AWS re:Invent

WPS317-R

Compliance automation for the Public Sector

Rob Nolen
Principal Solutions Architect
Amazon Web Services

AWS re:Invent

aws

Agenda

Criticality of maintaining compliance

Introduction to AWS security services

Scenario 1: Network connectivity

Scenario 2: Security group management

Scenario 3: Amazon GuardDuty findings

Maintaining compliance is critical

AWS has dozens of compliance certifications

For Government and Public Sector workloads, it’s vital to maintain confidentiality, integrity, and availability

Cloud enables agility and speed but has tooling to help with building in compliance

AWS security solutions

https://www.nist.gov/cyberframework

Identify

AWS Systems Manager

AWS Config

Protect

AWS Systems Manager

Amazon Inspector

Amazon Virtual Private Cloud

AWS Key Management Service

AWS CloudHSM

AWS Identity and Access Management

AWS Organizations

Amazon Cognito

AWS Directory Service

AWS Single Sign-On

AWS Certificate Manager

Amazon Inspector

Detect

AWS CloudTrail

AWS Config rules

Amazon CloudWatch Logs

Amazon GuardDuty

Amazon VPC Flow Logs

Amazon Macie

AWS Shield

AWS WAF

Respond

AWS Config rules

AWS Lambda

AWS Systems Manager

Amazon CloudWatch Events

Recover

AWS Lambda

AWS disaster recovery and backup solutions

Security benchmarks and frameworks

NIST 800-53 (RMF): Core of FedRAMP and DoD Security Requirements Guide

CIS AWS Benchmark: DoD and Fed reference CIS rules, and many large organizations use benchmark as a base for their postures

Key services

AWS CloudTrail

Amazon GuardDuty

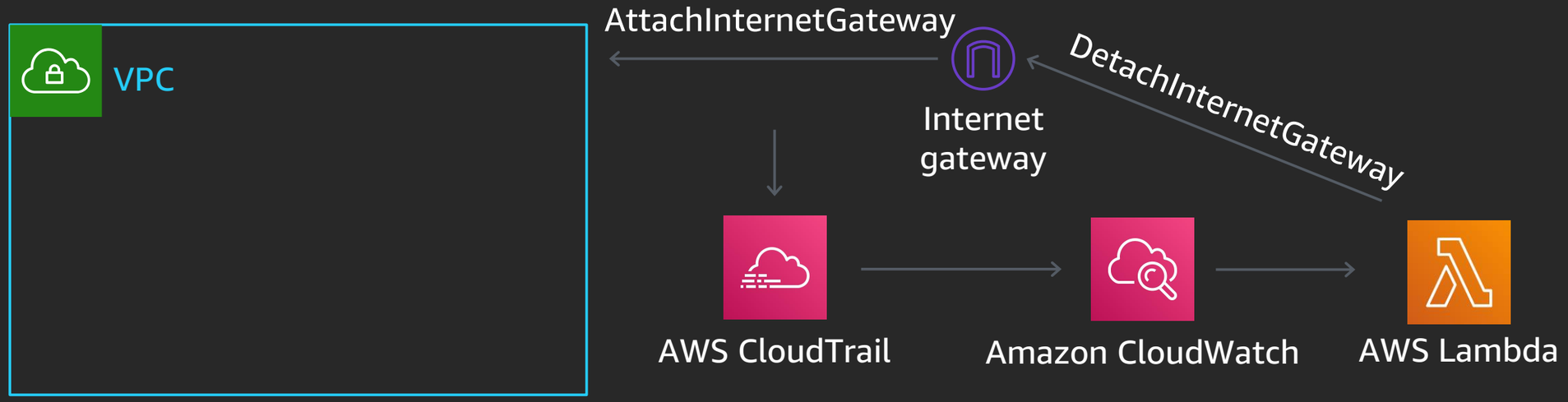
Amazon CloudWatch

https://bit.ly/2X7wkaM

Scenario 1

Scenario 1: VPC networking

Control of network traffic must be done via managed access points (CIS Benchmark 4.4, NIST 800-53 AC-17(3))



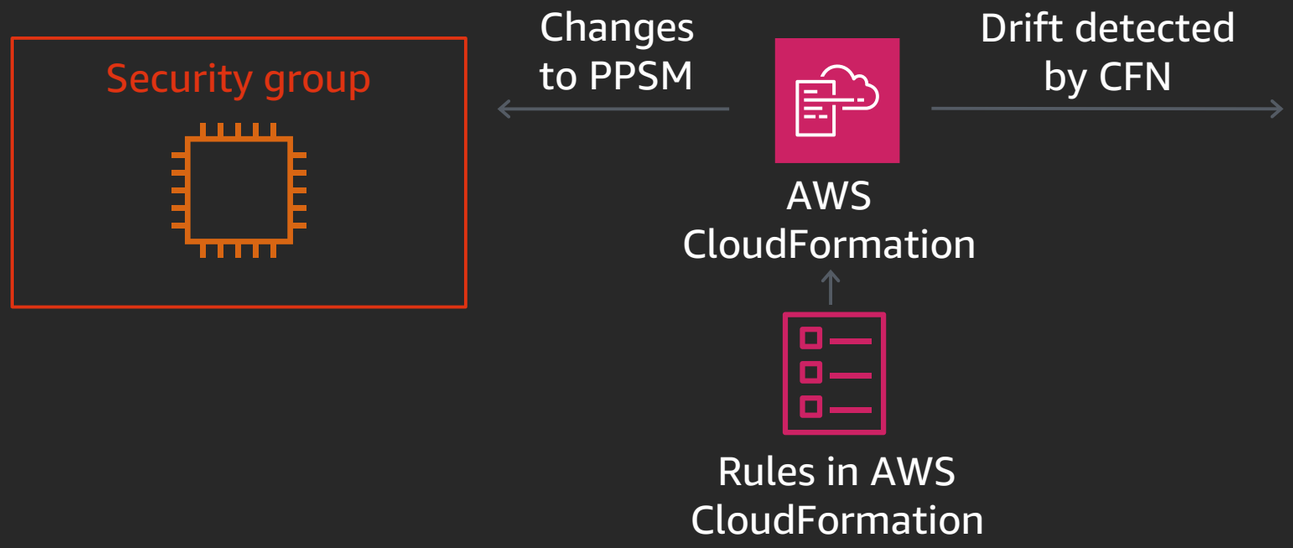
Scenario 2

Scenario 2: Security groups

NIST 800-53 CM-7(1)(a): Reviews the information system [Assignment: Organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services

NIST 800-53 CM-7(1)(b) Disables [Assignment: Organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure]

CIS Benchmark 4.1–4.3 for security group management

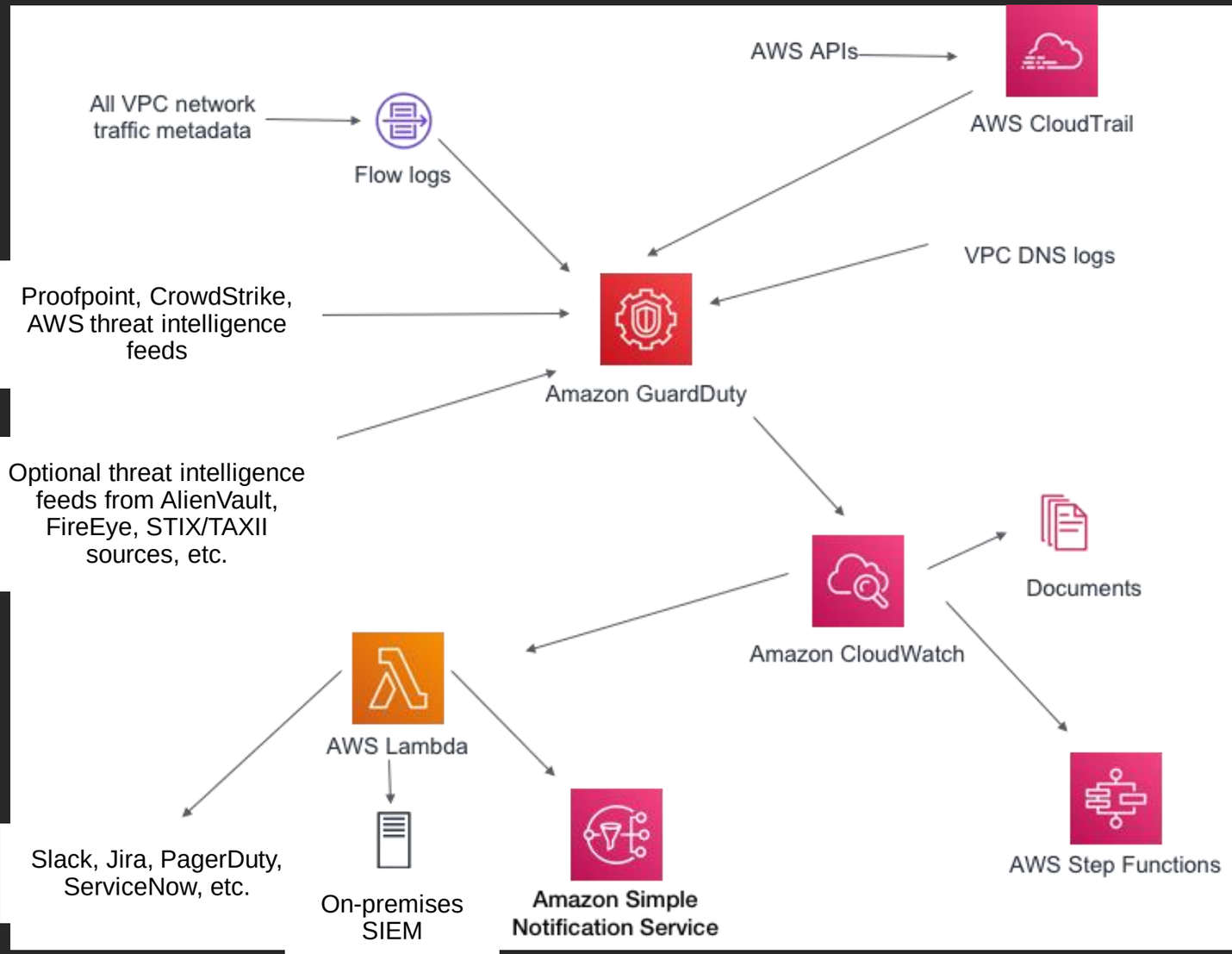


Scenario 3

Scenario 3: Amazon GuardDuty findings

CIS Benchmark 3.1: Ensure that a log metric filter and alarm exist for unauthorized API calls

NIST 800-53 IR-5(1): The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information



Thank you!

Rob Nolen

nolenr@amazon.com

AWS re:Invent

aws

Please complete the session survey in the mobile app.