across all workloads and infrastructures (on-premises, single cloud, or multi-cloud) and provides application-aware policy management and enforcement through intelligent and automated network, application and third-party services controls.

For more information, see https://aws.amazon.com/marketplace/pp/B07F21D2ZV?qid=1537887192136&sr=0-1&ref_=srh_res_product_title

Third-Party Security Tools for AWS Lambda Functions

Two of the third-party security tools available for Lambda functions are PureSec and Protego.

For more information, see:

- https://www.puresec.io/
- https://www.protego.io/

AWS Partner Offerings – Behavioral Monitoring, Response Tools and Services

AWS Partner offerings, such as Alert Logic and TrendMicro, provide insight into the real threats in your environments.

For more information, see:

- https://aws.amazon.com/marketplace/seller-profile?id=20e24245-5d10-4191-92f1-c7725d18a375
- https://aws.amazon.com/marketplace/seller-profile?id=934af31d-efde-4b34-bc44-2d477620a0c8

AWS Partner Offerings – Anti-Malware Protection

AWS Technology Partner anti-malware protection offerings detect and block malicious payloads.

AWS Lambda Partners

AWS Lambda Partners provide services and tools that help customers build or migrate their solutions to a microservices based serverless architecture, without having to worry about provisioning or managing servers.

AWS Lambda Partners for the *Security* technology include Protego, Puresec, and Twistlock.

For more information, see https://aws.amazon.com/lambda/partners/

AWS Container Partners – Security

AWS Container Competency Partners have a technology product or solution on AWS that offers support to run workloads on containers. The product or solution integrates with AWS services in a way that improves the AWS customer's ability to run workloads using containers on AWS.

AWS Containers Partners for Security include Alert Logic, Aporeto, Aqua, Sysdig, Tigera, Trend Micro, and Twistlock.

For more information, see https://aws.amazon.com/what-are-containers/partners/

AWS Secrets Manager

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

For more information, see https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

Amazon EC2 – Linux, Windows, FreeBSD – Address Space Layout Randomization (ASLR)

ASLR is a technology that prevents shellcode from being successful. It does this by randomly offsetting the location of modules and certain in-memory structures. While this can be helpful, there are limits to how effective it is. Processors, and operating systems need to provide ASLR support, and on some operating systems, applications must opt in.

Amazon EC2 – Linux, Windows, FreeBSD – Data Execution Prevention (DEP)

DEP is a memory safety feature that makes it more difficult for malware to run. It prevents certain memory blocks, such as the stack, from being executed.

For more information about DEP, see https://en.wikipedia.org/wiki/Executable_space_protection

Amazon EC2 – Windows – User Account Control (UAC)

UACs, also known as least-privilege user account, make it more difficult for malware to install and run.

For more information about UACs, see https://msdn.microsoft.com/en-us/library/windows/desktop/dn742497(v=vs.85).aspx

Amazon Simple Email Service

Spam and Viruses – Amazon Simple Email Service (Amazon SES) uses a number of spam and virus protection measures. It uses block lists to prevent mail from known spammers from entering the system. It also performs virus scans on every incoming email message that contains an attachment. Amazon SES makes its spam detection verdicts available to you, so you can decide if you trust each message. In addition to the spam and virus verdicts, Amazon SES provides the DKIM and SPF check results.

Amazon SES uses in-house content filtering technologies to scan email content for spam and malware. In exceptional cases, accounts identified as sending spam or other low-quality email might be suspended, or AWS SES may take such other action as it deems appropriate. When malware is detected, Amazon SES prevents these emails from being sent.

For more information, see https://aws.amazon.com/ses/faqs/

AWS Auto Scaling

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.

If a *Respond* control automatically kills an instance of an operating environment (such as an Amazon EC2 instance, container, or Lambda function), AWS Auto Scaling creates new instances from reference images to replace it in line with load requirements.

For more information, see https://aws.amazon.com/autoscaling/

AWS Systems Manager State Manager, AWS Systems Manager Inventory, AWS Config

AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against your specified configurations.

When attackers create new AWS assets, or if malware is installed with a regular package, the AWS System Manager Inventory identifies it and sends it to AWS Config for evaluation.

For more information, see https://aws.amazon.com/config/

AWS EC2 Forward Proxy Servers

A forward proxy server is an intermediary for requests from internal users and servers, often caching content to speed up subsequent requests. Companies usually implement proxy solutions to provide URL and web content filtering, IDS/IPS, data loss prevention, monitoring, and advanced threat protection.

For more information about AWS EC2 Forward Proxy Servers, see https://aws.amazon.com/answers/networking/controlling-vpc-egress-traffic/

Outbound Proxy Partners

Outbound proxy partner products such as Sophos UTM provide multiple security functions, including firewall, intrusion prevention, VPN, and web filtering. Sophos Outbound Gateway provides a distributed, fault-tolerant architecture to provide visibility, policy enforcement, and elastic scalability to outbound web traffic.

For more information, see https://aws.amazon.com/quickstart/architecture/sophos-outbound-web-proxy/

Amazon GuardDuty + AWS Lambda + AWS WAF, Security Groups, NACLs

Amazon GuardDuty gives you intelligent threat detection by collecting, analyzing, and correlating billions of events from AWS CloudTrail, Amazon VPC Flow Logs, and DNS Logs across all of your associated AWS accounts. It then cross-references them with threat intelligence feeds from AWS's Threat Intelligence team and third-party feeds.

When an attack is detected by Amazon GuardDuty, AWS Lambda responders can be used to modify security configurations to block traffic associated with an attack in progress as well as isolate the potentially-compromised environment.

For more information, see https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types.html

AWS DR Solutions

The AWS cloud supports many popular disaster recovery (DR) architectures, from *pilot light* environments that might be suitable for small customer workload data center failures, to *hot standby* environments that enable rapid failover at scale. With data centers in regions all around the world, AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of your IT infrastructure and data.

For more information about available disaster recover technology, see https://aws.amazon.com/disaster-recovery/

AWS Partners Offerings – SQL Behavioral Analytics Proxies

Third-party behavioral analytics proxies for SQL, such as SecuPi, can detect unauthorized actions on SQL applications and act to constrain access when there is unexpected behavior.

For more information, see https://www.secupi.com

AWS Key Management Service (KMS) + AWS CloudHSM

AWS Key Management Service and AWS CloudHSM can prevent attackers from exfiltrating clear text data that has been encrypted, as well as crypto key material used to encrypt data.

AWS Key Management Service makes it easy to manage encryption keys used to encrypt data stored by your applications regardless of where you store it.

For more information, see https://aws.amazon.com/kms/

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

For more information, see https://aws.amazon.com/cloudhsm/

AWS KMS Key Policies

The primary method to manage access to your AWS KMS CMKs is with policies. Policies are documents that describe who has access to what. Policies attached to an AWS IAM identity are identity-based policies (or IAM polices), and policies attached to

other kinds of resources are resource-based policies. In AWS KMS, you must attach resource-based policies to your customer master keys (CMKs). These are key policies. All KMS CMKs have a key policy.

For more information, see:

- https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html
- https://docs.aws.amazon.com/kms/latest/developerguide/control-access-overview.html#managing-access

Prioritizing Control Implementations

Each unique control included in *Breaking Intrusion Kill Chains with AWS Reference Material* has a unique control number assigned to it. The same control number appears in each place in the intrusion kill chain framework that the associated control is used. For example, each appearance of the *Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies* control in the intrusion kill chain framework includes the *Sec.IAM.5* control number.

The control numbers are based on the AWS Cloud Adoption Framework (AWS CAF). The guidance and best practices provided by the AWS CAF help you build a comprehensive approach to cloud computing across your organization, and throughout your IT lifecycle. Using the AWS CAF helps you realize measurable business benefits from cloud adoption faster and with less risk.

The AWS CAF organizes guidance into six areas of focus, known as perspectives. Each perspective covers distinct responsibilities owned or managed by functionally related stakeholders. In general, the Business, People, and Governance Perspectives focus on business capabilities, while the Platform, Security, and Operations Perspectives focus on technical capabilities.

For a full explanation of the AWS CAF, see https://aws.amazon.com/professional-services/CAF/

Most of the controls in *Breaking Intrusion Kill Chains with AWS* are from the AWS CAF Security perspective. To help you with your implementation, you can use the AWS CAF Security Epics. The Security Epics consist of groups of user stories (use cases and abuse cases) that you can work on during sprints. Each of these epics has multiple iterations that address increasingly complex requirements and layering in robustness. Although we advise the use of Agile methodologies, the epics can also be treated as general work streams or topics that help in prioritizing and structuring delivery using any

other framework. Some CAF perspectives, such as the Operations and Platform perspectives, do not have epics.

Control Number Format

The format of the control numbers is:

CAF perspective.CAF perspective epic.sequential_number

The *CAF perspective epic* only applies to AWS CAF perspectives that have epics, such as the Security perspective.

Some examples of control numbers:

- Sec.IAM.1 – CAF Security Perspective, Identity & Access Management Epic, control 1
- Sec.Det.1 – CAF Security Perspective, Detective Security Epic, control 1
- Sec.DP.3 – CAF Security Perspective, Data Protection Epic, control 3
- Sec.Inf.11 – CAF Security Perspective, Infrastructure Security Epic, control 11
- Sec.IR.5 – CAF Security Perspective, Incident Response Epic, control 5
- Platform.1 – CAF Platform Perspective, control 1
- Ops.2 – CAF Operations Perspective, control 2

Prioritize Controls with the Control Number and AWS CAF

Organizations that use AWS CAF to build a comprehensive approach to cloud computing across their organization and have also decided to implement some or all of the controls described in *Breaking Intrusion Kill Chains with AWS*, can use the following table to cross-reference their efforts. This table makes it easy to identify which intrusion kill chain controls can be implemented as organizations perform sprints associated with AWS CAF perspectives and epics.

For example, when an organization plans to work on the *Detective Controls Epic*, the table shows them that when they implement the controls listed under that epic, they will also be enabling other capabilities as part of their intrusion kill chain strategy.

This approach can help organizations prioritize which intrusion kill chain controls to implement as part of a broader AWS CAF strategy.

Table 1 – Controls Mapped to Amazon Cloud Adoption Framework (Amazon CAF)

Control ID	Control Name
Security Perspective – Identity and Access Management (AWS IAM) Epic	
Sec.IAM.1	AWS Identity and Access Management (AWS IAM) Roles
Sec.IAM.2	AWS Identity and Access Management (AWS IAM) + AWS IAM Policies and Policy Boundaries
Sec.IAM.3	AWS Identity and Access Management (AWS IAM) + AWS Organizations
Sec.IAM.4	AWS Organizations + Service Control Policies (SCPs) + AWS Accounts
Sec.IAM.5	Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies
Sec.IAM.6	Amazon Cognito
Sec IAM.7	AWS Secrets Manager
Security Perspective – Detective Controls Epic	
Sec.Det.1	Amazon GuardDuty
Sec.Det.2	Amazon GuardDuty Partners
Sec.Det.3	AWS Security Hub
Sec.Det.4	AWS Security Hub Partners
Sec.Det.5	AWS Config

Control ID	Control Name
Sec.Det.6	Amazon CloudWatch, CloudWatch Logs, CloudTrail + Insights, Reporting & Third Parties
Sec.Det.7	Amazon CloudWatch Events & Alarms + Amazon SNS + SIEM Solutions
Sec.Det.8	Amazon VPC Flow Logs + CloudWatch Alarms or other analytics tools
Security Perspective – Infrastructure Security Epic	
Sec.Inf.1	AWS WAF
Sec.Inf.2	AWS WAF, WAF Managed Rules + Automation
Sec.Inf.3	Amazon Virtual Private Cloud (VPC)
Sec.Inf.4	Amazon Virtual Private Cloud (VPC) + automation
Sec.Inf.5	Amazon Virtual Private Gateway (VGW) / AWS Direct Connect
Sec.Inf.6	Amazon EC2 Security Groups
Sec.Inf.7	Network Access Control Lists (NACLs)
Sec.Inf.8	Outbound Proxy Partners
Sec.Inf.9	Load Balancing
Sec.Inf.10	AWS Auto Scaling
Sec.Inf.11	Network infrastructure solutions in the AWS Marketplace
Sec.Inf.12	Reverse Proxy architecture
Sec.Inf.13	AWS EC2 Forward Proxy Servers
Sec.Inf.14	AWS Shield
Sec.Inf.15	AWS Systems Manager State Manager
Sec.Inf.16	AWS Systems Manager State Manager, or Third-Party or OSS File Integrity Monitoring Solutions on Amazon EC2
Sec.Inf.17	AWS Systems Manager State Manager, AWS Systems Manager Inventory, AWS Config
Sec.Inf.18	Honeypot and Honeynet Environments
Sec.Inf.19	Honeywords and Honeykeys
Sec.Inf.20	Amazon EC2 – Linux, SELinux – Mandatory Access Control
Sec.Inf.21	Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control
Sec.Inf.22	Amazon EC2 – Linux, FreeBSD – Hardening and Minimization

Control ID	Control Name
Sec.Inf.23	Amazon EC2 – Linux, Windows, FreeBSD – Address Space Layout Randomization (ASLR)
Sec.Inf.24	Amazon EC2 – Linux, Windows, FreeBSD – Data Execution Prevention (DEP)
Sec.Inf.25	Amazon EC2 – Windows – User Account Control (UAC)
Sec.Inf.26	Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC)
Sec.Inf.27	Microsoft Windows Security Baselines
Sec.Inf.28	Linux cgroups, namespaces, SELinux
Sec.Inf.29	Amazon EC2 – Windows – Device Guard
Sec.Inf.30	AWS Partner Offerings – File Integrity Monitoring
Sec.Inf.31	Third-Party Security Tools for Containers
Sec.Inf.32	Third-Party Security Tools for AWS Lambda Functions
Sec.Inf.33	AWS Partner Offerings – Anti-Malware Protection
Sec.Inf.34	AWS Lambda Partners
Sec.Inf.35	Container Partners – Security
Sec.Inf.36	AWS Partner Offerings – Behavioral Monitoring, Response Tools and Services
Security Perspective – Data Protection Epic	
Sec.DP.1	AWS Key Management Service (KMS) + AWS CloudHSM
Sec.DP.2	AWS KMS Key Policies
Sec.DP.3	AWS Certificate Manager + Transport Layer Security (TLS)
Sec.DP.4	AWS Partner Offerings – SQL Behavioral Analytics Proxies
Security Perspective – Incident Response Epic	
Sec.IR.1	Amazon GuardDuty + AWS Lambda
Sec.IR.2	AWS WAF + AWS Lambda
Sec.IR.3	Third-Party WAF Integrations
Sec.IR.4	Amazon GuardDuty + AWS Lambda + AWS WAF, Security Groups, NACLs
Sec.IR.5	AWS Config Rules
Sec.IR.6	Amazon CloudWatch Events + Lambda

Control ID	Control Name
Platform Perspective	
Platform.1	AWS Container and Abstract Services
Platform.2	AWS Lambda, Amazon Simple Queue Service (SQS), AWS Step Functions
Platform.3	Amazon Simple Email Service
Platform.4	Hypervisor-Level Guest-to-Guest and Guest-to-Host Segregation
Platform.5	AWS physical and operational security policies and processes
Operations Perspective	
Ops.1	CloudFormation + Service Catalog
Ops.2	Immutable Infrastructure – Short-Lived Environments
Ops.3	AWS Managed Services
Ops.4	AWS DR Solutions

Prioritize Controls Based on Control Coverage

Another way to leverage the unique control numbers, is to identify which controls provide the greatest level of coverage, and potentially provided the biggest ROI. Table 2 shows each place in the *courses of action matrix* that each control number appears.

For example, the table shows that by implementing control *Sec.Det.1*, (Amazon GuardDuty), you can provide Detection capabilities in all phases. This helps identify the benefits of enabling that one control, which provides significant Detection capability coverage across the phases of the intrusion kill chain framework.

You can use the control number for each control to help you prioritize your control implementations.

Table 2 – Controls Mapped to the Intrusion Kill Chain

	Detect	Deny	Disrupt	Degrade	Deceive	Contain	Respond	Restore
Recon – Pre-Intrusion	Sec.Det.1 Sec.Det.2 Sec.Inf.2 Sec.Det.6 Sec.Det.3 Sec.Det.4	Sec.Inf.3 Sec.IAM.3 Sec.DP.3 Sec.Inf.11 Sec.Inf.2 Sec.Inf.5	Sec.IR.1	Sec.Inf.18 Sec.Inf.19	Sec.Inf.18 Sec.Inf.19 Sec.IR.2	Sec.Inf.18 Sec.Inf.19	Sec.Inf.2 Sec.IR.1 Sec.Det.2 Sec.Det.4 Sec.Det.7	—
Recon – Post-Intrusion	Sec.Det.1 Sec.Det.2 Sec.Det.6 Sec.Det.3 Sec.Det.4	Sec.Inf.3 Sec.IAM.3 Sec.DP.3 Sec.Inf.11 Sec.Inf.12 Sec.IAM.6	Sec.IR.1	Sec.Inf.18 Sec.Inf.19	Sec.Inf.18 Sec.Inf.19 Sec.Inf.4	Sec.Inf.18 Sec.Inf.19 Sec.Inf.4	Sec.Inf.2 Sec.IR.1 Sec.Det.2 Sec.Det.4 Sec.Det.7	—
Weaponization	—	—	—	—	—	—	—	—

	Detect	Deny	Disrupt	Degrade	Deceive	Contain	Respond	Restore
Delivery	Sec.Det.1	Sec.Inf.3	Sec.Inf.3	Sec.IR.1	Sec.Inf.18	Sec.Inf.1	Sec.Inf.15	Sec.Inf.15
	Sec.Inf.2	Sec.Inf.5	Sec.Inf.6	Sec.Inf.14	Sec.Inf.19	Sec.Inf.3	Sec.Inf.30	Ops.1
	Sec.Inf.14	Sec.Inf.6	Sec.Inf.7	Sec.Inf.9	Sec.IR.2	Sec.Inf.6	Sec.IR.2	Ops.2
	Sec.Det.8	Sec.Inf.7	Sec.Inf.14	Ops.2		Sec.Inf.7	Sec.IR.3	
		Sec.Inf.14	Ops.2			Sec.IAM.4	Sec.IR.5	
		Sec.IAM.2				Sec.Inf.28	Sec.IR.6	
		Sec.IAM.4				Platform.1	Ops.3	
		Sec.IAM.5				Platform.2		
		Sec.IAM.6				Platform.4		
		Sec.Inf.20						
		Sec.Inf.21						
		Sec.Inf.22						
		Sec.Inf.26						
		Sec.Inf.27						
		Platform.5						

	Detect	Deny	Disrupt	Degrade	Deceive	Contain	Respond	Restore
Exploitation	Sec.Det.1	Sec.IAM.1	Sec.Inf.2	Sec.IR.1	Sec.Inf.18	Sec.IAM.1	Sec.Det.2	Sec.Inf.10
	Sec.Inf.2	Sec.IAM.5	Sec.IAM.5	Sec.Inf.1	Sec.Inf.19	Sec.IAM.4	Sec.Inf.31	Sec.Inf.15
	Sec.Inf.3	Sec.IAM.7	Sec.IAM.7	Sec.Inf.9	Sec.IR.2	Sec.Inf.20	Sec.Inf.32	Sec.Inf.30
	Sec.Inf.16	Sec.Inf.20	Sec.Inf.20	Ops.2		Sec.Inf.21	Sec.Inf.36	Ops.1
	Sec.Det.5	Sec.Inf.21	Sec.Inf.21			Sec.Inf.22	Ops.3	Ops.2
	Sec.Inf.31	Sec.Inf.22	Sec.Inf.23			Sec.Inf.26		
	Sec.Inf.32	Sec.Inf.23	Sec.Inf.24			Sec.Inf.28		
	Sec.Inf.33	Sec.Inf.24	Sec.Inf.25			Sec.Inf.31		
	Sec.Inf.34	Sec.Inf.25	Sec.Inf.26			Sec.Inf.32		
	Sec.Inf.35	Sec.Inf.26	Sec.Inf.31			Platform.1		
		Sec.Inf.27	Sec.Inf.32			Platform.4		
		Sec.Inf.31	Sec.Inf.33					
		Sec.Inf.32	Ops.2					
		Sec.Inf.33						
		Sec.Inf.34						
		Sec.Inf.35						
		Platform.3						
Installation	Sec.Det.1	Sec.IAM.2	Sec.IAM.5	Sec.Inf.9	Sec.Inf.18	Sec.IAM.4	Sec.Inf.15	Sec.Inf.10
	Sec.Det.6	Sec.IAM.4	Sec.Inf.15	Sec.Inf.15	Sec.Inf.19	Sec.Inf.20	Sec.Inf.16	Sec.Inf.15
	Sec.Det.3	Sec.IAM.5	Sec.Inf.20	Sec.Inf.22		Sec.Inf.21	Sec.Inf.17	Sec.Inf.30
	Sec.Det.4	Sec.IAM.6	Sec.Inf.21	Sec.Inf.29		Sec.Inf.26	Sec.Inf.30	Ops.1
	Sec.Inf.17	Sec.Inf.20	Sec.Inf.25	Sec.Inf.30		Sec.Inf.28		Ops.2
	Sec.Inf.31	Sec.Inf.21	Sec.Inf.26	Ops.2		Sec.Inf.31		
	Sec.Inf.32	Sec.Inf.25	Sec.Inf.29			Sec.Inf.32		
	Sec.Inf.33	Sec.Inf.26	Sec.Inf.30			Platform.1		
		Sec.Inf.29	Sec.Inf.33			Platform.4		
		Sec.Inf.33						

	Detect	Deny	Disrupt	Degrade	Deceive	Contain	Respond	Restore
Command and Control	Sec.Det.1	Sec.IAM.2	Sec.Inf.3	Sec.IR.1	Sec.Inf.18	Sec.IAM.2	Sec.Inf.31	Sec.Inf.10
	Sec.Det.6	Sec.IAM.4	Sec.Inf.6	Sec.IR.4		Sec.IAM.4	Sec.Inf.32	Sec.Inf.15
	Sec.Det.3	Sec.IAM.6	Sec.Inf.7	Ops.2		Sec.Inf.3	Sec.Inf.36	Sec.Inf.30
	Sec.Det.4	Sec.Inf.3	Sec.Inf.31			Sec.Inf.6	Sec.IR.1	Ops.1
	Sec.Inf.8	Sec.Inf.6	Sec.Inf.32			Sec.Inf.7	Ops.3	Ops.2
	Sec.Inf.13	Sec.Inf.7	Sec.IR.1			Platform.2		Ops.4
	Sec.Inf.31	Sec.Inf.31	Sec.IR.4					
	Sec.Inf.32	Sec.Inf.32	Ops.2					
Actions on Objectives	Sec.Det.1	Sec.IAM.2	Sec.IAM.2	Sec.IAM.2	Sec.Inf.18	Sec.IAM.2	Sec.Inf.31	Sec.Inf.10
	Sec.Det.6	Sec.IAM.4	Sec.Inf.20	Sec.Inf.9		Sec.IAM.4	Sec.Inf.32	Sec.Inf.30
	Sec.Det.3	Sec.IAM.6	Sec.Inf.21	Sec.Inf.20		Sec.Inf.3	Sec.Inf.36	Ops.1
	Sec.Det.4	Sec.Inf.20	Sec.Inf.26	Sec.Inf.21		Sec.Inf.6	Sec.IR.1	Ops.4
	Sec.Inf.8	Sec.Inf.21	Sec.Inf.31	Sec.Inf.26		Sec.Inf.7	Ops.3	
	Sec.Inf.13	Sec.Inf.26	Sec.Inf.32	Sec.DP.4		Sec.Inf.28		
	Sec.Inf.31	Sec.Inf.31	Sec.IR.5			Platform.1		
	Sec.Inf.32	Sec.Inf.32	Ops.2			Platform.4		
	Sec.DP.4	Sec.DP.1						
		Sec.DP.2						

Contributors

Contributors to this document include:

- Tim Rains, Leader Security & Compliance EMEA, Amazon Web Services
- Dave Walker, Security Solutions Architect, Amazon Web Services
- Enrico Massi, Security Solutions Architect, Amazon Web Services

Further Reading

For additional information, see:

- AWS Cloud Adoption Framework Security Perspective
- Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
- Security Pillar AWS Well-Architected Framework
- Comprehensive list of security-focused content

Document Revisions

Date	Description
February 2019	First publication

Notes

[1] Defined in the 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf