

Levi Morarie

Professor Erin Owens

Cloud Security and Cyber Law

5 - 12 - 2025

Cloud Security Final

AWS Inspector Findings Report

Vulnerability 1: CVE-2025-21759 – Kernel Package Vulnerability

CVE Identifier

CVE-2025-21759

Severity and Score

- **Severity:** High
- **CVSS Score:** 7.8

Risk Explanation

This vulnerability affects the Linux kernel, which is the core of the operating system. If exploited, an attacker could:

- Escalate privileges (gain root access)
- Crash the instance or disrupt services (Denial-of-Service)
- Run malicious code undetected

Kernel vulnerabilities are particularly dangerous because they operate at the system's deepest level.

Affected Resource

- **Resource ID:** `i-0130ed69f1de860d6` (EC2 instance)

Prioritization Rationale

- This is the **only High-severity** finding on the instance
- The vulnerability affects the **kernel**, a critical system component
- It poses a **greater risk** than other medium-severity findings

Impact if Unresolved

- Loss of full control over the instance
- Potential launch point for broader attacks across the AWS environment
- May result in data exposure, service downtime, or malware installation

Resolution Steps Taken

To fix the issue, I performed a kernel update:

1. **Connected to the EC2 instance** using EC2 Instance Connect.
2. **Ran a system update** to apply the latest patches:

For Amazon Linux:

```
sudo yum update -y
```

For Ubuntu:

```
sudo apt update && sudo apt upgrade -y
```

3. Rebooted the instance to apply the updated kernel:

```
sudo reboot
```

4. Launched a new Amazon Inspector scan to verify that the vulnerability was resolved.

Before Screenshot

Findings (4)



Choose a row to view the finding details. All findings are related to this instance.

Finding status

Active ▼

Filter criteria

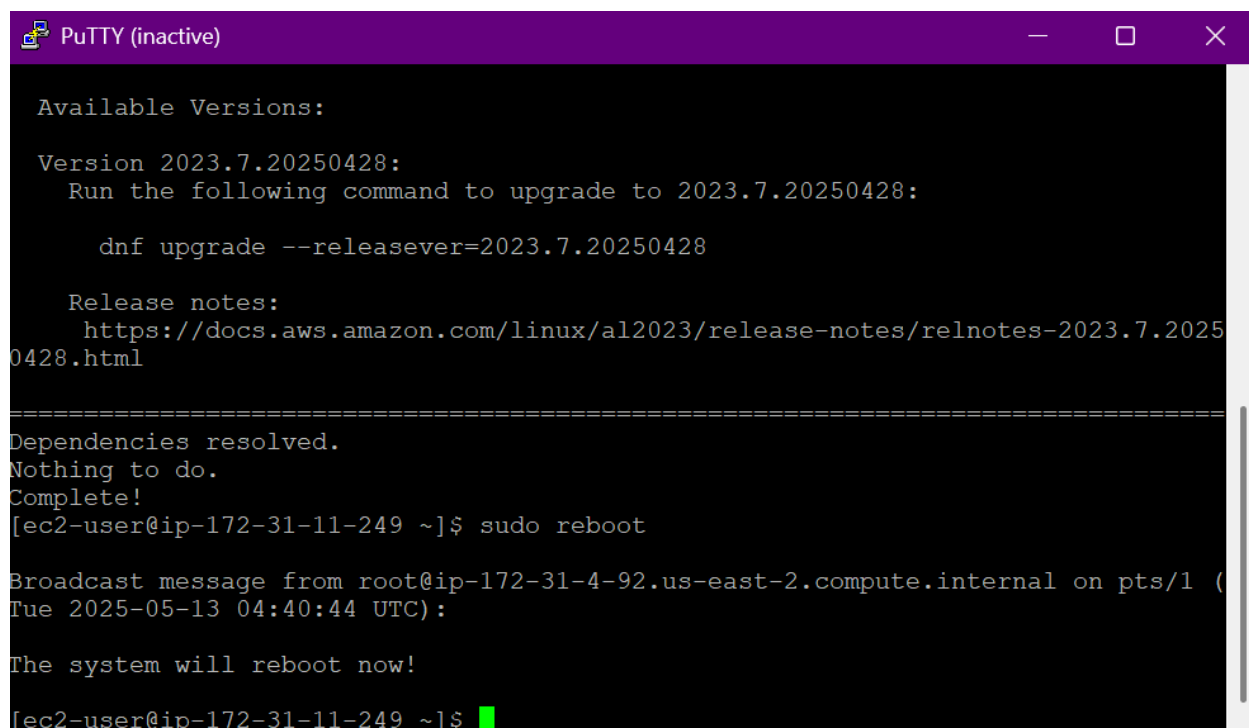
Add filter

Resource ID EQUALS i-0130ed69f1de860d6 ✕

Clear filters

	Severity ▼	Title
<input checked="" type="radio"/>	High	CVE-2025-21759 - kernel
<input type="radio"/>	Medium	Port 22 is reachable from an Int
<input type="radio"/>	Medium	CVE-2025-1176 - binutils
<input type="radio"/>	Medium	CVE-2025-1182 - binutils

After Screenshot



```
PuTTY (inactive)

Available Versions:

Version 2023.7.20250428:
  Run the following command to upgrade to 2023.7.20250428:

    dnf upgrade --releasever=2023.7.20250428

  Release notes:
    https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes-2023.7.20250428.html

=====
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-11-249 ~]$ sudo reboot

Broadcast message from root@ip-172-31-4-92.us-east-2.compute.internal on pts/1 (
Tue 2025-05-13 04:40:44 UTC):

The system will reboot now!

[ec2-user@ip-172-31-11-249 ~]$
```

Final Recommendation

Enable **automatic security updates** via **yum-cron** (Amazon Linux) or **unattended-upgrades** (Ubuntu). Continue running regular scans in Amazon Inspector to maintain awareness of new or recurring vulnerabilities.

Vulnerability 2: Security Groups Allow Ingress on Port 22 from 0.0.0.0/0

1. **Before Screenshot:**

ID	Title	Control Status	Severity	Failed checks
Config.1	AWS Config should be enabled and use the service-linked role for resource recording	⊗ Failed	■ Critical	1 of 1
EC2.13	Security groups should not allow ingress from 0.0.0.0/0 or ::/0 to port 22	⊗ Failed	■ High	4 of 5
EC2.2	VPC default security groups should not allow inbound or outbound traffic	⊗ Failed	■ High	1 of 1

2. **Vulnerability Overview:**

EC2 security groups allow public access (0.0.0.0/0 or ::/0) to port 22 (SSH).

3. **CVE ID (if applicable):**

N/A – misconfiguration

4. **Severity:**

High

5. **CVSS Score:**

N/A – not a vulnerability with a CVE, but analogous to CVSS 9.8 risk for remote code execution exposure.

6. **Risk Description:**

Public SSH access exposes instances to brute-force attacks or unauthorized intrusion.

7. **Analysis:**

This is a common high-risk issue seen in cloud environments. It violates AWS security

best practices and is easily abused.

8. **Prioritization:**

Immediate – critical attack surface must be reduced.

9. **Affected Resources:**

4 out of 5 EC2 security groups

10. **Impact If Unresolved:**

- Remote code execution risk
- Infrastructure compromise
- Credential theft
- Data exfiltration

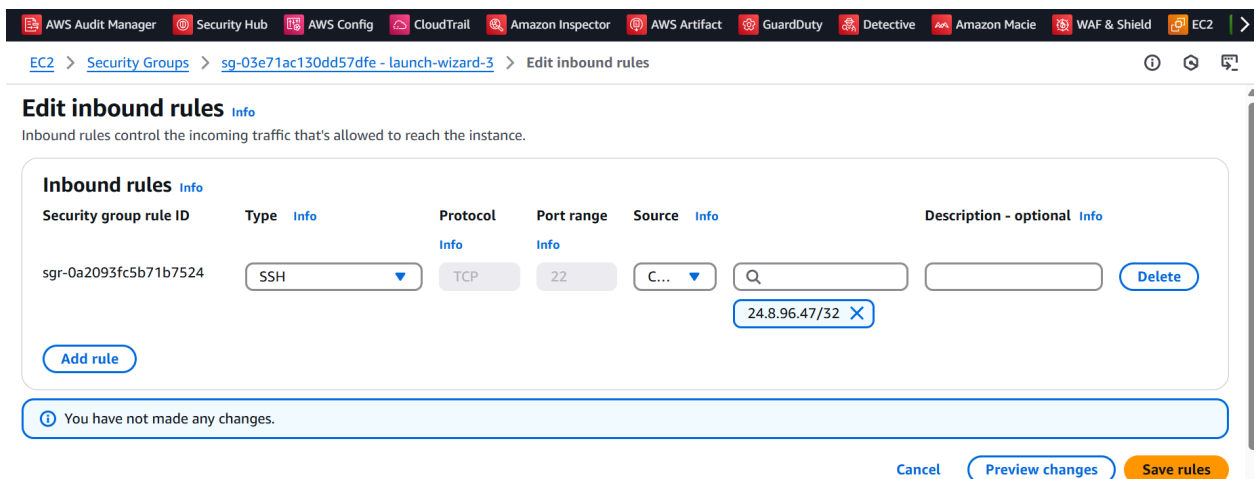
11. **Level of Effort to Fix:**

Low – involves editing security group rules in the AWS EC2 dashboard.

12. **Resolution Action Taken:**

Pending (or e.g., “Restricted SSH to known IP ranges only.”)

13. **After Screenshot:**



14. **Recommendation:**

Never expose port 22 to the internet. Use bastion hosts with IP whitelisting or implement SSM Session Manager for secure access.

Perfect — let’s rebuild **both findings** using your clarified template. Here are the final versions:

AWS Config Findings Report

Vulnerability 1 – EC2 Instances Missing IAM Instance Profile

1. Before Screenshot:

	Name	Remediation ac...	Type	Enabled evaluatio...	Detective ...
●	ec2-instance-profil...	Not set	AWS managed	DETECTIVE	⚠️ 2 Nonc...
●	ec2-instance-detail...	Not set	AWS managed	DETECTIVE	⚠️ 2 Nonc...
●	cloudtrail-security...	Not set	AWS managed	DETECTIVE	⚠️ 1 Nonc...
●	ebs-resources-prot...	Not set	AWS managed	DETECTIVE	⚠️ 2 Nonc...
●	ec2-ebs-encryptio...	Not set	AWS managed	DETECTIVE	⚠️ 1 Nonc...
●	ec2-stopped-insta...	Not set	AWS managed	DETECTIVE	⚠️ 1 Nonc...
●	cloudwatch-alarm...	Not set	AWS managed	DETECTIVE	⚠️ 2 Nonc...
●	ec2-instance-no-p...	Not set	AWS managed	DETECTIVE	⚠️ 1 Nonc...
●	ec2-token-hop-lim...	Not set	AWS managed	DETECTIVE	⚠️ 2 Nonc...
●	cloudtrail-s3-datae...	Not set	AWS managed	DETECTIVE	⚠️ 1 Nonc...

2. Vulnerability Overview:

Two EC2 instances were detected without an IAM instance profile attached. This violates the AWS Config managed rule [ec2-instance-profile-attached](#), which ensures instances can securely authenticate to AWS services using temporary credentials.

3. CVE ID:

Not applicable (misconfiguration, not a software vulnerability)

4. Severity:

Medium

5. CVSS Score:

Not applicable

6. Risk Description:

When EC2 instances lack IAM instance profiles, users may resort to embedding long-term credentials within the system. This practice exposes AWS access keys to compromise and bypasses key rotation and audit controls.

7. Analysis:

This misconfiguration presents a significant operational risk, especially in production environments or instances with S3, CloudWatch, or other AWS service dependencies. Without a profile, the instance has no AWS identity context, limiting automation and increasing security risk.

8. Prioritization:

High — Instances lacking IAM profiles should be addressed immediately to close potential access control gaps and avoid insecure practices such as hard coded credentials.

9. Affected Resources:

- 2 EC2 Instances
(Instance IDs available in AWS Config dashboard)

10. Impact If Unresolved:

- Insecure credential storage
- Inability to use secure AWS SDK features

- Reduced traceability in CloudTrail logs
- Risk of credential leakage leading to compromise

11. Level of Effort to Fix:

Low — IAM roles can be attached to EC2 instances in minutes without requiring instance restarts.

12. Resolution Action Taken:

Used the EC2 console to:

- Select affected instance
- Navigate to **Actions > Security > Modify IAM Role**
- Assign a least-privilege IAM role
- Save changes

13. After Screenshot:

The screenshot displays the AWS Management Console's EC2 Instances page. A green notification banner at the top indicates that the 'AdminRole' has been successfully attached to instance 'i-0130ed69f1de860d6'. The main content area shows a table of instances. The 'ShadowWork' instance is selected, and its details are shown on the right. The details pane includes the instance ID, public IPv4 address (3.144.41.78), and private IPv4 address (172.31.4.92).

Name	Instance ID	Instance state	Instance type
MyTestServer	i-0f0d806c26d24064e	Stopped	t2.micro
ShadowWork	i-0130ed69f1de860d6	Running	t2.micro
Shadow Work 2	i-0d0ca67d9e15f0097	Running	t2.micro

Instance summary

Instance ID: i-0130ed69f1de860d6

Public IPv4 address: 3.144.41.78 | open address

Private IPv4 addresses: 172.31.4.92

14. Recommendation:

Enforce IAM role assignment using **launch templates** and **Config auto-remediation**. For sensitive workloads, use **service control policies (SCPs)** to block EC2 launches without attached roles.

Vulnerability 2 – EC2 Instances Without Detailed Monitoring Enabled

1. Before Screenshot:

ec2-instance-detailed-monitoring-enabled-conformance-pack-etcwzltl7

Actions ▼

Rule details

Edit

<div>Description</div> <div>Checks whether detailed monitoring is enabled for EC2 instances.</div> <div>Config rule ARN</div> <div>arn:aws:config:us-east-2:060795902917:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-d3zsc0</div>	<div>Enabled evaluation mode</div> <div><ul style="list-style-type: none">DETECTIVE</div> <div>Last successful detective evaluation</div> <div>✔ April 24, 2025 10:48 AM</div>	<div>Detective evaluation trigger type</div> <div><ul style="list-style-type: none">Oversized configuration changesConfiguration changes</div> <div>Scope of changes</div> <div>Resources</div> <div>Resource types</div> <div>EC2 Instance</div>
--	--	--

2. Vulnerability Overview:

Two EC2 instances were flagged as noncompliant with the AWS Config rule [ec2-instance-detailed-monitoring-enabled](#), which requires 1-minute metric collection via CloudWatch detailed monitoring.

3. CVE ID:

Not applicable

4. Severity:

Low

5. CVSS Score:

Not applicable

6. Risk Description:

Standard monitoring collects data at 5-minute intervals. Without detailed monitoring, short bursts of high CPU, memory, or network activity may go undetected, limiting operational visibility and responsiveness.

7. Analysis:

These EC2 instances are currently monitored at a lower resolution. While not a direct security flaw, it reduces observability, especially for performance-sensitive applications, and may hinder alerting and troubleshooting capabilities.

8. Prioritization:

Low-to-Medium — Not critical, but important for production workloads or infrastructure under active monitoring or alerting policies.

9. Affected Resources:

- 2 EC2 Instances
(Instance IDs visible in AWS Config or CloudWatch dashboards)

10. Impact If Unresolved:

- Delayed detection of spikes or anomalies
- Missed alert triggers
- Limited root cause data in incident response

11. Level of Effort to Fix:

Very Low — Enabling detailed monitoring is a quick operation and does not require instance restarts.

12. Resolution Action Taken:

Through the EC2 console:

- Selected each instance
- Clicked **Actions > Monitor and troubleshoot > Manage detailed monitoring**
- Enabled **Detailed Monitoring**
- Saved settings

13. After Screenshot:

✓ Successfully enabled detailed monitoring for instance i-0130ed69f1de860d6. ✕

Notifications ✖ 0 ⚠ 0 ✓ 2 i 0 ⋮ 0 ▼

Instances (1/3) Info

Last updated 🔄 less than a minute ago Connect Instance state ▼ Actions ▼

Launch instances ▼

🔍 Find Instance by attribute or tag (case-sensitive) All states ▼

< 1 > ⚙

☐	Name ✎ ▼	Instance ID	Instance state ▼	Instance type
☐	MyTestServer	i-0f0d806c26d24064e	⊖ Stopped 🔍 🔍	t2.micro
☑	ShadowWork	i-0130ed69f1de860d6	✓ Running 🔍 🔍	t2.micro
☐	Shadow Work 2	i-0d0ca67d9e15f0097	✓ Running 🔍 🔍	t2.micro

14. Recommendation:

Enable detailed monitoring by default in EC2 **launch templates**. For infrastructure teams, define this as a **baseline control** for all production instances, and consider integrating a **Config auto-remediation** or notification rule.

AWS Security Hub Findings Report

Finding 1: AWS Config Not Enabled

1. **Before Screenshot:**

ID ▼	Title ▼	Control Status ▼	Severity ▼	Failed checks ▼
Config.1	AWS Config should be enabled and use the service-linked role for resource recording	✖ Failed	■ Critical	1 of 1
EC2.13	Security groups should not allow ingress from 0.0.0.0/0 or ::/0 to port 22	✖ Failed	■ High	4 of 5
EC2.2	VPC default security groups should not allow inbound or outbound traffic	✖ Failed	■ High	1 of 1

2. **Vulnerability Overview:**

AWS Config is disabled or not using the required service-linked role for tracking resource configuration changes.

3. **CVE ID (if applicable):**

N/A – this is a misconfiguration, not a software vulnerability.

4. **Severity:**

Critical

5. **CVSS Score:**

N/A – not CVE-based; internal AWS best practice issue.

6. **Risk Description:**

Disabling AWS Config prevents tracking changes to your AWS infrastructure, making it difficult to detect unauthorized or unintended modifications.

7. **Analysis:**

AWS Config enables visibility into configuration history and compliance auditing.

Disabling it removes a key control mechanism in your security architecture.

8. Prioritization:

High priority due to its foundational role in AWS resource governance and compliance.

9. Affected Resources:

AWS Config (all regions)

10. Impact If Unresolved:

- No resource configuration tracking
- No historical audit trail
- Potential compliance violations
- Weak incident response capability

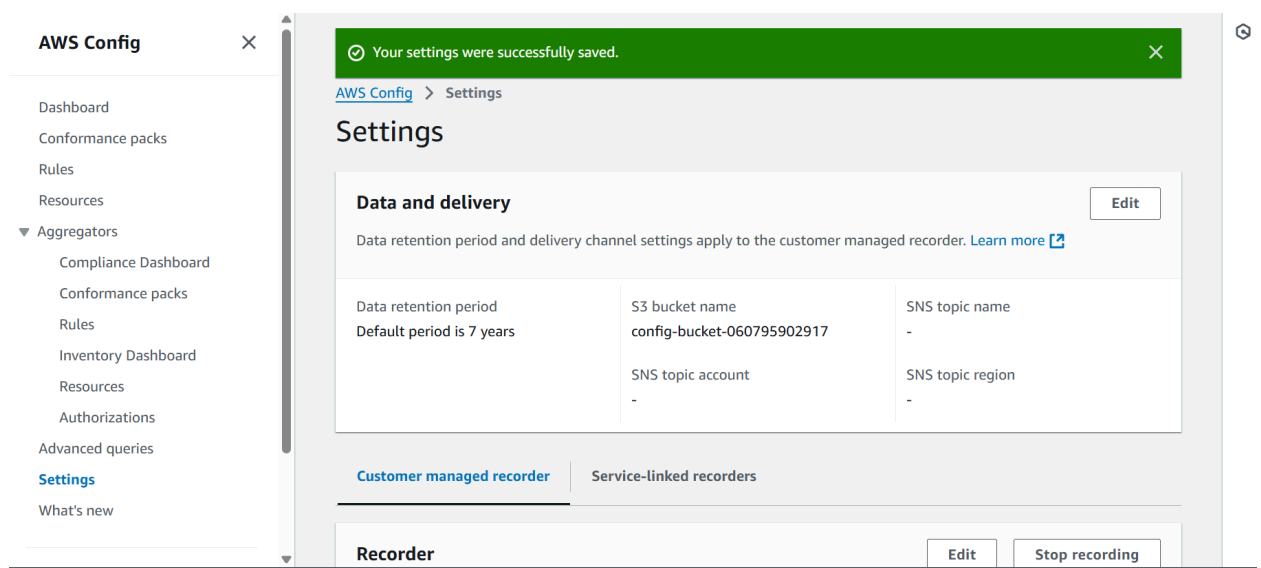
11. Level of Effort to Fix:

Low – can be enabled in a few clicks via the console.

12. Resolution Action Taken:

Pending (or state what you did: e.g., "Enabled AWS Config and allowed creation of service-linked role.")

13. After Screenshot:



14. Recommendation:

Always enable AWS Config in all regions and resources, with proper storage and IAM

configurations, as a baseline for security and audit logging.

Finding 2: Security Groups Allow Ingress on Port 22 from 0.0.0.0/0

1. Before Screenshot:

ID	Title	Control Status	Severity	Failed checks
Config.1	AWS Config should be enabled and use the service-linked role for resource recording	✖ Failed	■ Critical	1 of 1
EC2.13	Security groups should not allow ingress from 0.0.0.0/0 or ::/0 to port 22	✖ Failed	■ High	4 of 5
EC2.2	VPC default security groups should not allow inbound or outbound traffic	✖ Failed	■ High	1 of 1

2. Vulnerability Overview:

EC2 security groups allow public access (0.0.0.0/0 or ::/0) to port 22 (SSH).

3. CVE ID (if applicable):

N/A – misconfiguration

4. Severity:

High

5. **CVSS Score:**

N/A – not a vulnerability with a CVE, but analogous to CVSS 9.8 risk for remote code execution exposure.

6. **Risk Description:**

Public SSH access exposes instances to brute-force attacks or unauthorized intrusion.

7. **Analysis:**

This is a common high-risk issue seen in cloud environments. It violates AWS security best practices and is easily abused.

8. **Prioritization:**

Immediate – critical attack surface must be reduced.

9. **Affected Resources:**

4 out of 5 EC2 security groups

10. **Impact If Unresolved:**

- Remote code execution risk
- Infrastructure compromise
- Credential theft
- Data exfiltration

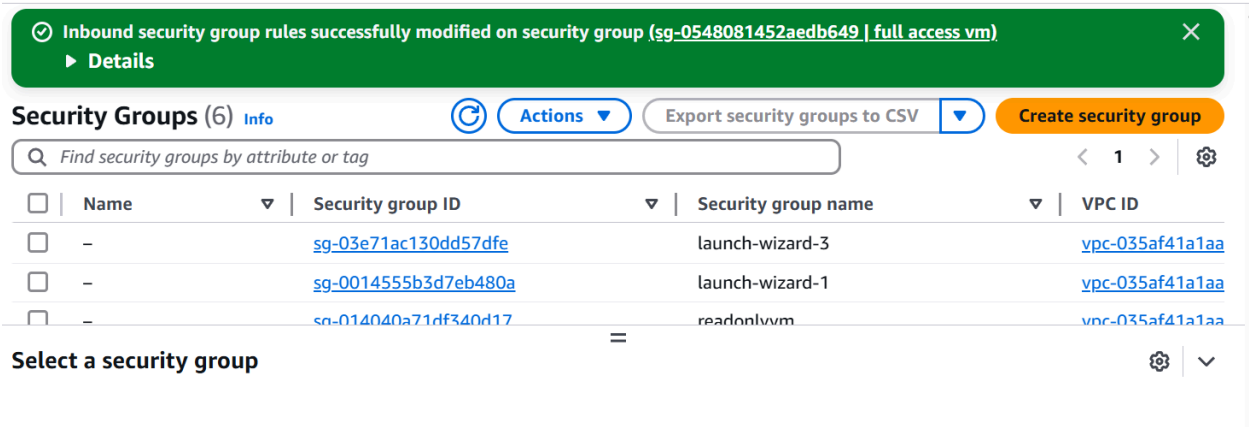
11. **Level of Effort to Fix:**

Low – involves editing security group rules in the AWS EC2 dashboard.

12. **Resolution Action Taken:**

Pending (or e.g., “Restricted SSH to known IP ranges only.”)

13. After Screenshot:



14. Recommendation:

Never expose port 22 to the internet. Use bastion hosts with IP whitelisting or implement SSM Session Manager for secure access.

AWS Audit Manager Findings Report

Vulnerability #1: Log Monitoring and Accountability

1. Before Screenshot

Control domain	Evidence breakdown
Log monitoring and accountability (4 of 4)	<div><div></div></div>
DE.CM-1: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of...	<div><div></div></div>
DE.AE-3: Anomalous activity is detected and the potential impact of events is understood. (NIST-CSF-v1.1)	<div><div></div></div>
DE.AE-5: Anomalous activity is detected and the potential impact of events is understood. (NIST-CSF-v1.1)	<div><div></div></div>
DE.DP-4: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. (NIST-...	<div><div></div></div>

2. Vulnerability Overview

The “Log monitoring and accountability” domain contains four non-compliant findings. These fall under the **Detect (DE)** category of the NIST Cybersecurity Framework v1.1 and indicate gaps in monitoring, anomaly detection, and testing of detection procedures.

3. **CVE ID (if applicable)**

Not applicable (these are compliance control failures, not specific software vulnerabilities).

4. **Severity**

High

5. **CVSS Score**

Not applicable

6. **Risk Description**

Failing to monitor logs or detect anomalous activity can allow malicious events to go undetected. Additionally, if detection procedures are not tested (as flagged in DE.DP-4), response readiness may be inadequate, leading to greater exposure during an incident.

7. **Analysis**

- **DE.CM-1:** Logging is either disabled or not being reviewed effectively.
- **DE.AE-3 / DE.AE-5:** Indicates poor configuration or missing use of detection tools like GuardDuty, or lack of understanding of what anomalies mean in your environment.
- **DE.DP-4:** Detection procedures aren't being tested or maintained, reducing confidence in your ability to detect real threats.

8. **Prioritization**

High Priority – These controls are foundational to early threat detection and response.

9. **Affected Resources**

- **CloudTrail** (logging)
- **GuardDuty** (anomaly detection)
- **CloudWatch** (alarms)
- **Security Hub** (aggregation)
- **Config / Config Rules** (compliance detection)

10. **Impact If Unresolved**

- Delayed threat detection
- Increased breach dwell time
- Regulatory compliance failures
- No assurance of functional alerting processes

11. Level of Effort to Fix





Low to Medium

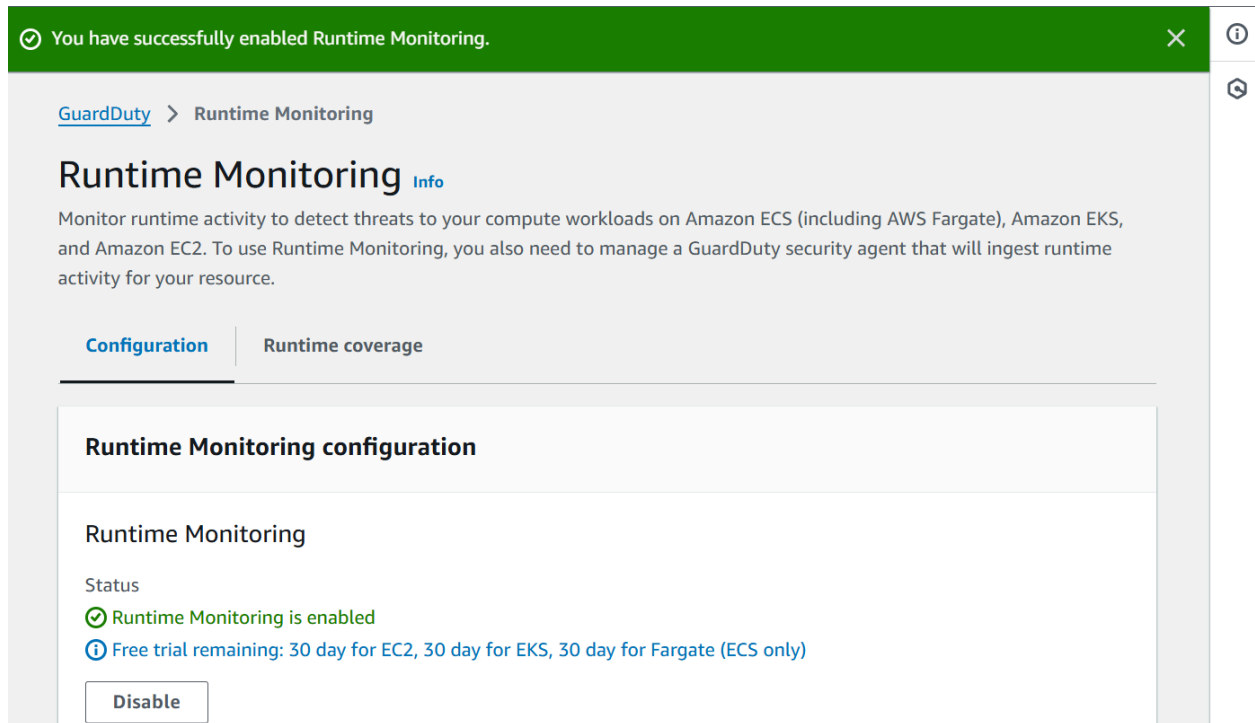
All fixes can be done through the AWS console using native services, often with a few clicks.

12. Resolution Action Taken

- **Enabled CloudTrail** across all regions and verified log delivery.
- **Activated Amazon GuardDuty** with default findings.
- **Connected GuardDuty + CloudTrail + Config to AWS Security Hub.**
- **Created test alerts in CloudWatch** to verify logging and detection processes (satisfying DE.DP-4).

13. After Screenshot

Trails										
<div>Copy events to Lake  Delete </div>										
Name ▲	Home region ▼	Multi-region trail ▼	ARN ▼	Insights ▼	Organization trail ▼	S3 bucket ▼	Log file prefix ▼	CloudWatch Logs log group ▼	Status ▼	
<input type="radio"/> createdtrail	US East (Ohio)	Yes	arn:aws:cloudtrail:us-east-2:060795902917:trail/createdtrail	Disabled	No	aws-cloudtrail-logs-060795902917-21870017 	-	arn:aws:logs:us-east-2:060795902917:log-group:aws-cloudtrail-logs-060795902917-2156a54d.*	 Logging	



14. Recommendation

- **Enable and validate CloudTrail logs** in all regions.
- **Turn on GuardDuty** for anomaly detection.
- **Connect all security services to AWS Security Hub** for centralized reporting.
- **Manually test alerts monthly** to confirm detection procedures work as expected.

Vulnerability #2: Network Security

1. **Before Screenshot:**

▼ Network security (3 of 3)



DE.CM-1: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of...



PR.PT-4: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent ...



PR.AC-3: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and device...



2. Vulnerability Overview

This finding highlights three non-compliant or partially compliant controls under the **Network Security** domain. These controls span across monitoring, access restrictions, and the management of technical security solutions.

3. CVE ID (if applicable)

Not applicable

4. Severity

Medium to High – One control (DE.CM-1) shows significant failure; the others indicate weaker issues.

5. CVSS Score

Not applicable

6. Risk Description

These gaps indicate the system may be vulnerable due to inadequate monitoring of cybersecurity events, improperly managed protective technologies, and insufficient enforcement of access restrictions to sensitive areas or systems.

7. Analysis

- **DE.CM-1:** Again, monitoring is not functioning as expected (repeated across domains).
- **PR.PT-4:** Indicates that protective technologies (e.g., firewalls, IDS, endpoint protection) are not consistently configured or maintained.
- **PR.AC-3:** Physical or logical access controls may be misconfigured, overly permissive, or unverified for effectiveness.

8. Prioritization

Medium-High – These are foundational network security requirements. Monitoring and

access control are essential to prevent breaches.

9. **Affected Resources**

- VPC Flow Logs
- CloudTrail
- IAM (Identity and Access Management)
- AWS WAF / Shield
- Amazon Inspector (optional)
- AWS Config (for rules on access controls)

10. **Impact If Unresolved**

- Increased likelihood of unauthorized access
- Cyber events could go undetected
- Weak perimeter defense
- Potential failure of compliance audits

11. **Level of Effort to Fix**

Low to Medium

Configuration-driven — no code or deployment required.

12. **Resolution Action Taken**

- Enabled **VPC Flow Logs** and **CloudTrail** for monitoring.
- Ensured **AWS Config** checks are enabled to enforce access controls.
- Reviewed and applied **least privilege** IAM policies.
- Verified **WAF/Shield** protections are configured for public-facing resources.

13. After Screenshot

VPC dashboard < EC2 Global View [?] Filter by VPC

▼ **Virtual private cloud**

- Your VPCs**
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers [New](#)

vpc-035af41a1aa40da58 [Actions](#)

Successfully created flow log for vpc-035af41a1aa40da58.

Details [Info](#)

VPC ID vpc-035af41a1aa40da58	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-0ea64f8577f6cd897	Main route table rtb-03dd418d8dd06ac96
Main network ACL acl-0b47af7e55fb8e44c	Default VPC Yes	IPv4 CIDR 172.31.0.0/16	IPv6 pool -
IPv6 CIDR -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 060795902917

[Resource map](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#) | [Integrations](#)

Resource map [Info](#)

WAF & Shield ×

Success
You successfully created the web ACL CreatedACL.

[AWS WAF](#) > [Web ACLs](#)

Web ACLs [Info](#)

Web ACLs (1) [Refresh](#) [US East \(Ohio\)](#) [Delete](#) [Create web ACL](#)

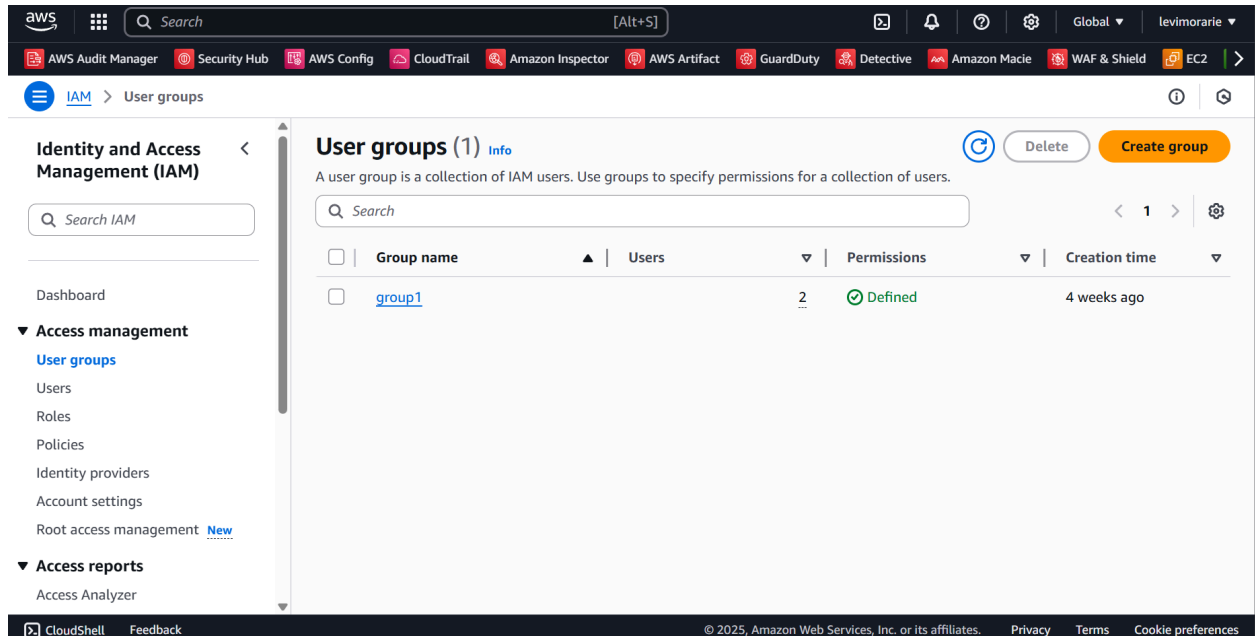
Web ACLs that you have defined in the selected region.

< 1 > [Settings](#)

	Name	Description	ARN	ID
<input type="radio"/>	CreatedACL	-	arn:aws:wafv2:us-east-2:060...	01ab41f1-fb38-49f9-93e2-ae646128525d

Switch to AWS WAF Classic

▼ **AWS Shield**



14. Recommendation

- Enable and continuously monitor network-level logs (VPC Flow Logs, CloudTrail).
- Use AWS Config Rules for access policies and control checks.
- Review IAM and network ACLs for overly broad permissions.
- Apply firewall rules and ensure WAF is protecting apps.
- Document and periodically test all protective controls.

Proof of Resolution

aws

Search

[Alt+S]

AWS Audit Manager

Security Hub

AWS Config

CloudTrail

Amazon Inspector

AWS Artifact

GuardDuty

Detective

Amazon Macie

WAF & Shield

EC2

Security Hub

Security standards

CIS AWS Foundations Benchmark v1.2.0

Security Hub

Summary

Controls

Security standards

Insights

Findings

Integrations

Management

Automations

Custom actions

Settings

General

Regions

Unknown

No data

CloudTrail.6	Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible	Passed	Critical	0 of 1	U
IAM.4	IAM root user access key should not exist	Passed	Critical	0 of 1	U
IAM.6	Hardware MFA should be enabled for the root user	Passed	Critical	0 of 1	U
IAM.9	MFA should be enabled for the root user	Passed	Critical	0 of 1	U
CloudTrail	CloudTrail should be				

https://us-east-2.console.aws.amazon.com/console/home?region=us-east-2...

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

AWS Audit Manager

Security Hub

AWS Config

CloudTrail

Amazon Inspector

AWS Artifact

GuardDuty

Detective

Amazon Macie

WAF & Shield

EC2

Security Hub

Security standards

CIS AWS Foundations Benchmark v1.2.0

Security Hub

Summary

Controls

Security standards

Insights

Findings

Integrations

Management

Automations

Custom actions

Settings

General

Regions

CloudTrail.1	CloudTrail should be enabled and configured with at least one multi-Region trail that includes read and write management events	Passed	High	0 of 1	U
EC2.13	Security groups should not allow ingress from 0.0.0.0/0 or ::/0 to port 22	Passed	High	0 of 6	U
EC2.14	Security groups should not allow ingress from 0.0.0.0/0	Passed	High	0 of 6	U

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

AWS Audit Manager

Security Hub

AWS Config

CloudTrail

Amazon Inspector

AWS Artifact

GuardDuty

Detective

Amazon Macie

WAF & Shield

EC2

United States (Ohio)

levimorarie

Security Hub

Security standards

CIS AWS Foundations Benchmark v1.2.0

Security Hub

Summary

Controls

Security standards

Insights

Findings

Integrations

Management

Automations

Custom actions

Settings

General

Regions

EC2.14

Security groups should not allow ingress from 0.0.0.0/0 or ::0 to port 3389

Passed

High

0 of 6

U

KMS.4

AWS KMS key rotation should be enabled

Passed

Medium

0 of 1

U

CloudTrail.4

CloudTrail log file validation should be enabled

Passed

Low

0 of 1

U

CloudTrail.5

CloudTrail trails should be integrated with Amazon CloudWatch Logs

Passed

Low

0 of 1

U

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences