Breaking Intrusion Kill Chains with AWS

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

Abstract

Today, many Chief Information Security Officers and cybersecurity practitioners are looking for an effective cybersecurity strategy that will help them achieve measurably better security for their organization. One strategy that has helped many organizations accomplish this is the *Intrusion Kill Chain* strategy.

This paper provides background context on this framework, outlines how to mitigate attackers' intrusion kill chains using the AWS cloud platform, and offers advice on how to measure the effectiveness of this approach.

Introduction

Cybersecurity threats continue to challenge organizations around the world. Many of the cybersecurity strategies that organizations have employed over the past two decades have failed to stop networks from being compromised and data breaches. This has led many Chief Information Security Officers (CISOs) and cybersecurity practitioners to look for more effective strategies to manage cybersecurity risk for their organizations.

One such strategy, pioneered by Lockheed Martin Corporation, is described in the Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains paper.

> Intelligence-driven computer network defense is a necessity in light of advanced persistent threats. As conventional, vulnerability-focused processes are insufficient, understanding the threat itself, its intent, capability, doctrine, and patterns of operation is required to establish resilience. The intrusion kill chain provides a structure to analyze intrusions, extract indicators and drive defensive courses of actions. Furthermore, this model prioritizes investment for capability gaps, and serves as a framework to measure the effectiveness of the defenders' actions.[1]

Since Lockheed Martin's paper was published in 2011, many variations of intrusion kill chain strategies have been developed in the cybersecurity industry, and many organizations have benefited from implementing an intrusion kill chain strategy.

This whitepaper offers a variation of Lockheed Martin's intrusion kill chain strategy, based on the AWS cloud platform. Combining an intrusion kill chain approach with the inherent benefits of the cloud, and the plethora of security

---

[1] Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. (Lockheed Martin, Bethesda, MD, 2011), 12.

* For consecutive citations (such as Footnotes 2–16): Ibid.

controls that AWS provides will help many organizations achieve measurably better cybersecurity versus what they have been able to accomplish in on-premises and managed service provider environments, likely at a lower cost.

What is an Intrusion Kill Chain?

Many attackers employ a repeatable process that helps them identify their target and potential weaknesses in their target's security posture, as well as ways to exploit these weaknesses. Once the victim's weaknesses are successfully exploited, attackers use illicit access to their victim's infrastructure for a range of nefarious purposes, including data theft, compromising data integrity, destroying data and/or infrastructure, disrupting operations, and perpetrating attacks on other victims. The process that attackers use to conduct an attack is known as an *intrusion kill chain*.[2]

Attackers perform different tasks in each phase of their intrusion kill chain, as they plan and execute their intrusion attempts. The AWS Cloud Intrusion Kill Chain approach modifies previous models slightly, so that organizations can leverage the inherent benefits of the cloud and the mitigations provided by AWS to break intrusion kill chains.

[2] Ibid.

This approach includes the following phases:

1. *Reconnaissance – Pre-intrusion*

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

2. *Reconnaissance – Post-intrusion*

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

3. *Weaponization*[3]

   In this phase, attackers plan and acquire the tools they'll use to try to exploit the weaknesses they believe the victim has. For example, they could build a malformed PDF file that is specially crafted to exploit a vulnerability in a PDF parser they know their intended victim uses. Attackers might also develop malware to steal system login credentials from the victim.

4. *Delivery*[4]

   This is the phase in the intrusion kill chain where the attackers transmit their weapon to the intended victim. Examples of delivery mechanisms include phishing emails, malicious email attachments, drive-by download sites, etc.

[3] Ibid.

[4] Ibid.

5. *Exploitation*[5]

   After the weapon has been delivered to the target, the weapon seeks 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—also known as *social engineering*. Another weakness that attackers typically try to exploit is weak, leaked or stolen passwords.

6. *Installation*[6]

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

7. *Command and Control*[7]

   Attackers maintain illicit access to their victims' environments and potentially remotely control compromised infrastructure.

8. *Actions on Objectives*[8]

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

---

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

Breaking Intrusion Kill Chains

Understanding intrusion kill chain phases helps security teams formulate ways to break them. Lockheed Martin's intrusion kill chain strategy describes a *courses of actions matrix*[9] (illustrated below) that helps plan courses of action against each phase in the intrusion kill chain. These actions include, detect, deny, disrupt degrade deceive, and destroy.[10]

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Courses of Action Matrix

The concept is for defenders to build capabilities that detect, deny, disrupt, degrade, deceive, and destroy attackers' efforts in each phase of the intrusion kill chain. Stopping the intrusion as early in the attack as possible is the goal, because this reduces the recovery time, effort, cost, and damage associated with each attack. For example, detecting an attack in the Reconnaissance phase is preferable to degrading the attack in the Command and Control phase.

[9] Ibid.

[10] Ibid.

The AWS approach extends the courses of action available to defenders so that organizations can leverage the inherent benefits of the cloud and the mitigations provided by AWS.

The courses of action have been modified in the following ways:

1. *Destroy*[11] has been removed.
   Although this course of action is appropriate in a military context, few non-military organizations have the capability or charter to destroy their adversaries. Outside of a military context such activities would likely be illegal as well.

2. *Contain* has been added to the courses of action.
   Containing attackers that successfully penetrate an IT environment is a prudent course of action. Preventing lateral movement and the credential theft and reuse attacks typically associated with lateral movement, will reduce potential damage and speed recovery. AWS provides several controls that enable customers to contain attackers. For more information, see the *Breaking Intrusion Kill Chains with AWS Reference Material*.

3. *Respond* has been added to the courses of action.
   Security teams need to plan for successful intrusions in order to be prepared to respond effectively and efficiently, should an intrusion ever occur. AWS provides customers with response capabilities that help reduce the time, effort, damage, and costs associated with intrusion attempts.

[11] Ibid.

4. *Restore* has been added.
   In the scenario where every course of action that an organization has implemented fails across every phase of the intrusion kill chain, restoring data and infrastructure as quickly as possible will be important to restoring business as usual. The AWS Cloud supports many popular disaster recovery (DR) architectures from *pilot light* environments that may 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.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain	Respond	Restore
Reconnaissance: pre-intrusion								
Reconnaissance: post-intrusion								
Weaponization								
Delivery								
Exploitation								
Installation								
Command and Control								
Actions on Objectives								

Modified Courses of Action Matrix[12]

[12] Ibid.

Definitions of the courses of action included in the matrix are below. All of the following definitions are based on definitions published in *Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment*.[13]

- *Detect* – To discover or discern the existence, presence, or fact of an intrusion into information systems.
- *Deny* – To prevent the adversary from accessing and using critical information, systems, and services.
- *Disrupt* – To break or interrupt the flow of information.
- *Degrade* – To reduce the effectiveness or efficiency of adversary C2 [command and control] or communications systems, and information collection efforts or means.
- *Deceive* – 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.
- *Protect* – To take action to guard against espionage or capture of sensitive equipment and information.
- *Respond* – To react quickly to an adversary's or another's IO attack or intrusion.
- *Restore* – To bring information and information systems back to their original state.
- *Contain* – The action of keeping something harmful under control or within limits.

[13] Defined in 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

AWS services and AWS Partners' services can be mapped to this *Courses of Action matrix*[14]. Performing this mapping exercise can help identify which services, features, and functionality can help organizations detect, deny, disrupt, deceive, contain attacks, as well as respond to them and help recover from them when necessary.

Using the Installation phase as an example, you can use the following AWS services and third-party services to help you to detect, deny, disrupt, deceive, contain, respond, and recover during this phase of the intrusion kill chain.

- *Detect* – Using log data from Amazon CloudWatch and AWS CloudTrail, and reporting tools such as Amazon Elasticsearch, Amazon QuickSight and third-party tools can help to detect installation activity.
- *Deny* – AWS Identity and Access Management (IAM) can enforce authentication, authorization, and permissions to resources that can limit the blast radius of an exploit and subsequent installation of malware.
- *Disrupt* – AWS Systems Manager State Manager can monitor the configuration of a large set of instances, specify a configuration policy for the instances, and automatically apply updates or configuration changes. This can help disrupt post-exploitation changes to operating systems.
- *Deceive* – Third-party deception technologies present themselves as part of legitimate infrastructure so that when an attacker attempts to compromise it, it helps detect, contain, and recover faster.
- *Contain* – With AWS Organizations, Service Control Policies (SCPs) can be created that centrally control AWS service use across multiple AWS accounts. SCPs put bounds around the permissions that AWS Identity and Access Management (IAM) policies can grant to entities in an account, such as IAM users and roles. For example, SCP policies can be used to allow or deny certain activities so that no principals, not even the *super-user* in a child AWS account can bypass them, thus implementing a form of mandatory access control. This can help contain attackers during the Installation phase.

[14] Hutchins, Op.Cit., Page. 5.

- *Respond* – 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. Some of these solutions can help respond during the Installation phase. Additionally, AWS Lambda can be used to automatically execute a function in response to an event in order to mitigate the threat or stop lateral movement. AWS Systems Manager State Manager and some AWS Technology Partners can monitor file integrity.
- *Restore* – During the response to an incident, if a tool automatically shuts down a virtual instance of an operating environment, for example, autoscaling can create a new instance automatically from reference images to replace it, thus helping to restore infrastructure automatically and quickly.

In addition to the services and functionality listed above, numerous other AWS and third-party services and functionality are available courses of action in the Installation phase of the intrusion kill chain.

Using multiple services and features to detect, deny, disrupt, deceive, contain, respond, and recover, in each phase of the intrusion kill chain can make it increasingly difficult for attackers to be successful. Attackers are faced with the challenge of defeating layers of defensive cybersecurity capabilities in each phase of their intrusion kill chain, in order to be successful.

How to Get Started

Where to start depends on where your organization is in its cloud adoption journey. For example, it makes little sense for you to leverage an approach that relies on a well-implemented identity strategy if your organization doesn't have such a strategy. Put another way, investing the time and resources to ensure your organization has successfully implemented the building blocks that a cybersecurity strategy requires, is a prerequisite to implementing and operating a successful cybersecurity program.

Two tools that can help you in your cloud adoption journey are the AWS Cloud Adoption Framework and the AWS Well-Architected Framework.

The AWS Cloud Adoption Framework is designed to help organizations develop efficient and effective plans for their cloud adoption journey. The guidance and best practices provided by the framework help you build a comprehensive approach to cloud computing across your organization, and throughout your IT lifecycle.

The Well-Architected Framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure appropriate for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help implement designs that will scale with your application needs over time. It includes strategies to help you compare your workload against our best practices, and obtain guidance to produce stable and efficient systems so you can focus on functional requirements. There is also a comprehensive list of security-focused content that members of your security team should review as you prepare for AWS adoption initiatives.

For organizations that decide to leverage an intrusion kill chain cybersecurity strategy, AWS provides an example of how AWS services and functionality can be mapped to the intrusion kill chain model. This example mapping can help organizations save time, resources and budget when architecting and implementing an intrusion kill chain strategy in AWS.

For more detailed information about how to get started, see the Break Intrusion Kill Chains with AWS Reference Material.

Measuring the Effectiveness of Mitigations

Another advantage of using an intrusion kill chain strategy is the ability to measure its effectiveness. To do this, defenders use the *intrusion reconstructions*[15] concept, which is outlined in the Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains paper, to measure the effectiveness of the mitigations they've implemented to break attackers' intrusion kill chains.

An intrusion reconstruction is an exercise conducted by security teams whenever there is an intrusion attempt—whether the intrusion is successful, partially successful, or completely unsuccessful. The objective of the intrusion reconstruction is to determine which phase of the intrusion kill chain the attackers were stopped in, and why the attackers weren't stopped earlier in the intrusion kill chain. A reconstruction exercise should be done days or weeks after the attack has been mitigated, not during an attack, to ensure resources are properly focused on both the attack and later on the reconstruction.

To ensure all the information required for an accurate reconstruction is readily available, participants in an intrusion reconstruction should include all the individuals and teams that architected, implemented, and operate the intrusion kill chain strategy. The Incident Response team responsible for responding to the attack should lead the intrusion reconstruction. In some scenarios, it also makes sense to include vendors whose products and services were involved in the intrusion attempt.

The participants work together to create a timeline of events that occurred during the intrusion. When did the intrusion attempt start and what does the organization know about the attacker's kill chain from the data collected on the intrusion? If attackers were stopped before the end of their kill chain, in which phase did the kill chain break and how did it break? If attackers weren't stopped, what was the result of the intrusion? The more detailed and accurate the information collected on the intrusion is, the easier it is to pinpoint failures and substandard performance of people, process, and technologies.

Intrusion reconstructions can be very helpful to:

[15] Ibid.

- Identify which controls worked as advertised and expected
- Identify which controls failed to perform as expected
- Identify which control integrations worked or failed, and correct them
- Discover where there are gaps in security control coverage, and address them
- Confirm the organization's security control investment priorities
- Identify people and processes that performed/underperformed
- Help inform pen test/red team exercises
- Better understand security control capability efficacy
- Provide helpful data for security vendor renewal discussions
- Inform governance, risk, and compliance, and build a business case for appropriate changes

Key questions to ask during an intrusion reconstruction include:

- How far did attackers get with their intrusion kill chain before they were detected?
- How long did it take for the attack to be detected?
- What controls failed to protect and detect?
- Where did gaps in protection and detection controls contribute to attacker success?
- Did the defender's success rely on good fortune instead of specific mitigating controls that were designed to stop attacks?
- Was data exfiltration attempted and successful?
- Did the Security Operations Center get the data they needed to detect intrusions?
- Did the Incident Response process work as designed?
- Did IT partner with the Cybersecurity team and Incident Response team during the intrusion as planned?
- How did your vendors help?

The output from an intrusion reconstruction exercise should include a clearer picture of what the attacker's intrusion kill chain looked like, and how the organization's current security control set performed. It should be clear how attackers defeated or by-passed the organization's security controls in any phase of the kill chain they were successful in. Finally, a plan to address the shortcomings identified in the reconstruction, to reduce the time to detection and improve security control efficacy for future intrusion attempts, is a critical output.

Conclusion

For organizations looking for an effective cybersecurity strategy, the intrusion kill chain strategy is a strong option. It is an effective strategy for on-premises, hybrid, and cloud environments alike. Systematically architecting and implementing controls that break attackers' intrusion kill chains make it much more difficult for attackers to be successful. Intrusion reconstructions are powerful tools in measuring the effectiveness of an intrusion kill chain strategy, and help security team rationalize their future cybersecurity capability investments.

Document Revisions

Date	Description
February 2019	First publication