AWS

Cloud-Native Security Maturity: Designing for Scalability and Compliance

Purnaresa Yuliartanto
Sr Security Solutions Architect
AWS ASEAN

AWS, the Trusted Cloud Platform for Secured Regulated Workload in Indonesia

Ransomware Attack Prompts Transfer of Indonesia's Immigration Data to Amazon Web Service

Bella Evanglista, Antara
June 28, 2024 | 9:54 pm

SHARE

Justice Minister Yasonna Laoly speaks during an interview at BTV studio in Jakarta on January 5, 2023. (B-Universe photo/Uthan A. Rachim)

Jakarta. Law and Human Rights Minister Yasonna Laoly has confirmed that immigration data services, now hosted on Amazon Web Service (AWS) following a cyberattack, are secure.

Erick Thohir Gandeng Amazon Web Service Demi Efisiensi Kerja BUMN

Menteri BUMN Erick Thohir resmi menggandeng Amazon Web Service (AWS) dalam rangka efisiensi operasional BUMN

Arief Rahman H
Diperbarui 14 Nov 2024, 11:00 WIB

Copy Link Share 12

Implementasi Keamanan Siber bagi BUMN di AWS

Blog AWS Indonesia

by Purnaresa Yuliartanto and Muhamad Yopan | on 05 MAR 2025 | in Best Practices, Security, Identity, & Compliance | Permalink | Share

Keamanan adalah prioritas utama di AWS (Amazon Web Services). Untuk memastikan penggunanya memiliki sistem keamanan yang memadai, AWS telah menerbitkan berbagai dokumen panduan, termasuk AWS Cloud Adoption Framework Security dan AWS Blueprint for Ransomware Defense.

Melalui blog ini, AWS ingin memberikan panduan khusus bagi pengguna AWS di Indonesia, terutama Badan Usaha Milik Negara (BUMN), dalam mengimplementasikan Prioritas Penerapan Keamanan Siber sesuai dengan ketentuan yang tercantum dalam Keputusan Menteri (Kepmen) BUMN Nomor SK-275/MBU/11/2024. Penting untuk dicatat bahwa di luar solusi teknologi yang akan dibahas, setiap organisasi perlu memastikan kesiapan sumber daya manusia (SDM) dan proses yang matang untuk menjalankan operasional keamanan secara efektif dan berkelanjutan.

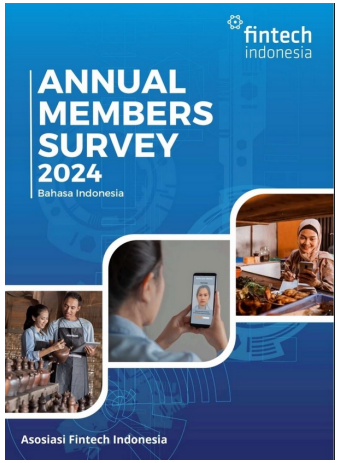
Ringkasan

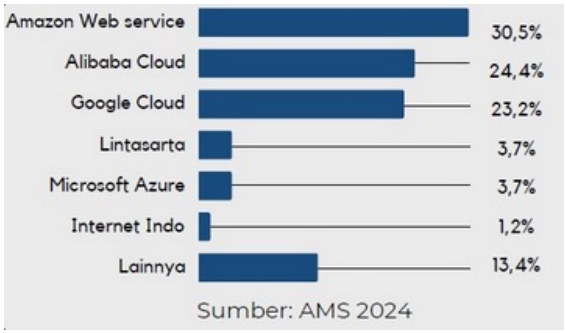
Kepmen Prioritas Penerapan Keamanan Siber mengatur dua kategori penerapan keamanan siber:

A. Penerapan 15 kontrol prioritas

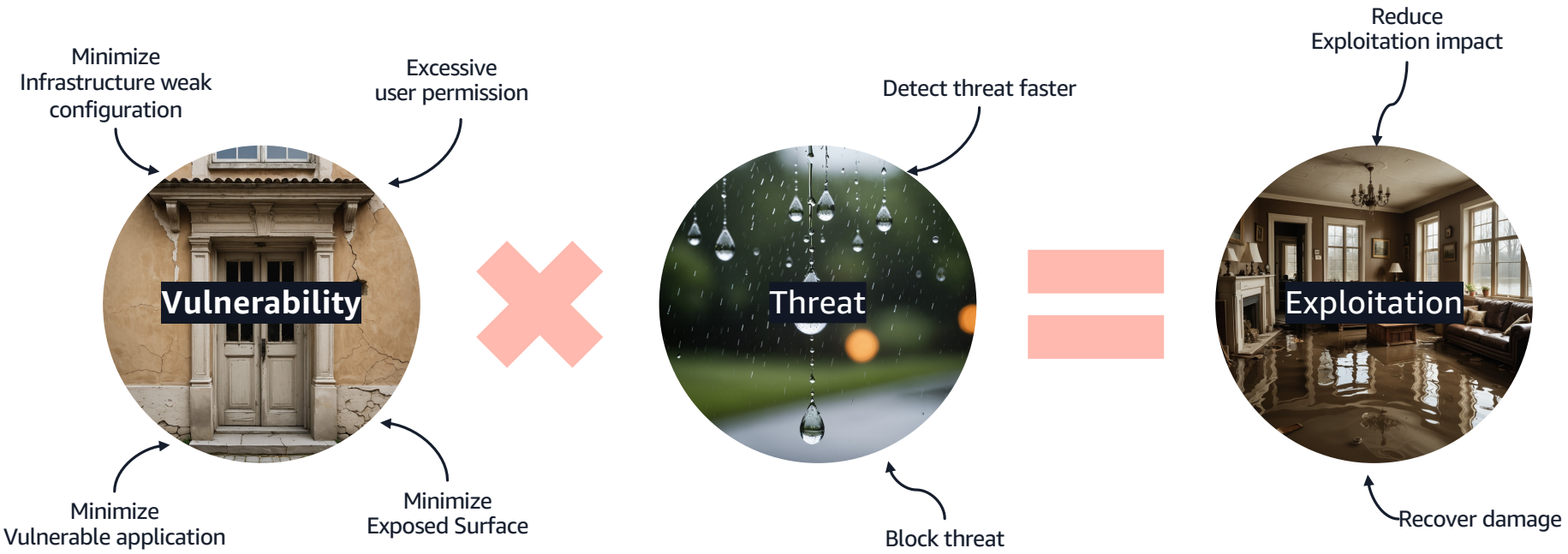
B. Penerapan Kerangka Keamanan Siber (Security Framework) dengan standar internasional seperti NIST atau CIS

Kedua kategori tersebut dapat diterapkan secara simultan dan bersifat komplementer untuk menciptakan sistem keamanan yang komprehensif.





Component of Cybersecurity Incident



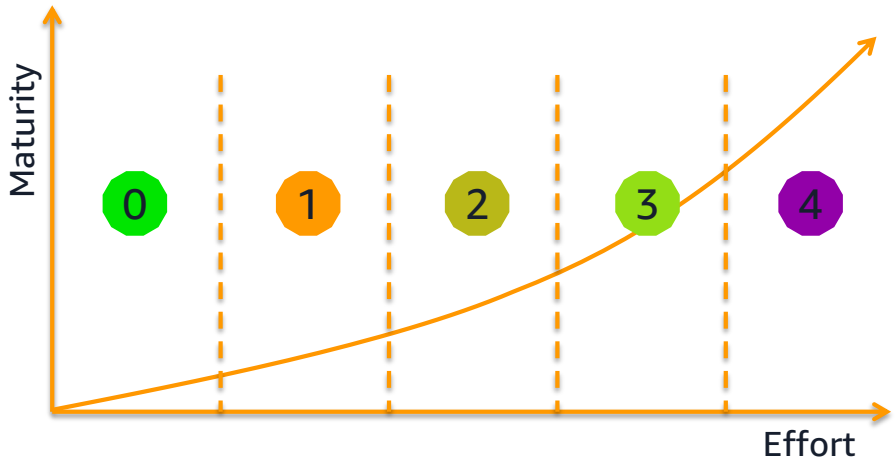
AWS Security Maturity Model

Security Capabilities

Identity & access management	Security assurance	Threat detection
Vulnerability management	Security governance	Infrastructure protection
Data protection	Application security	Incident response

The AWS Cloud Adoption Framework (CAF) offers capabilities to achieve confidentiality, integrity, and availability for data and workloads.

Security Maturity Phase



1 Quick Wins

2 Foundations

3 Efficient

4 Optimizing

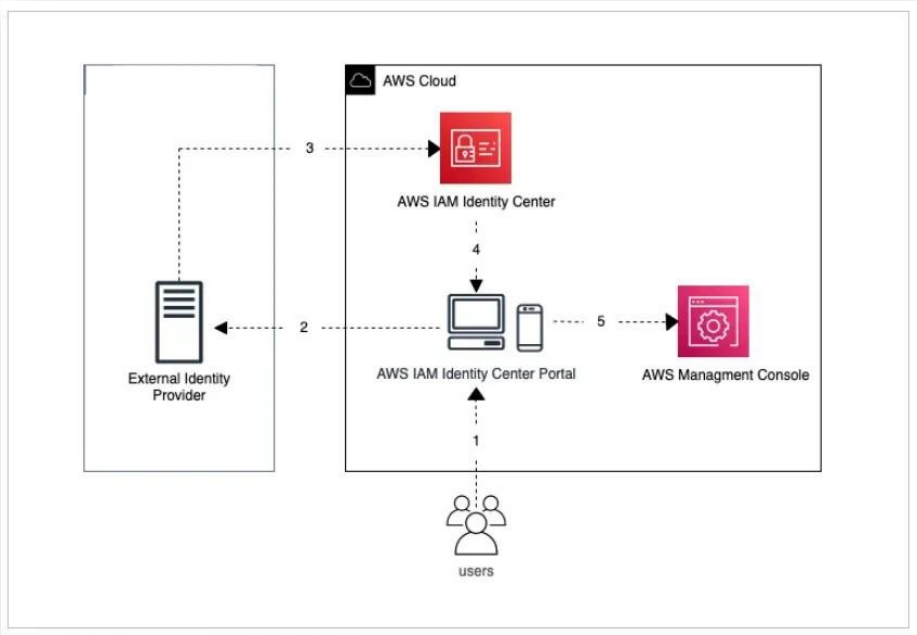
1. Identity and Access Management

Secures identities (human and machine) and permissions to AWS resources, enforcing least privilege access and automating access control.

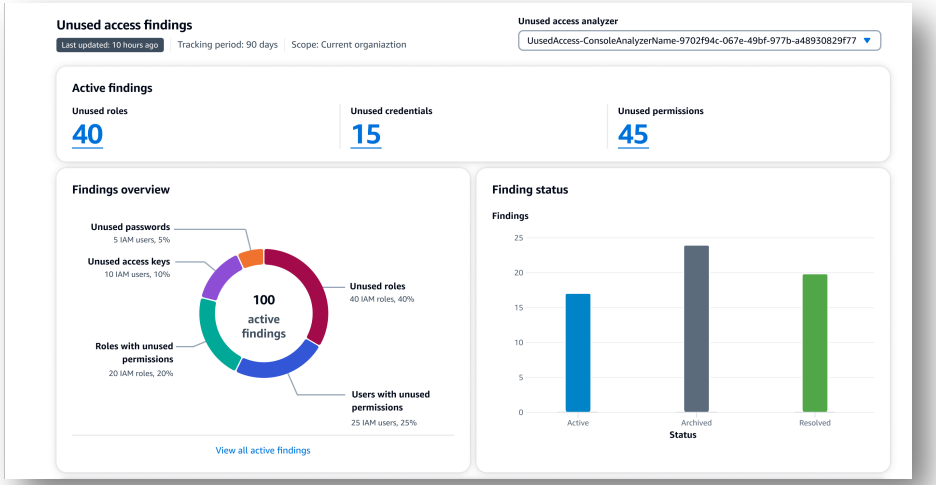
Identity and Access Management

Operation Workflow

[1] Provision Access → [2] Grant Permission → [3] Review Permission Usage



Provision Access using Single Sign On

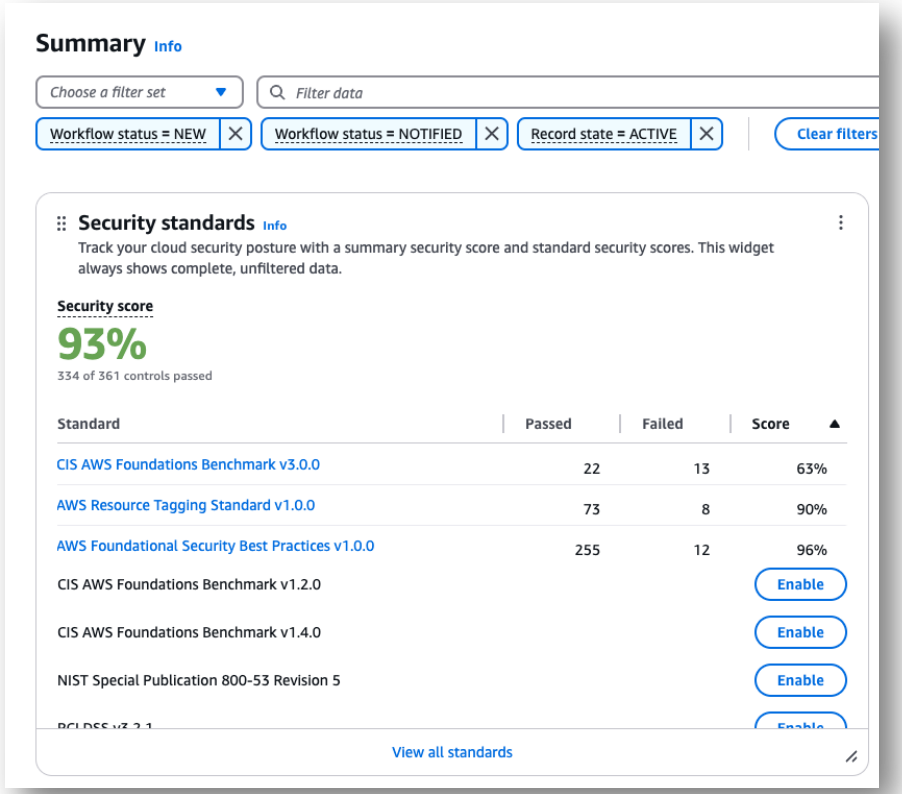


Review Permission using IAM Access Analyzer

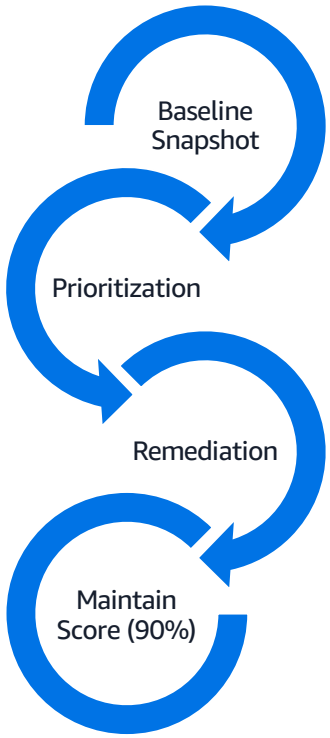
2. Security Assurance

Monitors, evaluates, and validates security controls to ensure they work as intended and meet security standard.

Build Security Posture using AWS Security Hub

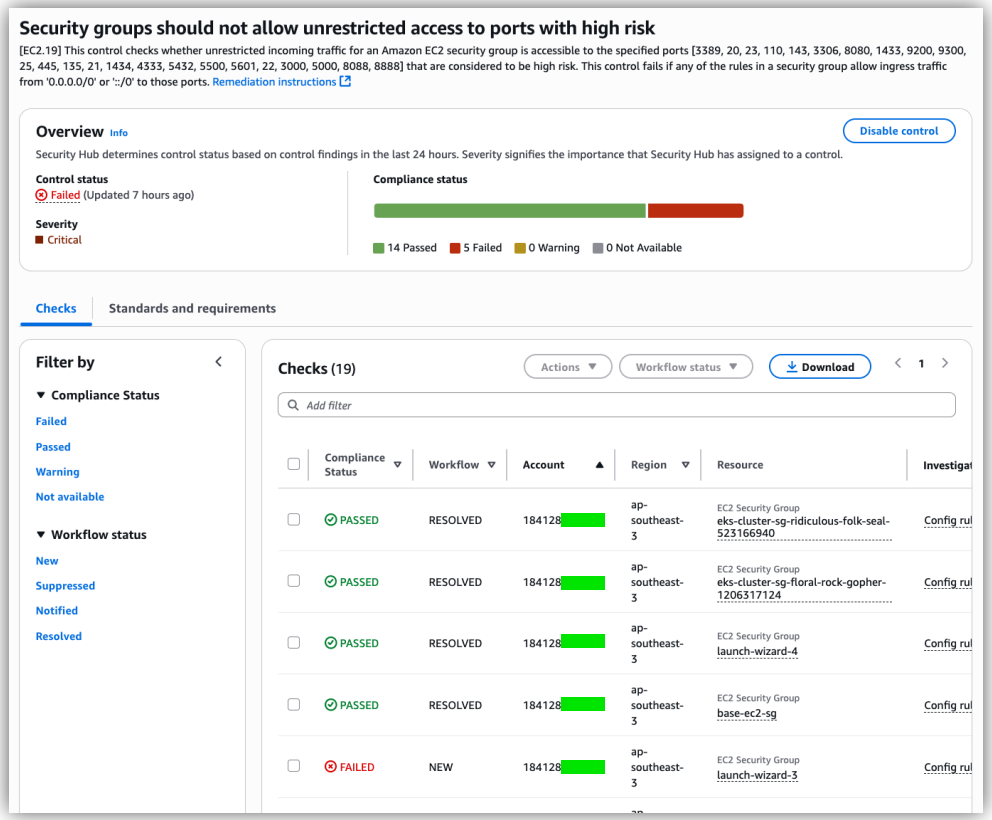


AWS Security Hub



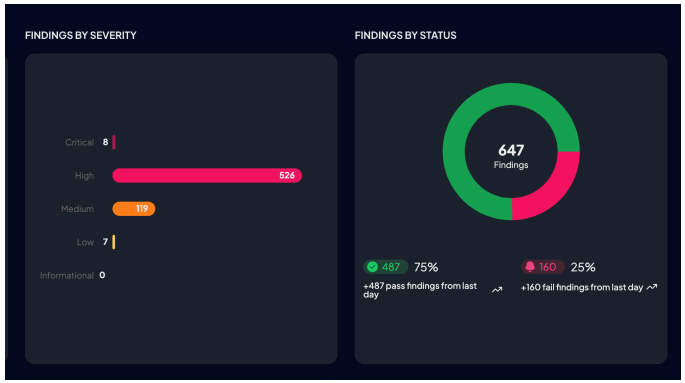
Operation Workflow

Remediate Weak Configuration



Failed Compliance Check

- Security Hub provides granular visibility into non-compliant resources, highlighting exactly which security groups have unrestricted access to high-risk ports.
- This detailed resource-level reporting enables targeted remediation efforts.

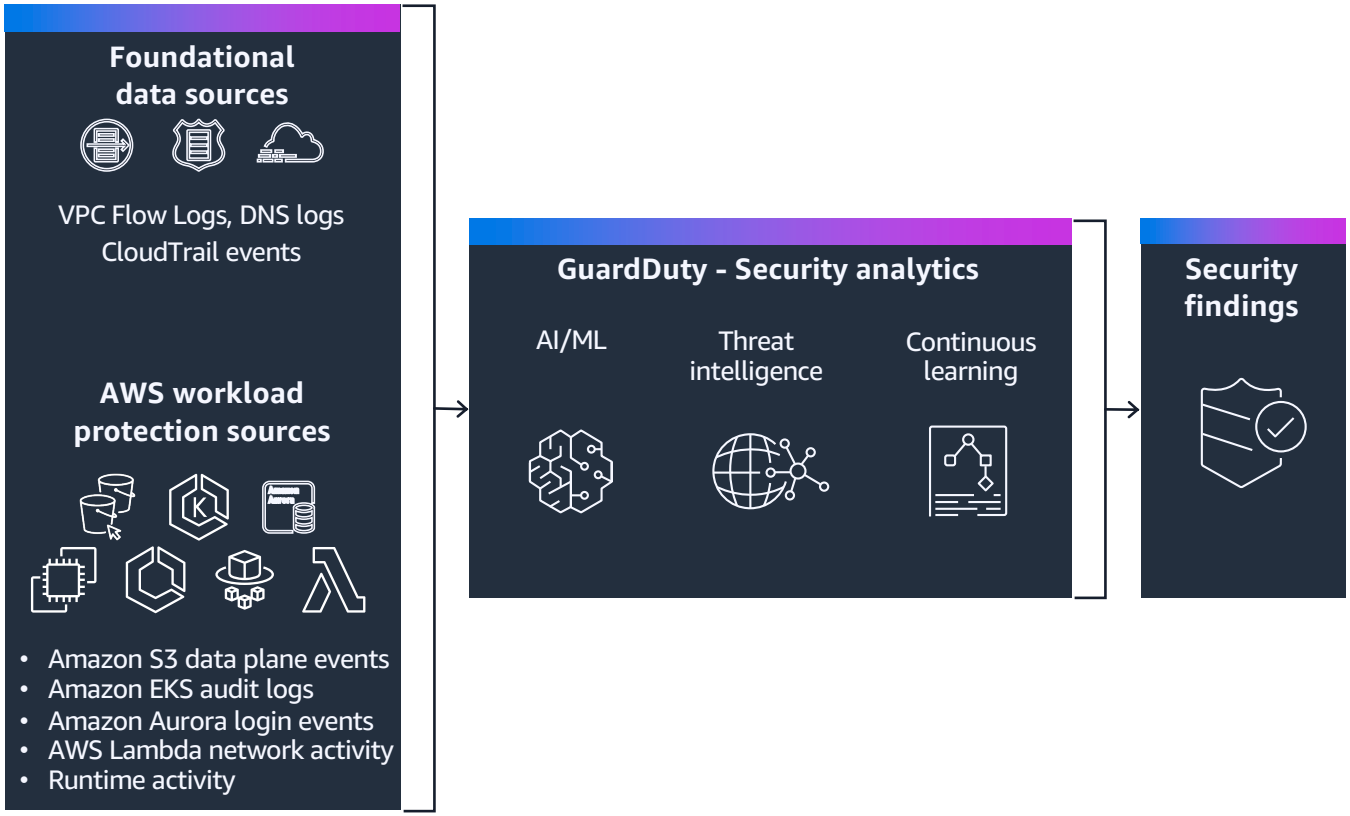


Prowler - Open Source Alternative

3. Threat Detection

Monitors, analyzes, and alerts on potential security events to detect malicious activities.

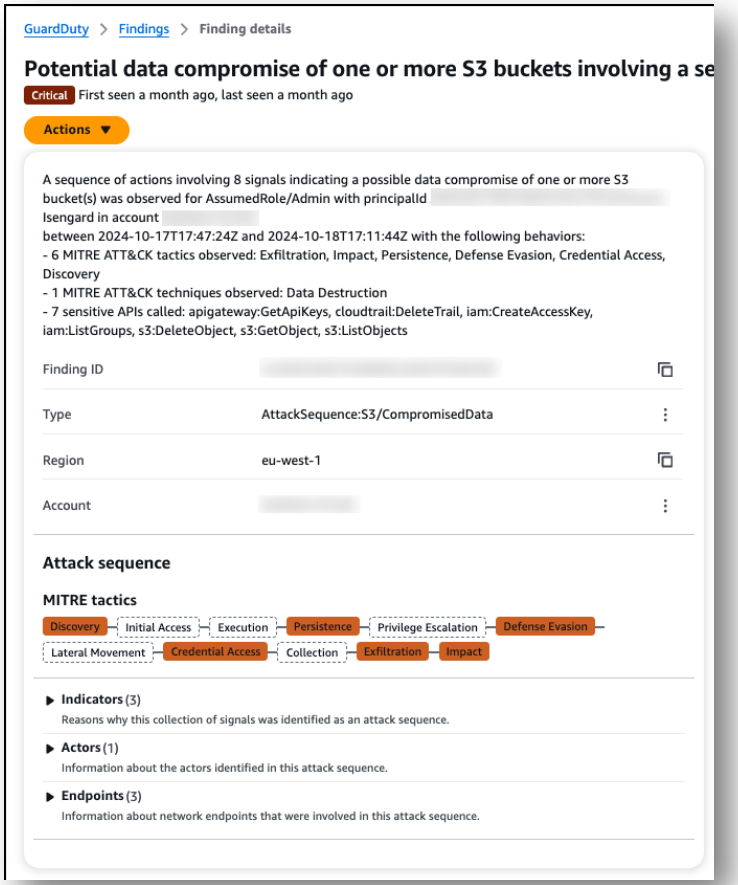
Threat Detection on AWS



Operation Workflow

Threat Detection Strategy

GuardDuty detection Findings



Success Metrics:

- ~~Number of finding~~
- ~~Severity of finding~~
- Time to resolve finding

4. Infrastructure protection

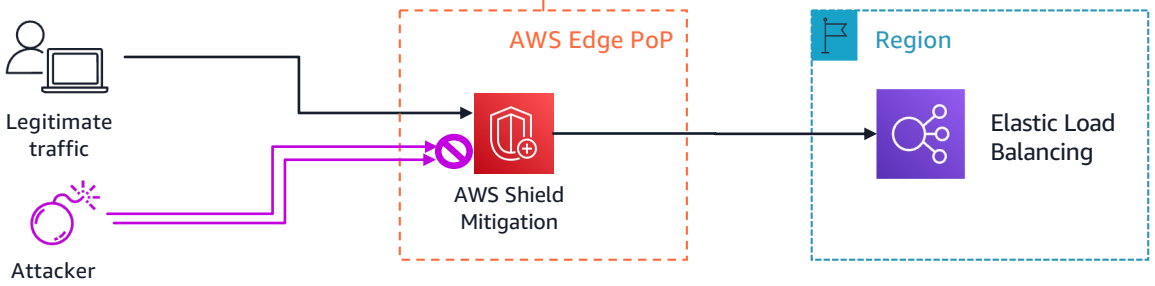
Confirm that systems and services within your workload are protected against unintended and unauthorized access and potential vulnerabilities.

Infrastructure (L3-4) Protection with AWS Shield

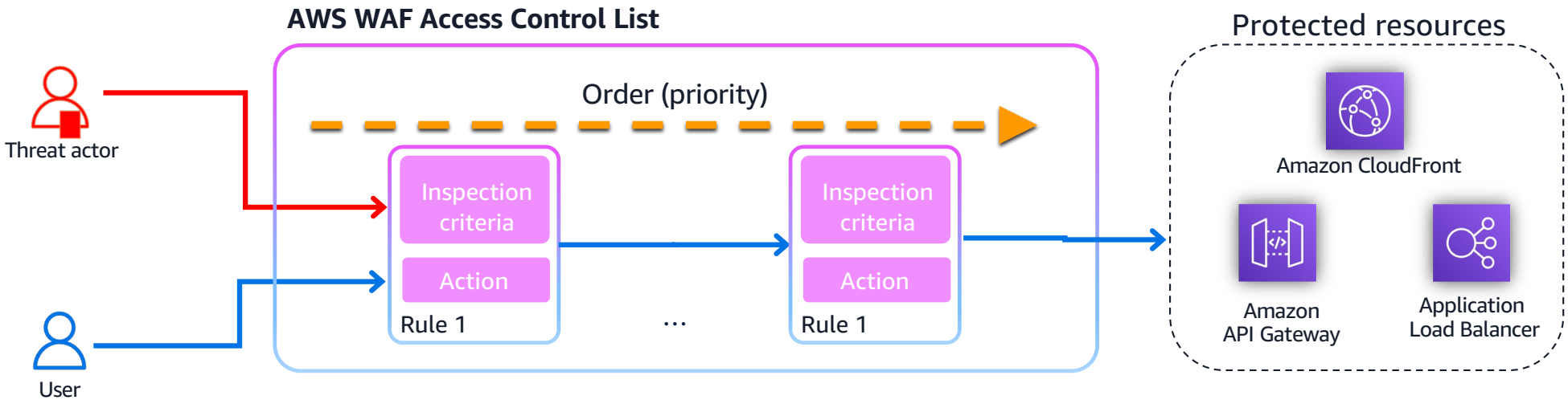
AWS Shield DDoS **mitigation systems** are present at the AWS network border and at AWS edge locations.

AWS Shield @Edge

- SYN Proxy
- Continuous inspection (inline)
- Packet validation
- Distributed scrubbing capacity
- Automated routing policies to absorb large attacks



Application L7 Protection with AWS WAF



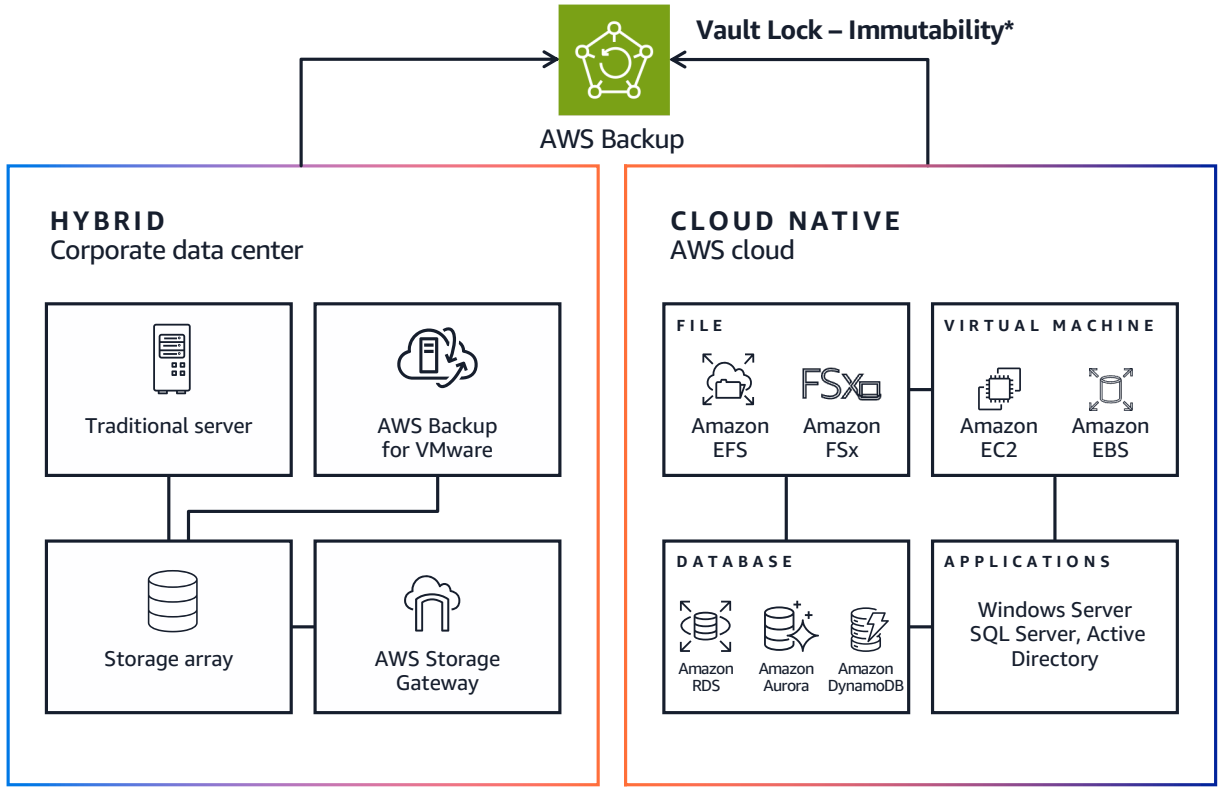
AWS WAF Rule Type

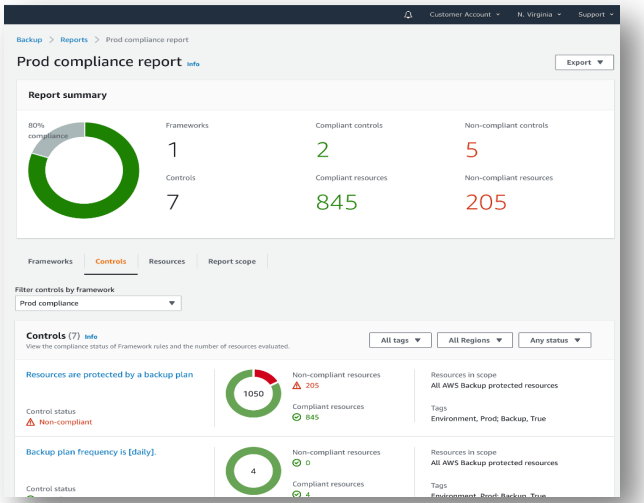
5. Data Protection

Maintains data security through classification, encryption, access controls, and availability.

Data Protection on AWS

AWS Blueprint for Ransomware Defense:
https://d1.awsstatic.com/whitepapers/compliance/AWS-Blueprint-for-Ransomware-Defense.pdf





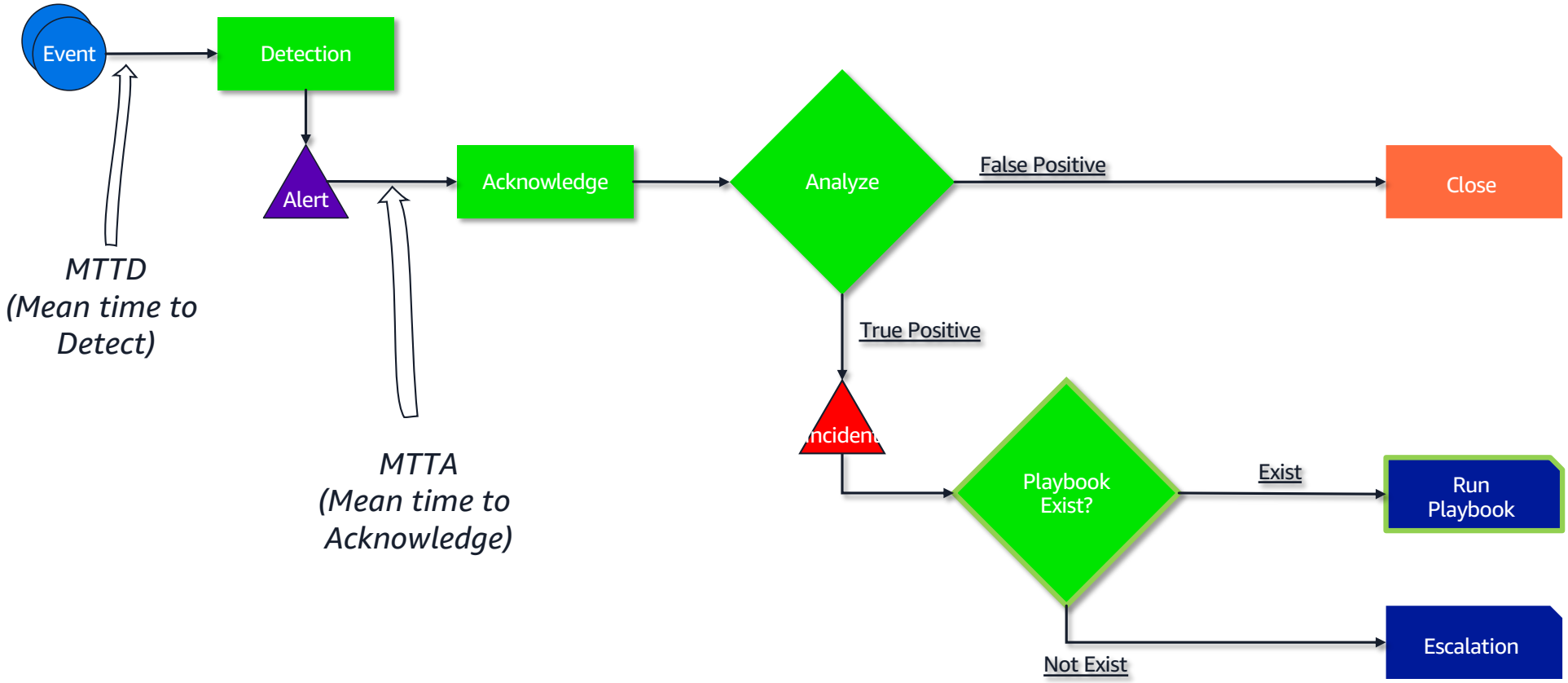
AWS Backup Report

**Immutable, meaning the data within a backup cannot be altered or deleted once created.*

9. Incident Response

Reduce potential harm by effectively responding to security incidents.

Detection Workflow



Example Playbook: Compromised AWS Credentials

Incident Type	**Compromised AWS Account Credentials**
Runbook Status	Approved
Playbook Link	[Link]
Last Modified Date	20 February 2025
Responders	[name]
Incident Source	GuaradDuty Finding URL / Email Notification
Status	Triage / Containment / Resolved / False Positive

Execution

No	Action	Time	Evidence	Responder
Triage				
1	Navigate to the GuardDuty console and open the **Findings** page. You should see a finding that starts with "**UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom**". If you do not see one, try refreshing the page.	14:17	*screenshot*	*Resa*
2	Select a finding with type "UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom" by clicking the row for that finding. This finding informs you that an API operation (for example, an attempt to launch an EC2 instance, create a new IAM user, modify AWS privileges) was invoked from an IP address that is included on a threat list that you uploaded. A threat list consists of known malicious IP addresses. This can indicate unauthorized access to AWS resources within your environment. As part of a risk driven detection strategy, your organization prioritizes AWS IAM related security alerts.		Filename_1.jpg	
3	You can see that the access key referenced in this finding is from an IAM assumed role, which means the Access Key credentials used to invoke these API calls belong to an IAM Role assumed by			

	will open a shell (a session with that instance).			

22	Run the following two commands and compare the access key ID to the one you copied down earlier to ensure it has changed. Make sure you replace the word "**ROLE**" at the end of the second command below with the "User name" or IAM role that you noted in step
	
	`1. TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/`
	`2. curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/ROLE`			

23	Compare the **AccessKeyId** in the response to the Access key ID you noted earlier to confirm the successful credential rotation (they should be different).			
Eradication: Identify affected resources				
1	Go to CloudTrail console. Click on "Event history". In the filter dropdown, select "AWS access key". Enter your compromised access key ID. Set the appropriate time range. Look for resource creation events (CreateInstance, CreateBucket, etc.)			
2	Document all resources created or modified.			
3	Navigate to AWS Config console. Go to "Resources" view. Use the search filter to find resources. Look at the resource timeline. Check configuration changes.			
4	Note resources modified by the key			

Security Maturity Initial Phase - Outcome

Access to AWS environment is based on Least Privilege Access.

- KPI example: 100% user using MFA

Configuration on AWS complies with Security Framework.

- KPI example: 95% compliant to NIST Framework

Threats against AWS environment are quickly resolved.

- KPI example: Average resolution time is 1 hour

Public application endpoint is protected.

- KPI example: 100% WAF coverage

Data in AWS environment is actively backed up.

- KPI example: 100% backup coverage

Thank you