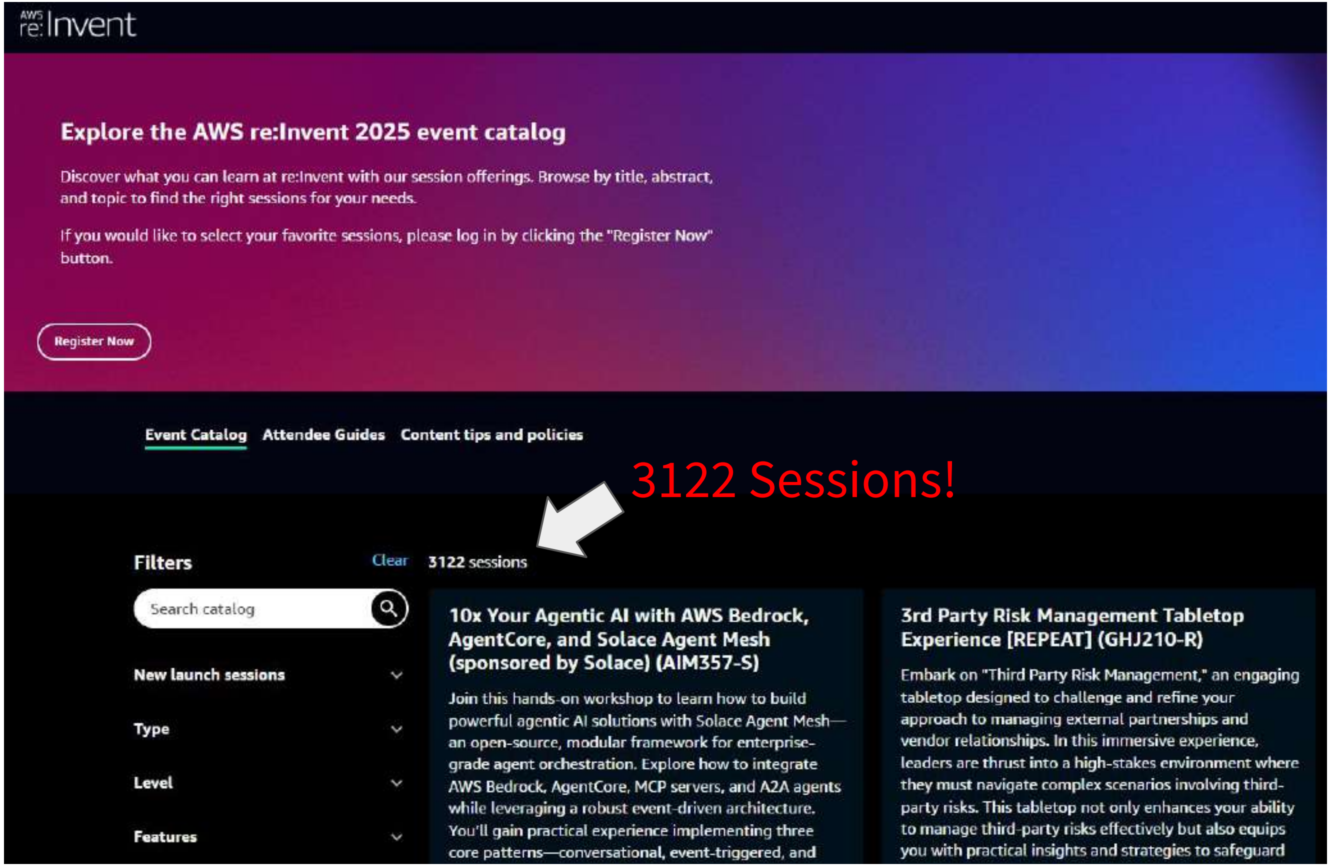
AWS re:Invent 2025 참관기 & recap

KRUG 보안 소모임

AWS re:Invent란?

AWS re:Invent는 Amazon Web Services(AWS)가 매년 개최하는 세계 최대 규모의 클라우드 컴퓨팅 컨퍼런스입니다. AWS의 최신 기술 발표, 키노트 강연, 수천 개의 세션, 엑스포, 네트워킹 기회가 제공됩니다.



Explore the AWS re:Invent 2025 event catalog

Discover what you can learn at re:Invent with our session offerings. Browse by title, abstract, and topic to find the right sessions for your needs.

If you would like to select your favorite sessions, please log in by clicking the "Register Now" button.

3122 Sessions!

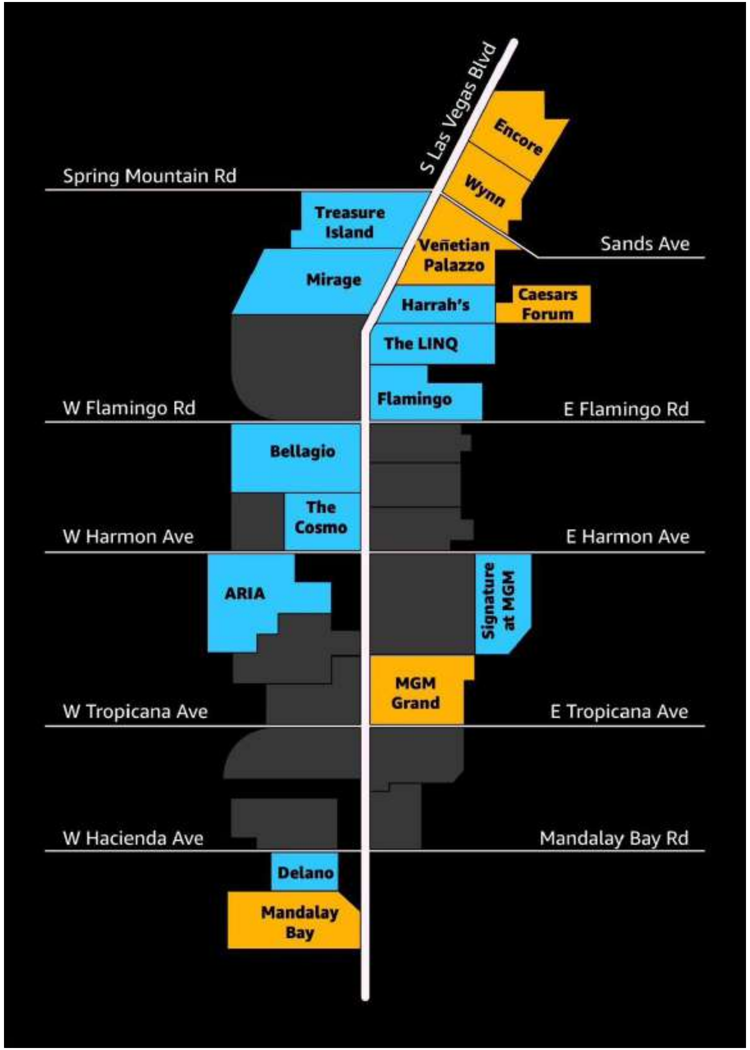
3122 sessions

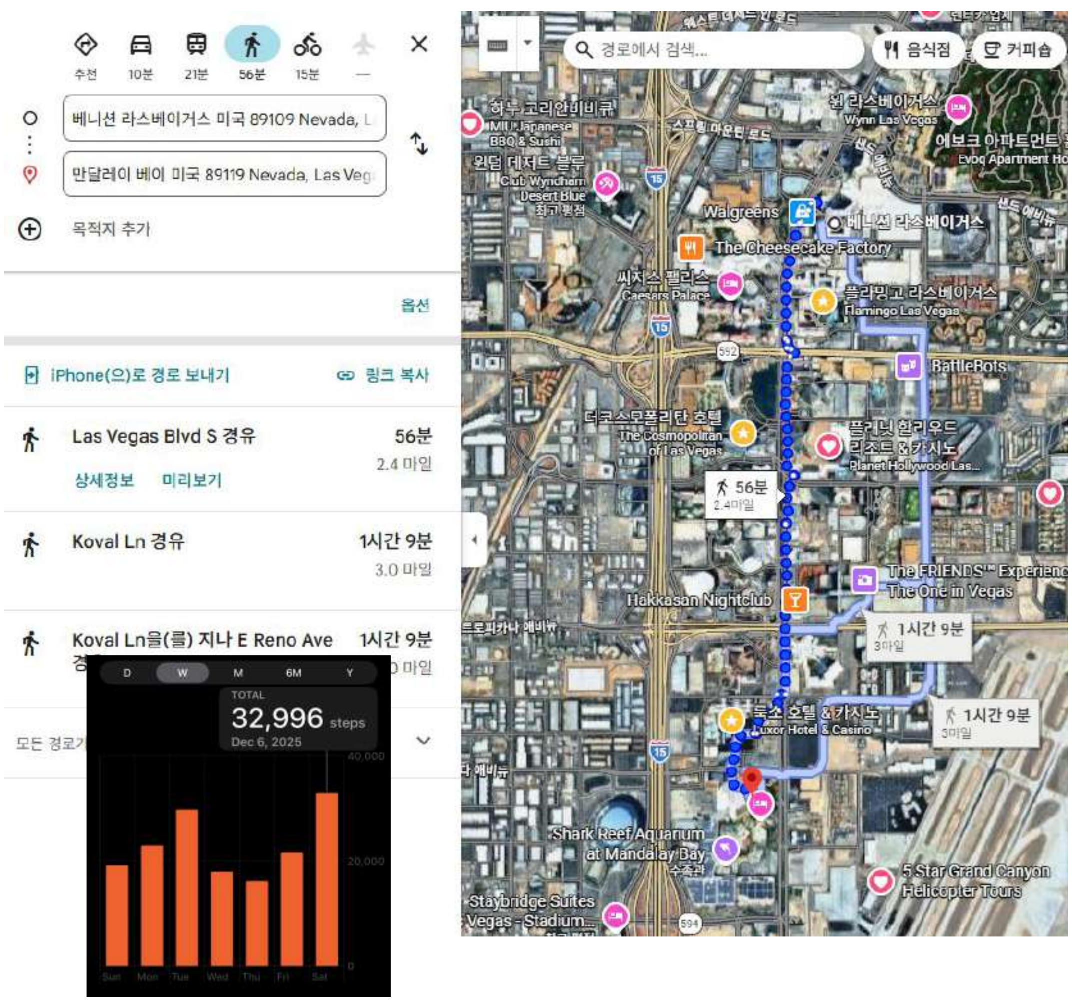
10x Your Agentic AI with AWS Bedrock, AgentCore, and Solace Agent Mesh (sponsored by Solace) (AIM357-S)

Join this hands-on workshop to learn how to build powerful agentic AI solutions with Solace Agent Mesh—an open-source, modular framework for enterprise-grade agent orchestration. Explore how to integrate AWS Bedrock, AgentCore, MCP servers, and A2A agents while leveraging a robust event-driven architecture. You'll gain practical experience implementing three core patterns—conversational, event-triggered, and

3rd Party Risk Management Tabletop Experience [REPEAT] (GHJ210-R)

Embark on "Third Party Risk Management," an engaging tabletop designed to challenge and refine your approach to managing external partnerships and vendor relationships. In this immersive experience, leaders are thrust into a high-stakes environment where they must navigate complex scenarios involving third-party risks. This tabletop not only enhances your ability to manage third-party risks effectively but also equips you with practical insights and strategies to safeguard





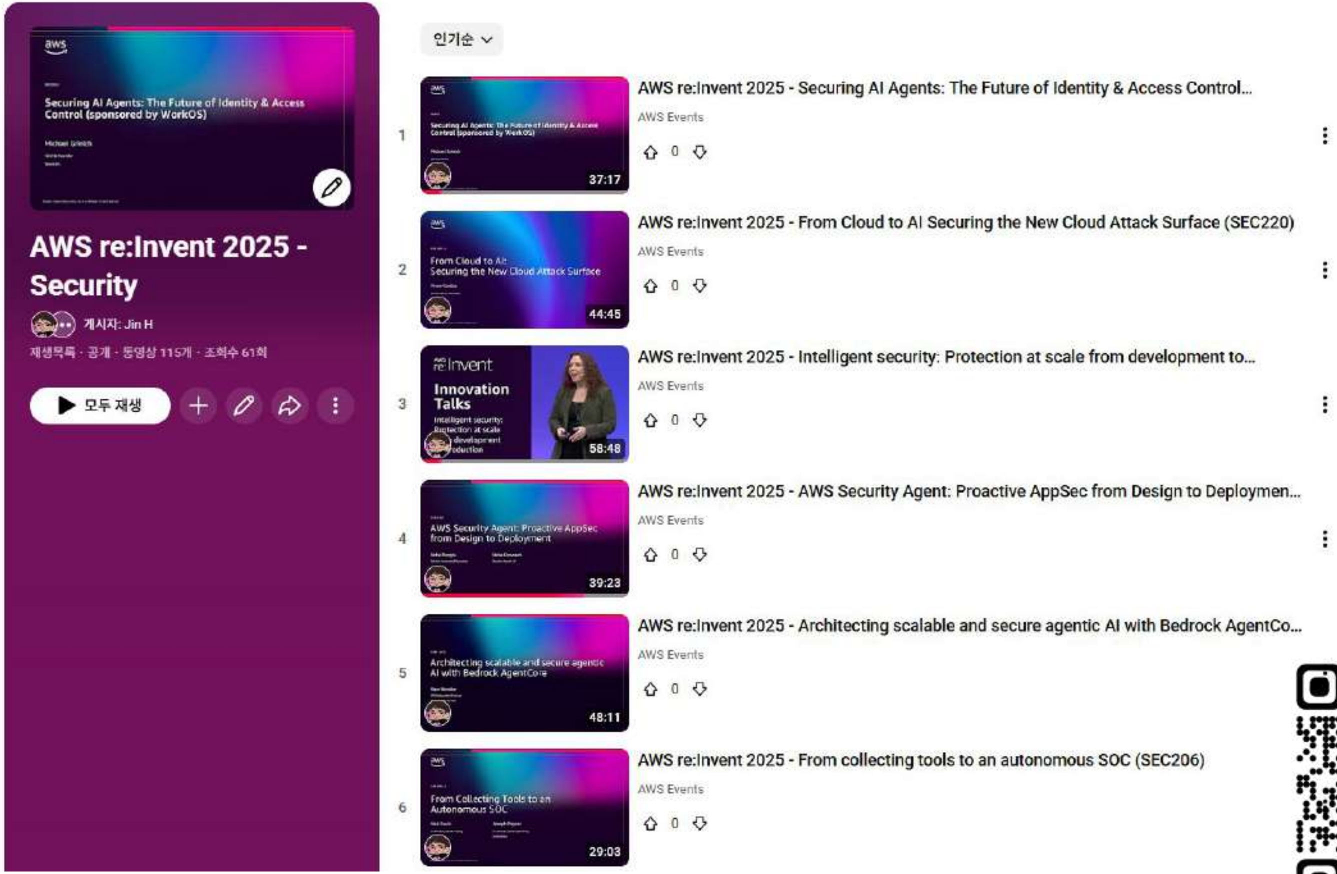
베니션 라스베이거스 미국 89109 Nevada, L

만달레이 베이 미국 89119 Nevada, Las Veg

Las Vegas Blvd S 경유 56분 2.4 마일

Koval Ln 경유 1시간 9분 3.0 마일

Koval Ln을(를) 지나 E Reno Ave 경 1시간 9분 마일



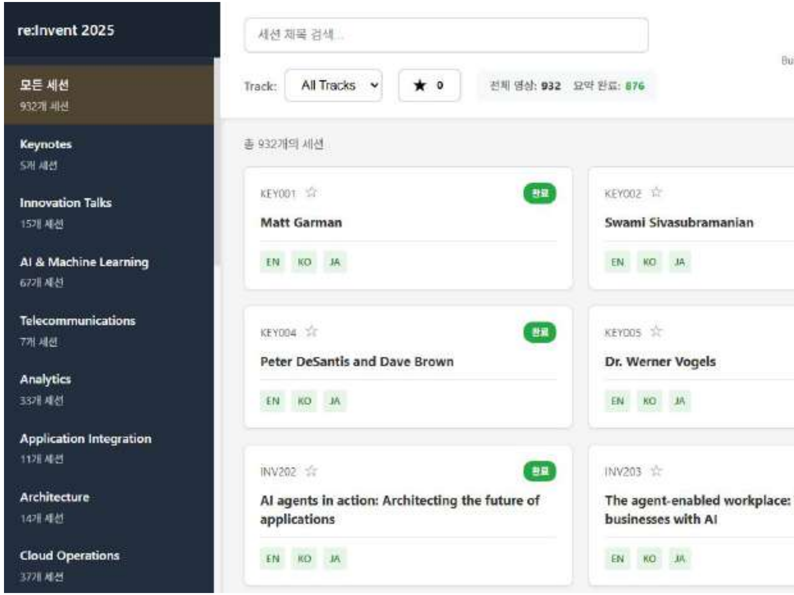
AWS re:Invent 2025 - Security

게시자: Jin H

재생목록 · 공개 · 동영상 115개 · 조회수 61회

1. AWS re:Invent 2025 - Securing AI Agents: The Future of Identity & Access Control...
   AWS Events
   0
2. AWS re:Invent 2025 - From Cloud to AI Securing the New Cloud Attack Surface (SEC220)
   AWS Events
   0
3. AWS re:Invent 2025 - Intelligent security: Protection at scale from development to...
   AWS Events
   0
4. AWS re:Invent 2025 - AWS Security Agent: Proactive AppSec from Design to Deploymen...
   AWS Events
   0
5. AWS re:Invent 2025 - Architecting scalable and secure agentic AI with Bedrock AgentCo...
   AWS Events
   0
6. AWS re:Invent 2025 - From collecting tools to an autonomous SOC (SEC206)
   AWS Events
   0

https://www.youtube.com/playlist?list=PLwyLgAhlAsi4SgLC61zj5qMBxsHkLC1J5


re:Invent 2025

세션 제목 검색...

Track: All Tracks ★ 0 전체 영상: **932** 요약 완료: **876**

Built with **Kiro**, **Strands Agents** & **Amazon Bedrock** **About** Language: 한국어

- **모든 세션** 932개 세션
- **Keynotes** 5개 세션
- **Innovation Talks** 15개 세션
- **AI & Machine Learning** 67개 세션
- **Telecommunications** 7개 세션
- **Analytics** 33개 세션
- **Application Integration** 11개 세션
- **Architecture** 14개 세션
- **Cloud Operations** 37개 세션

총 932개의 세션

KEY001 ☆ 완료
Matt Garman
EN KO JA

KEY002 ☆ 완료
Swami Sivasubramanian
EN KO JA

KEY003 ☆ 완료
Ruba Borno
EN KO JA

KEY004 ☆ 완료
Peter DeSantis and Dave Brown
EN KO JA

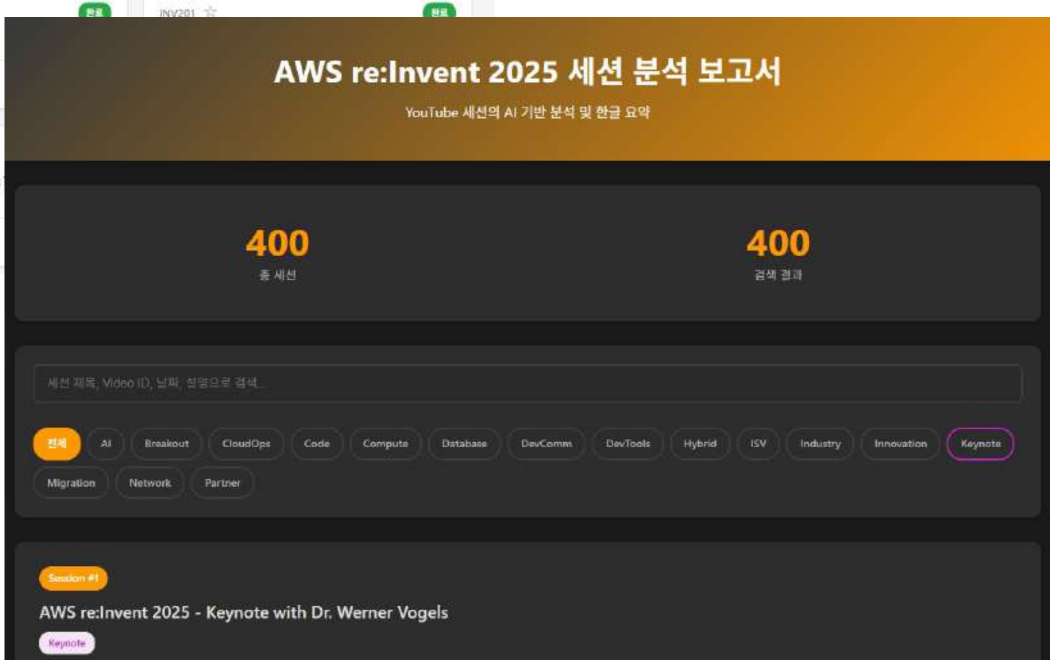
KEY005 ☆ 완료
Dr. Werner Vogels
EN KO JA

INV201 ☆ 완료

INV202 ☆ 완료
AI agents in action: Architecting the future of applications
EN KO JA

INV203 ☆
The agent-enabled workplace: businesses with AI
EN KO JA

https://reinvent2025.summary.events


AWS re:Invent 2025 세션 분석 보고서

YouTube 세션의 AI 기반 분석 및 한글 요약

400 총 세션

400 검색 결과

세션 제목, Video ID, 날짜, 설명으로 검색...

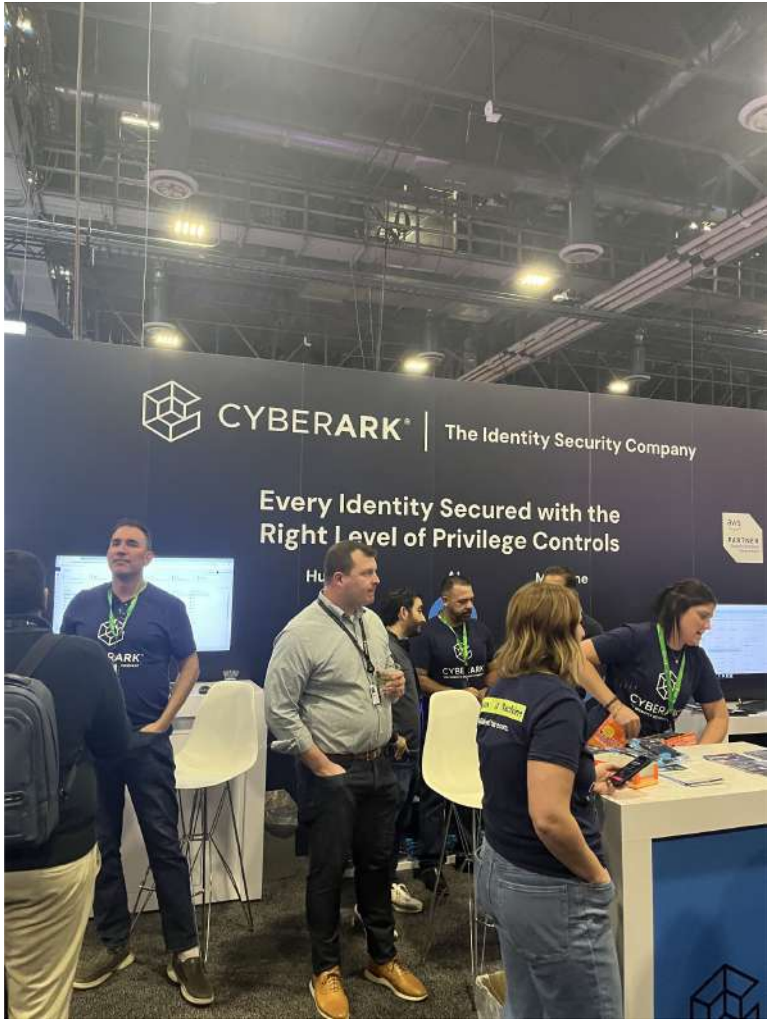
Session #1

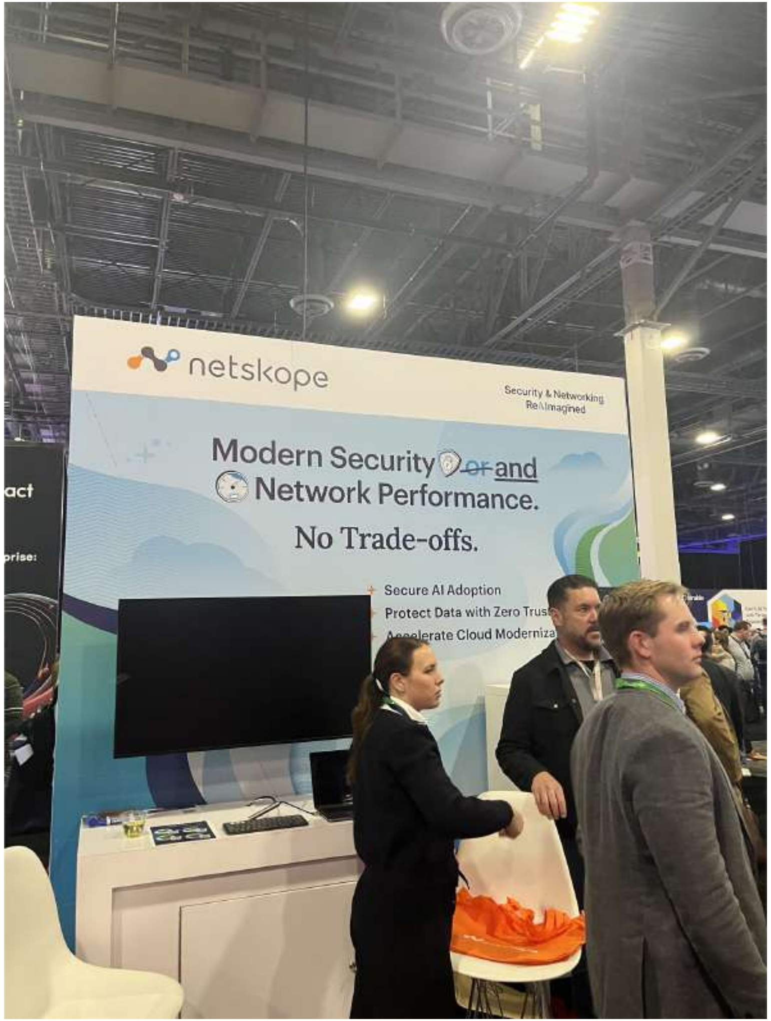
AWS re:Invent 2025 - Keynote with Dr. Werner Vogels

Keynote

https://djn5cn31a5nkh.cloudfront.net

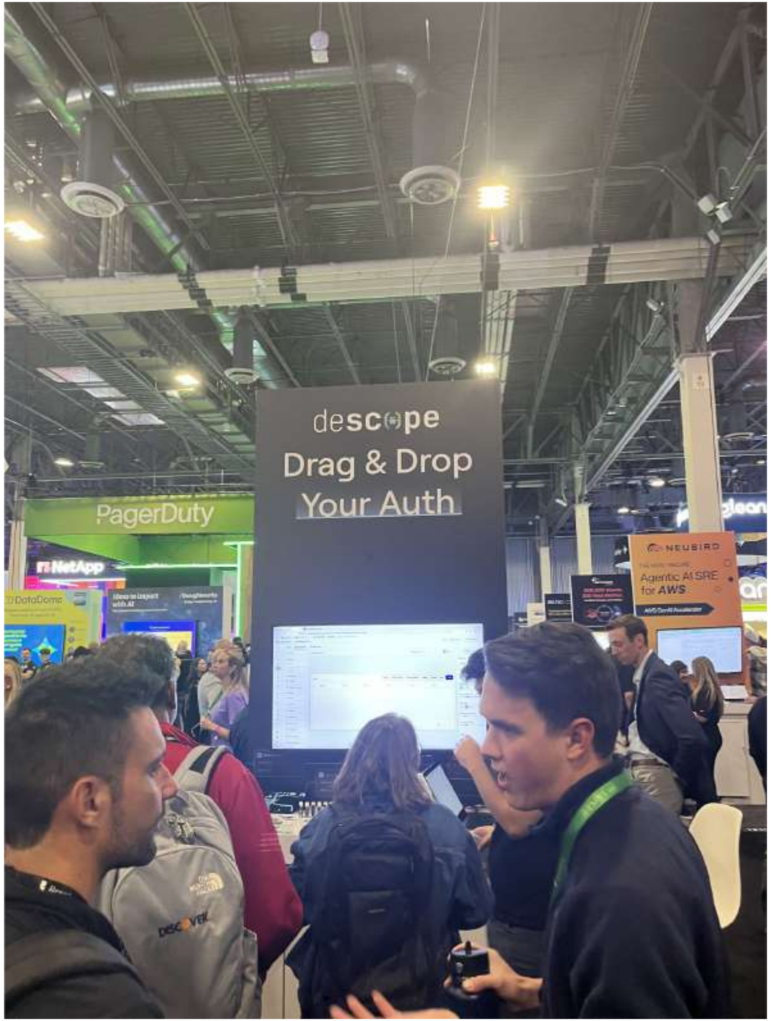
엑스포 (빠르게 넘어 갑니다. 트렌드만 보세요!)

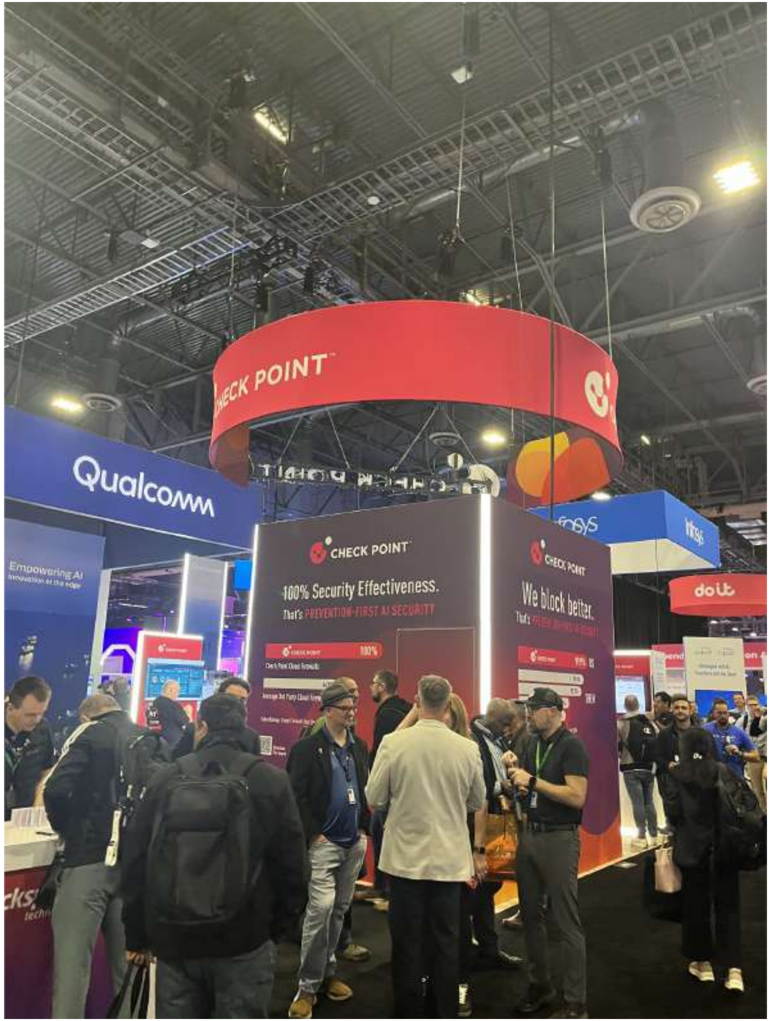

CYBERARK
The Identity Security Company
Every Identity Secured with the Right Level of Privilege Controls

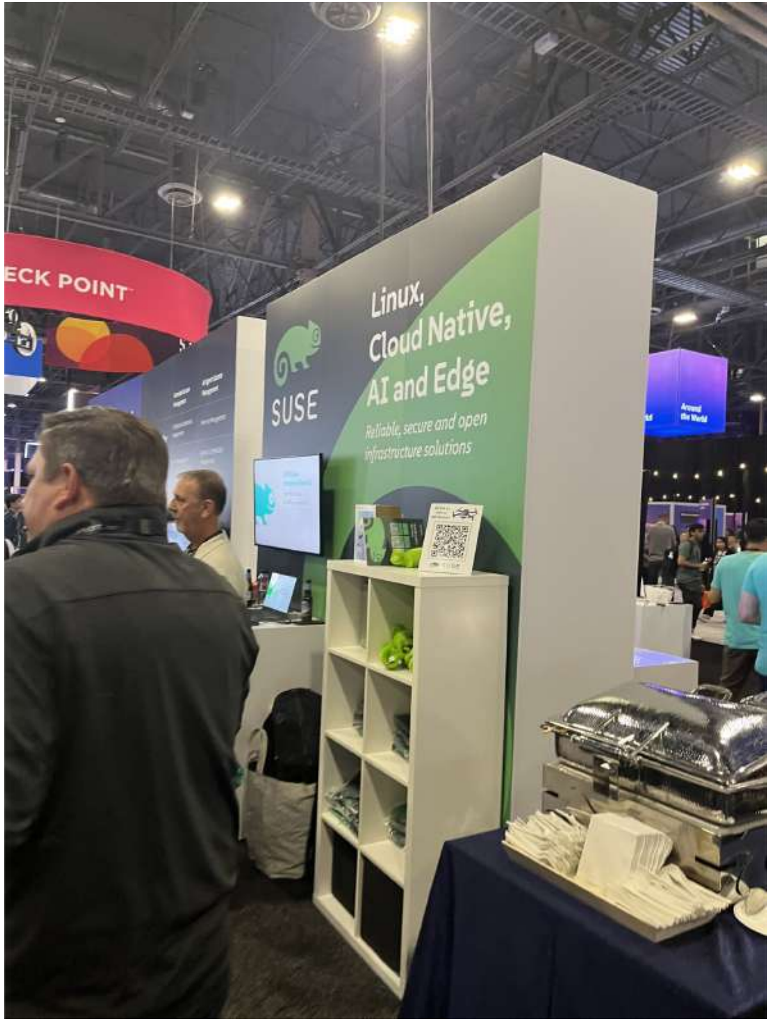

netskope
Security & Networking Re/Imagined
Modern Security ~~or~~ and Network Performance.
No Trade-offs.
Secure AI Adoption
Protect Data with Zero Trus
Accelerate Cloud Moderniza

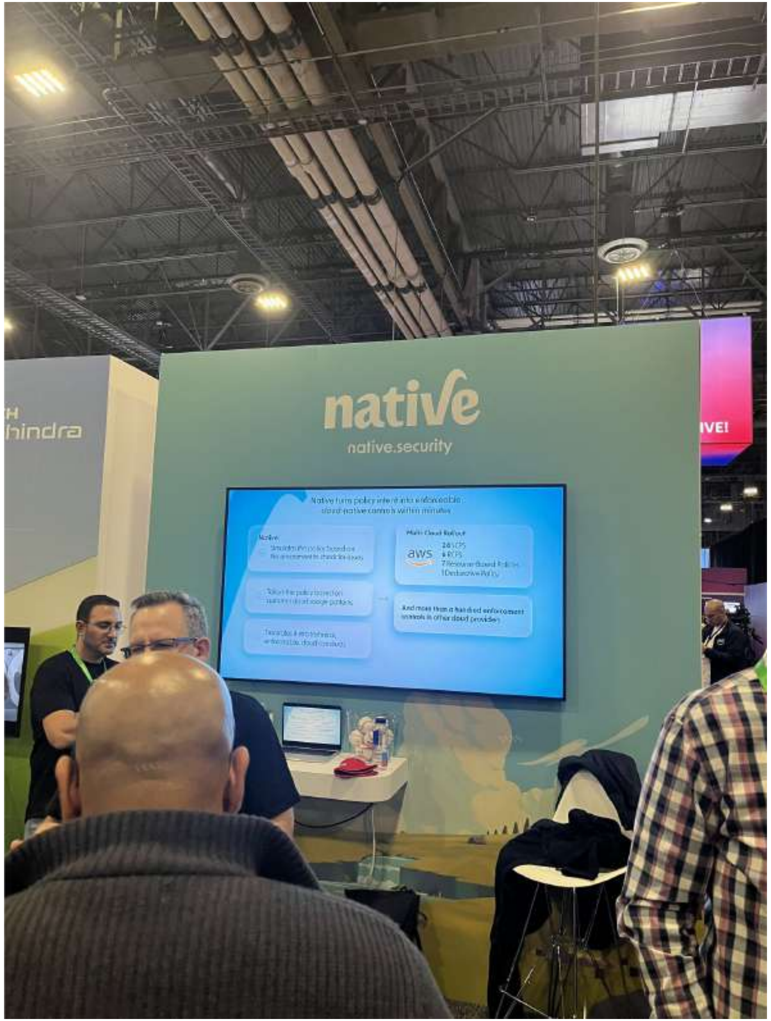
druva
Cyber Resilience, Simplified.
Get the ransomware monkey off your back.
Cyber Resilience Maturity Assessment
WIZ
Feeling so
contentful
RES

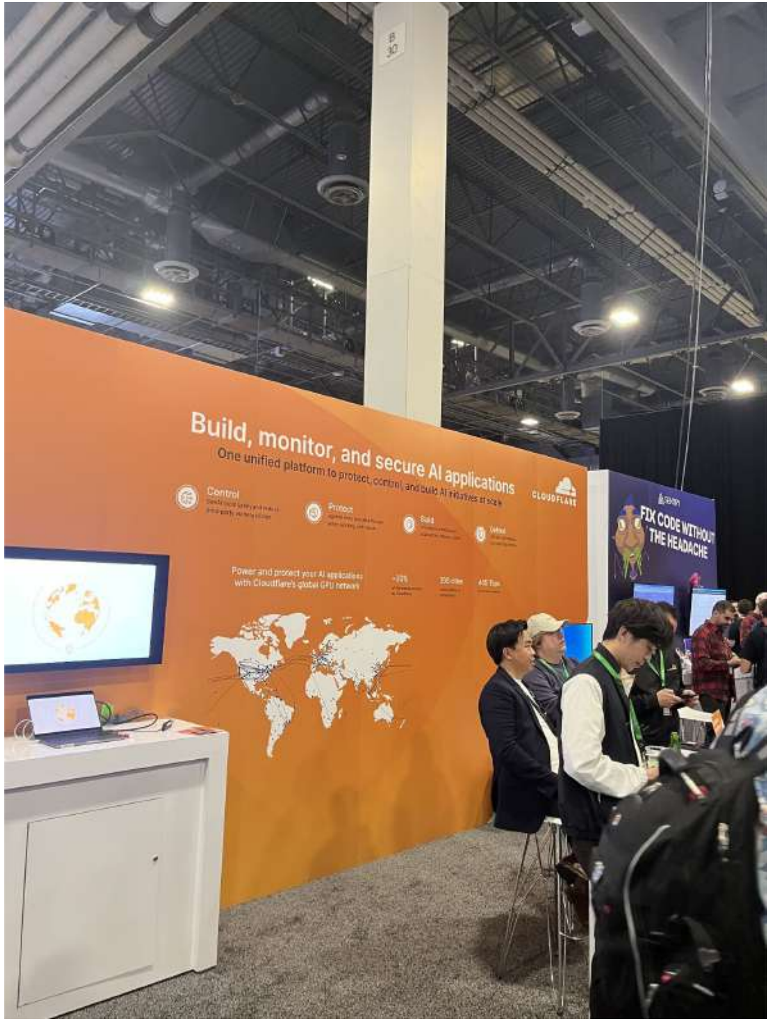
Cribl
CONTROL
Cribl
ACCELERATE
SIEM augmentation and migration to modernize securely
Servers
Network
APIs
Stream


descope
Drag & Drop
Your Auth
PagerDuty
NetApp
DataDome
NEUBIRD
Agentic AI SRE for AWS
AWS GenAI Accelerator
glean


CHECK POINT
Qualcomm
Empowering AI innovation at the edge
CHECK POINT
100% Security Effectiveness.
That's PREVENTION-FIRST AI SECURITY
CHECK POINT
We block better.
Infosys
doit


ECK POINT
SUSE
Linux,
Cloud Native,
AI and Edge
Reliable, secure and open
infrastructure solutions

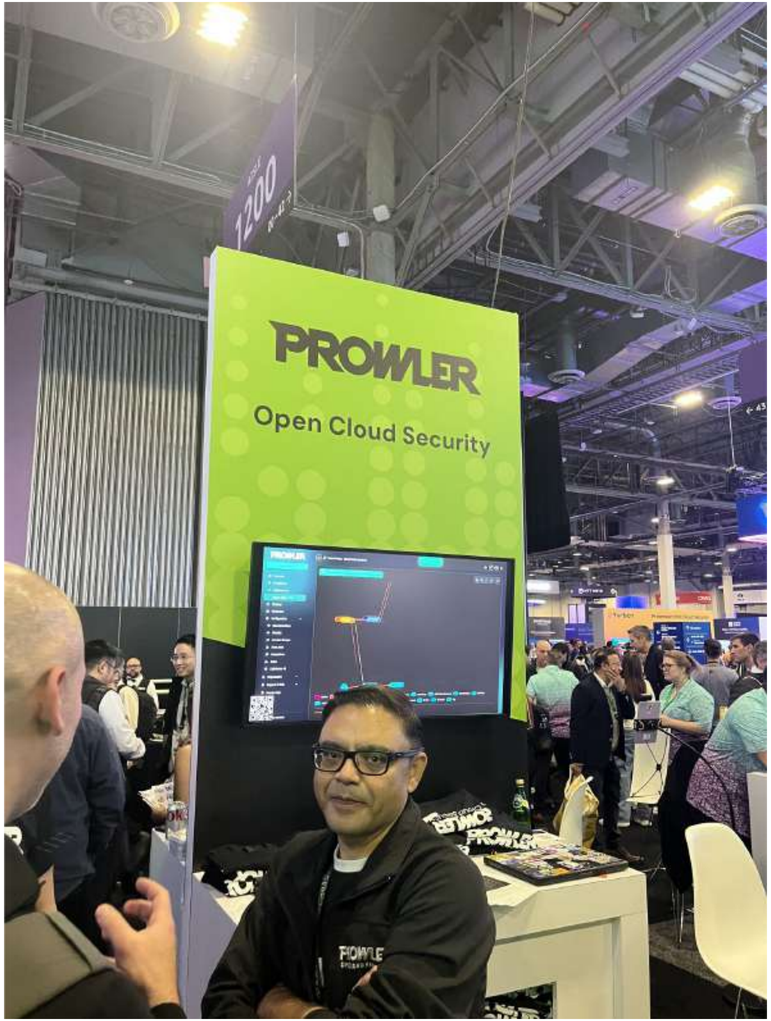

native
native.security
hindra
IVE!
Multi Cloud Rollout
aws
And more than a hundred enforcement controls in other cloud providers


B 30
Build, monitor, and secure AI applications
One unified platform to protect, control, and build AI initiatives at scale
CLOUDFLARE
Control
Protect
Build
Defend
Power and protect your AI applications with Cloudflare's global GPU network
FIX CODE WITHOUT THE HEADACHE

SentinelO
SOLARWINDS
AI-powere
ITSM, an
cohere

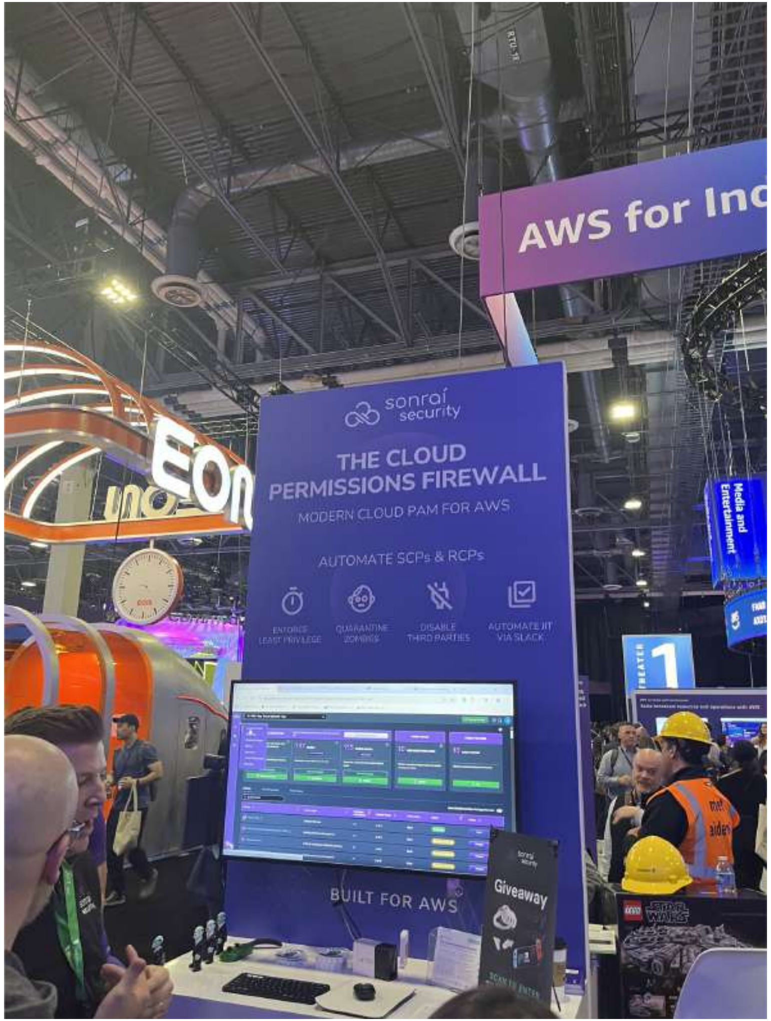
CONCIERTO
REVOLUTIONAIZING TRANSFORMATIONS
MODERNIZE
Legacy to AI Ready Apps
MIGRATE
Unified Pl
for Hype
Transfo

Don't ~~block~~ MCP
skyflow
Don't ~~DIY~~ PII
skyflow
Want a follow-up demo?


1200
PROWLER
Open Cloud Security
PROWLER

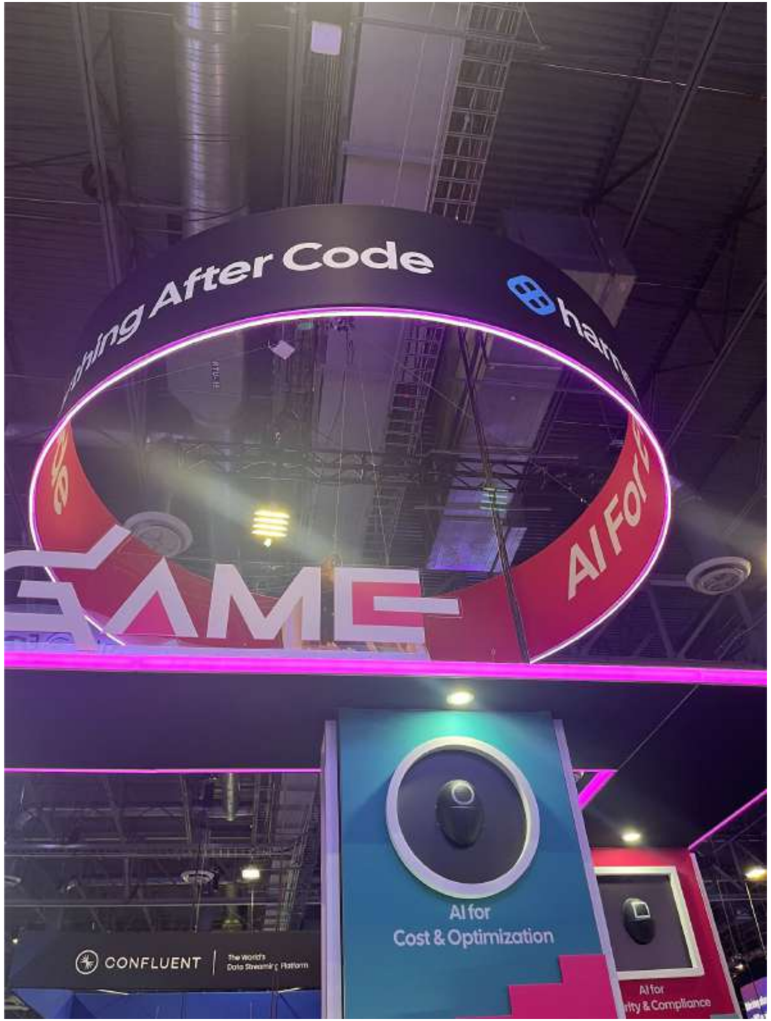
Turbot
Prevention-first Cloud Security
Reduce risk. End alert fatigue.
Turbot powers prevention
Identify Preventive Gaps
Turbot

Financial Services
Games
Healthcare and Life Sciences
synopsys
Leader In Engineering Solutions From Silicon to Systems
AGENTIC
433


AWS for Ind
EON
sonrai security
THE CLOUD PERMISSIONS FIREWALL
MODERN CLOUD PAM FOR AWS
AUTOMATE SCPs & RCPs
ENFORCE LEAST PRIVILEGE
QUARANTINE ZOMBIES
DISABLE THIRD PARTIES
AUTOMATE JIT VIA SLACK
BUILT FOR AWS
Giveaway
Media and Entertainment
THEATER 1
LEGO STAR WARS

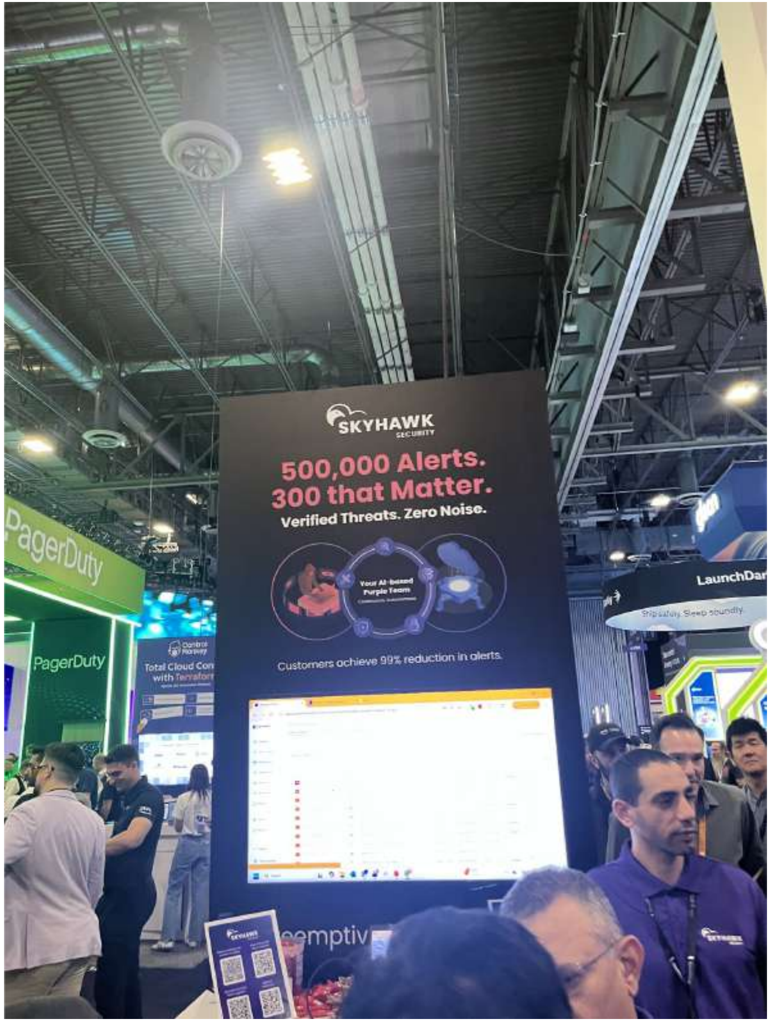
GitLab
Join us and learn more
HashiCorp
an IBM Company

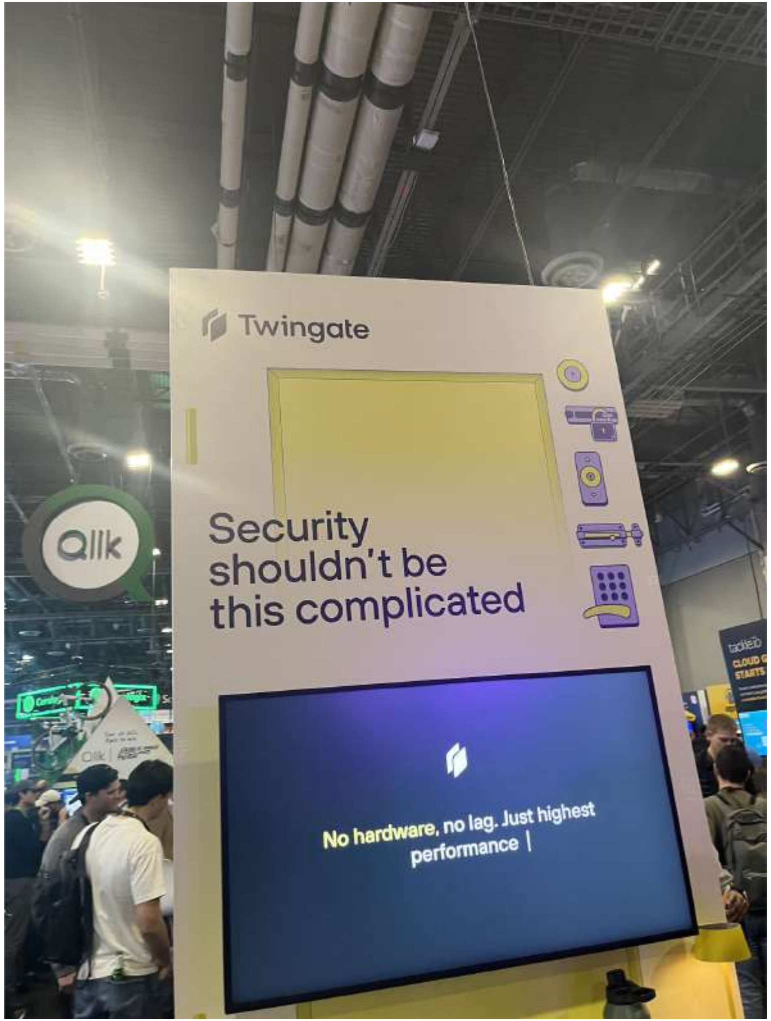
Teleport
Access and Protect
Your AI and Classic Infrastructure


hing After Code
harn
AI For
GAME
AI for
Cost & Optimization
CONFLUENT
The World's Data Streaming Platform
AI for
rity & Compliance

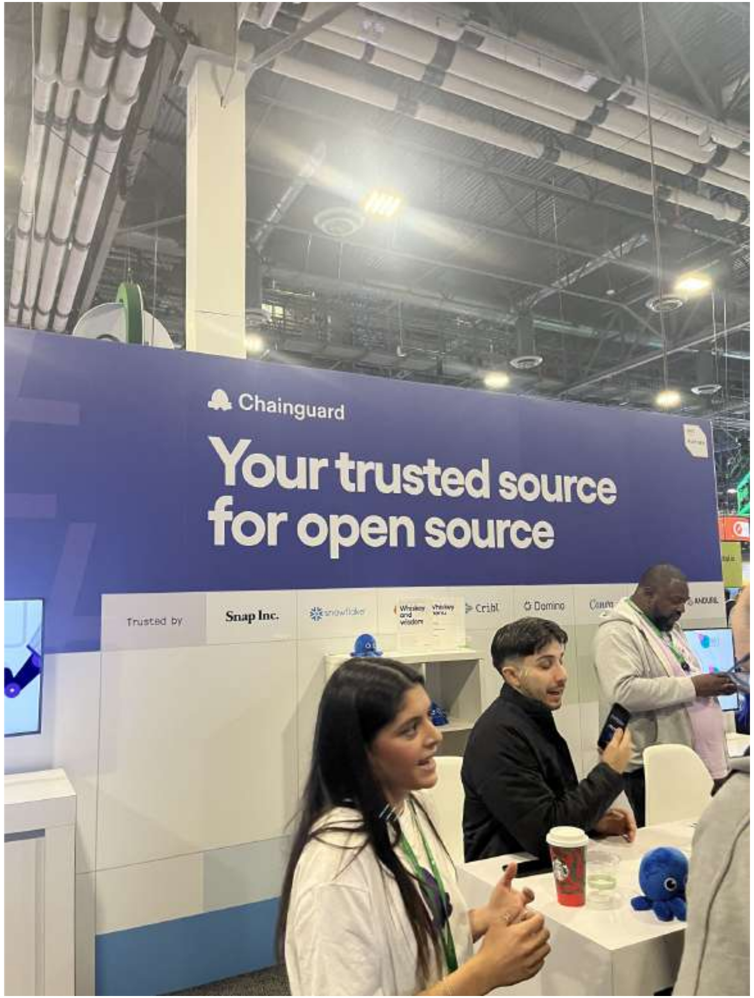
AI For Everything After Code
hing Afte
e to the Agentic Enterp
upwind
Cloud Security Happens At Runtime

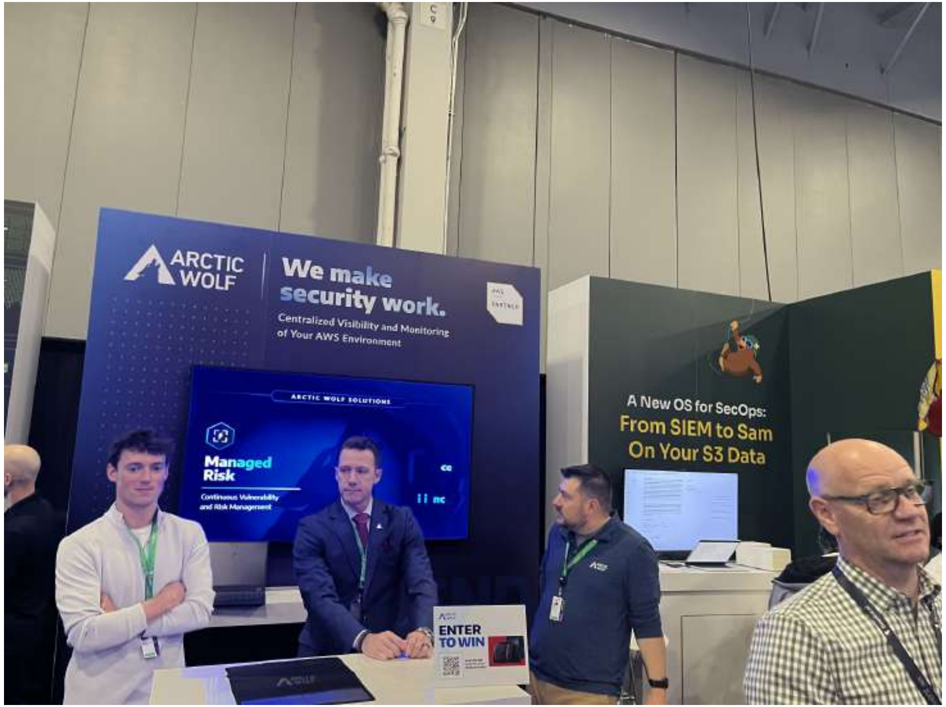
splunk
a cisco compa
CLOUD
STORAGE SECURITY
aws
PARTNER
DSPM for the Cloud Storage Layer
Activity Monitoring
Data Classification
Threat Detection
Anomaly Detection
Inventory
The Blind Spot in Cloud Security
d on you.
duckbill
Stop reacting
to cloud costs.
Start mastering them.


SKYHAWK
SECURITY
500,000 Alerts.
300 that Matter.
Verified Threats. Zero Noise.
Your AI-based
Purple Team
Customers achieve 99% reduction in alerts.
PagerDuty
PagerDuty
LaunchDar
Ship safely. Sleep soundly.
Total Cloud Con
with Terrafor
emptiv

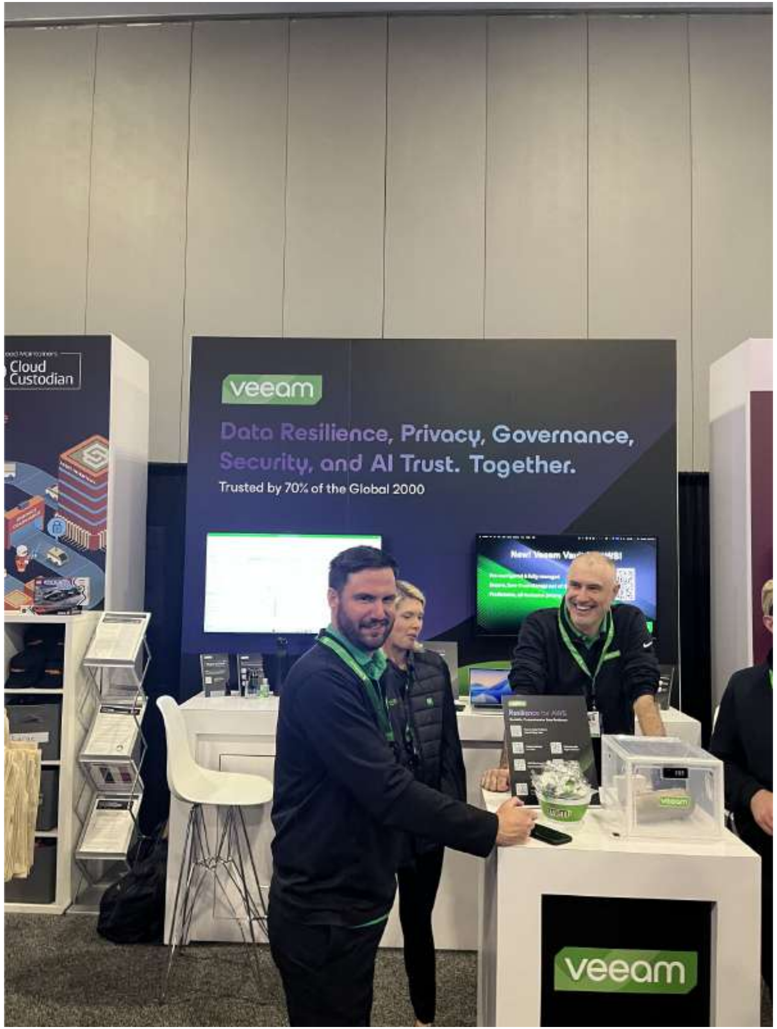

Twingate
Security shouldn't be this complicated
No hardware, no lag. Just highest performance |
Qlik

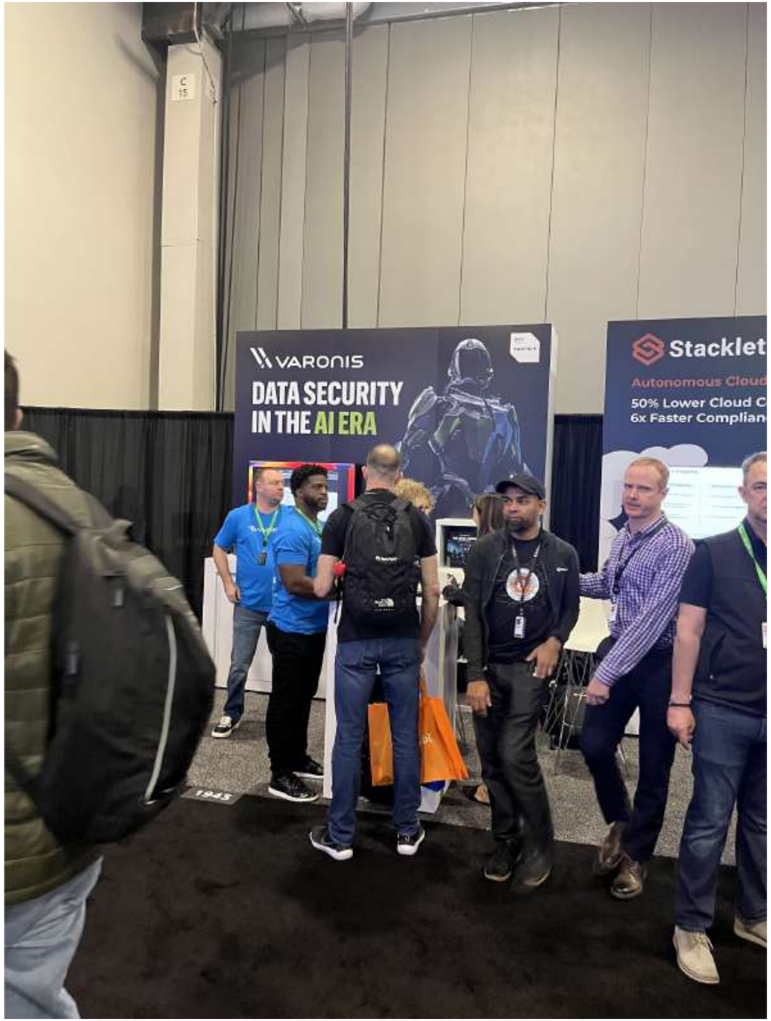
tailscale
The secure ne
for devs , IT
GTM SUCCESS
IDENTIFY
CO-SELL
CLOSE

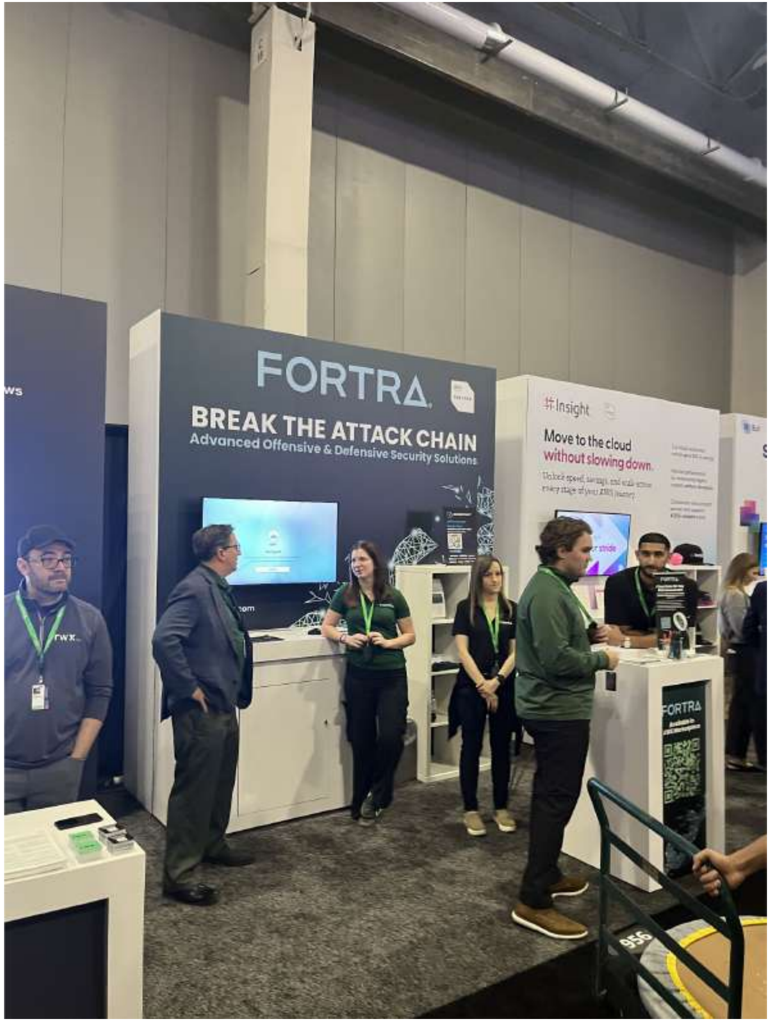

Chainguard
Your trusted source for open source
Trusted by
Snap Inc.
snowflake
Whiskey and wisdom
Cribl
Domino
Canva
ANDURIL

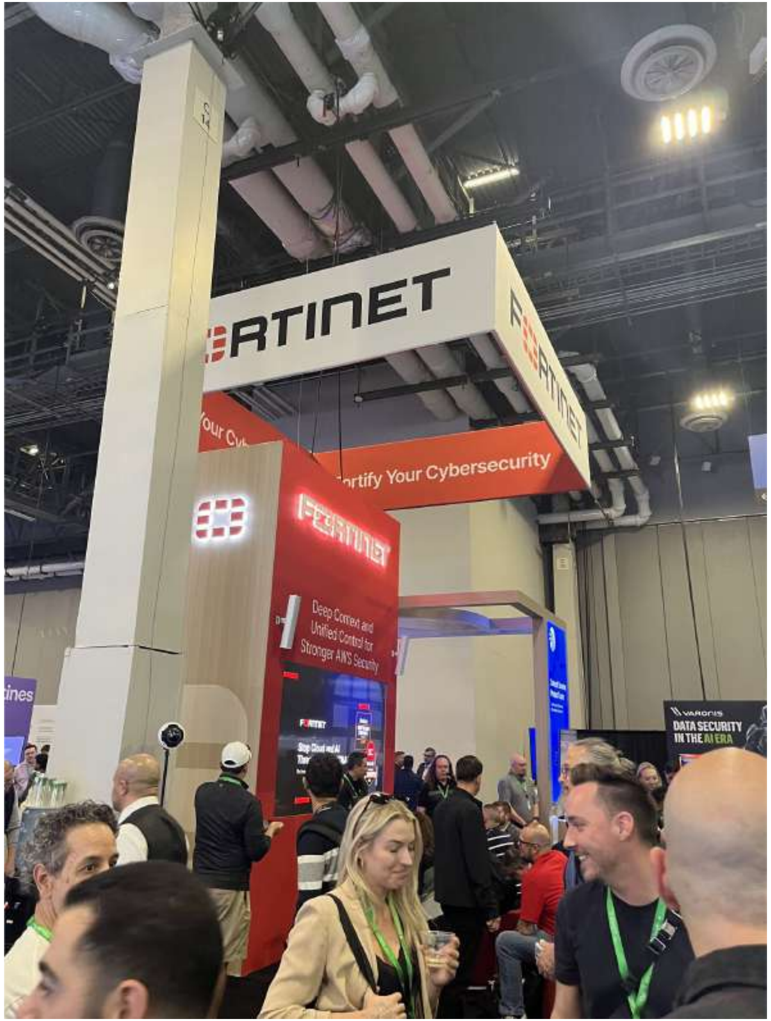

ARCTIC WOLF
We make security work.
Centralized Visibility and Monitoring of Your AWS Environment
ARCTIC WOLF SOLUTIONS
Managed Risk
Continuous Vulnerability and Risk Management
ENTER TO WIN
A New OS for SecOps:
From SIEM to Sam
On Your S3 Data

CloudQuery
Cloud asset inventory for security and platform
CloudQuery is AI-powered data integration that unifies all of your cloud infrastructure configuration
All Your Clouds. One Query.
aws
WIZ
70+ cloud infrastructure data sources
CloudQuery
Embed
Asset Management
Cost Savings
AI pipelines
STAR WARS


Cloud Custodian
veeam
Data Resilience, Privacy, Governance, Security, and AI Trust. Together.
Trusted by 70% of the Global 2000
New! Veeam Vault
Resilience for AWS
veeam


C 15
VARONIS
DATA SECURITY IN THE AI ERA
Stacklet
Autonomous Cloud
50% Lower Cloud C
6x Faster Complian
1945


FORTRA
BREAK THE ATTACK CHAIN
Advanced Offensive & Defensive Security Solutions
Insight
Move to the cloud without slowing down.
FORTRA
956

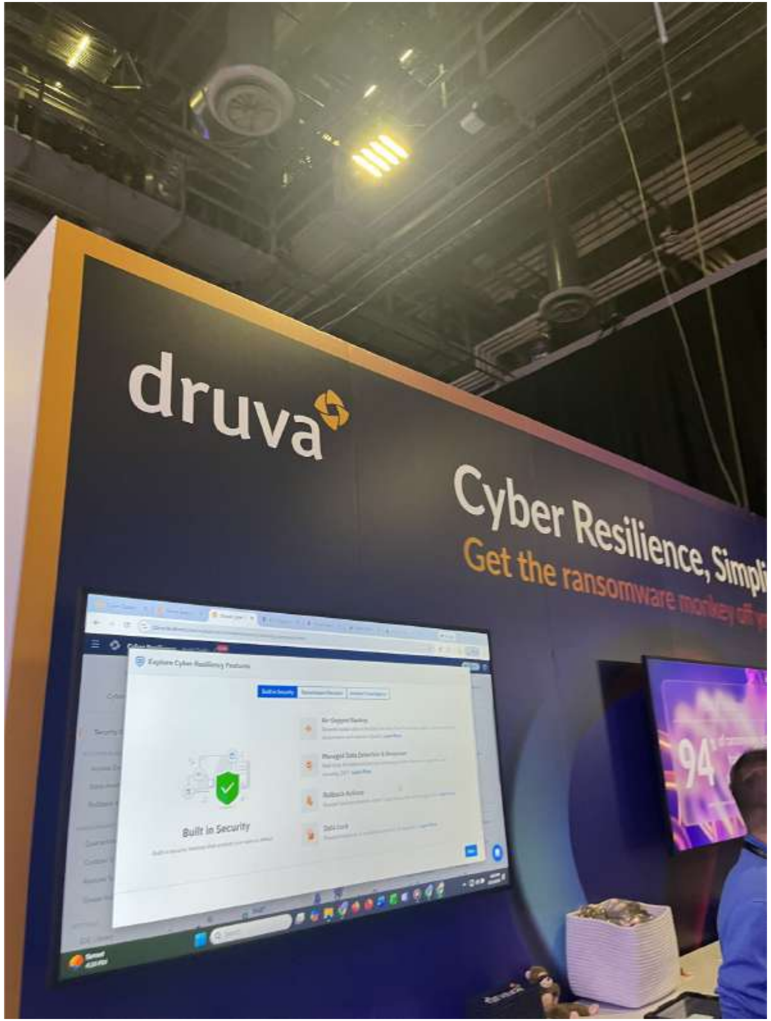

FORTINET
Fortify Your Cybersecurity
FORTINET
Deep Context and Unified Control for Stronger AWS Security
VARONIS
DATA SECURITY IN THE AI ERA

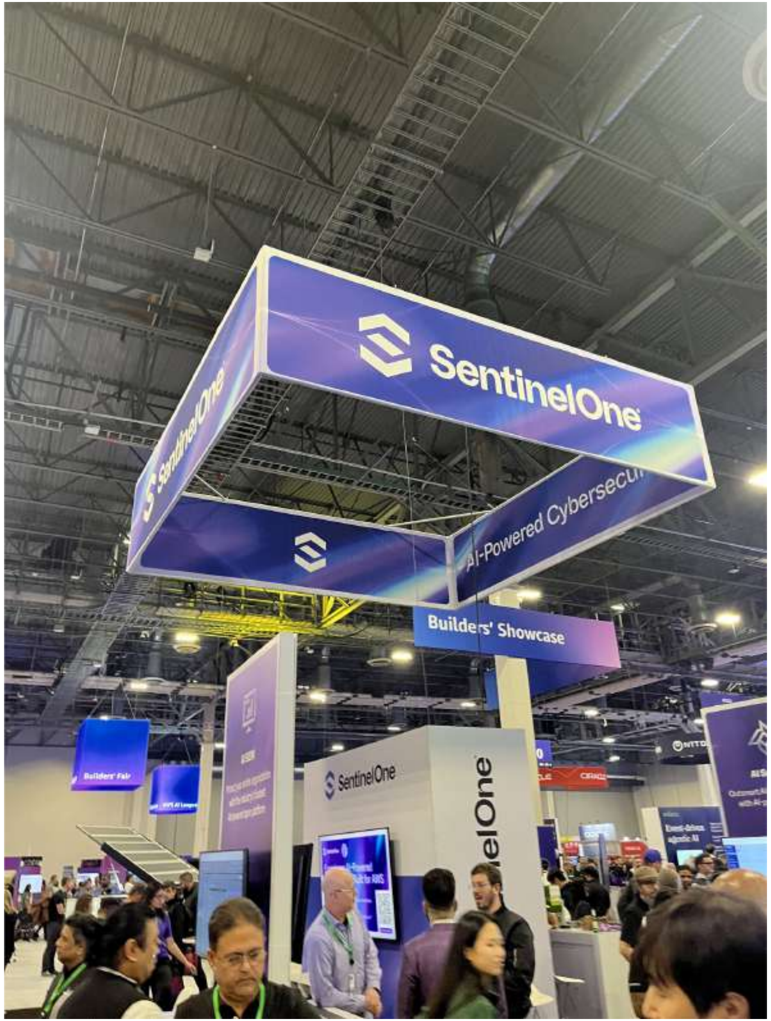
Scylla
CYERA
The AI-Native Data Security Platform
DISCOVER AND CLASSIFY DATA
ORCHESTRATE DLP WITH EASE
95%
80%
AWS PARTNER
MONITOR ACCESS ACTIVITIES
SECURE AI ADOPTION
The Futur
CYERA

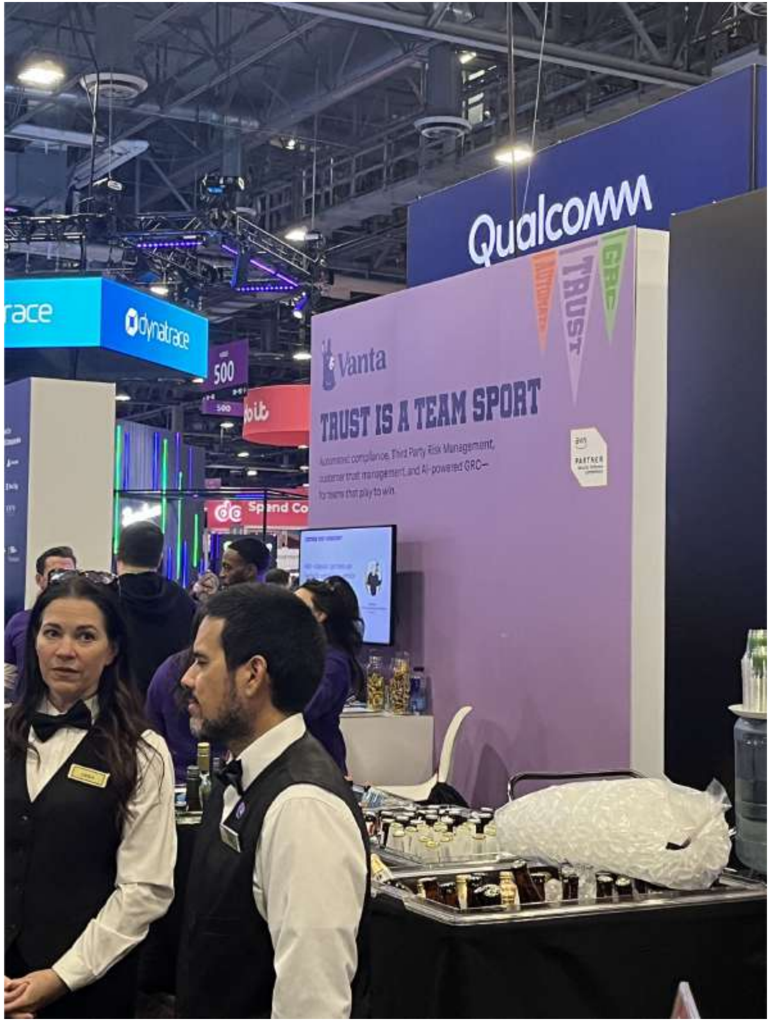
Trellix Wise
Your Sixth Sense for Security
No alert left behind, 100% investigated
5x Improved analyst efficiency by 5x
50% Reduced MTTD and MTTR by 50%
8hrs recovered for every 100 alerts investigated
Outbound Data Loss Prevention: Email
Trellix Email Security Cloud
Monitors and controls data transfers within any outbound emails
Stops sensitive data exfiltration before breaches occur
Trellix Data Loss Prevention
Trellix DLP
Identifies and blocks sensitive data from within emails and their attachments based on comprehensive DLP Policies
BEDTIME STORIES
BETTER WITH WIZ
WIZzz
STMAN

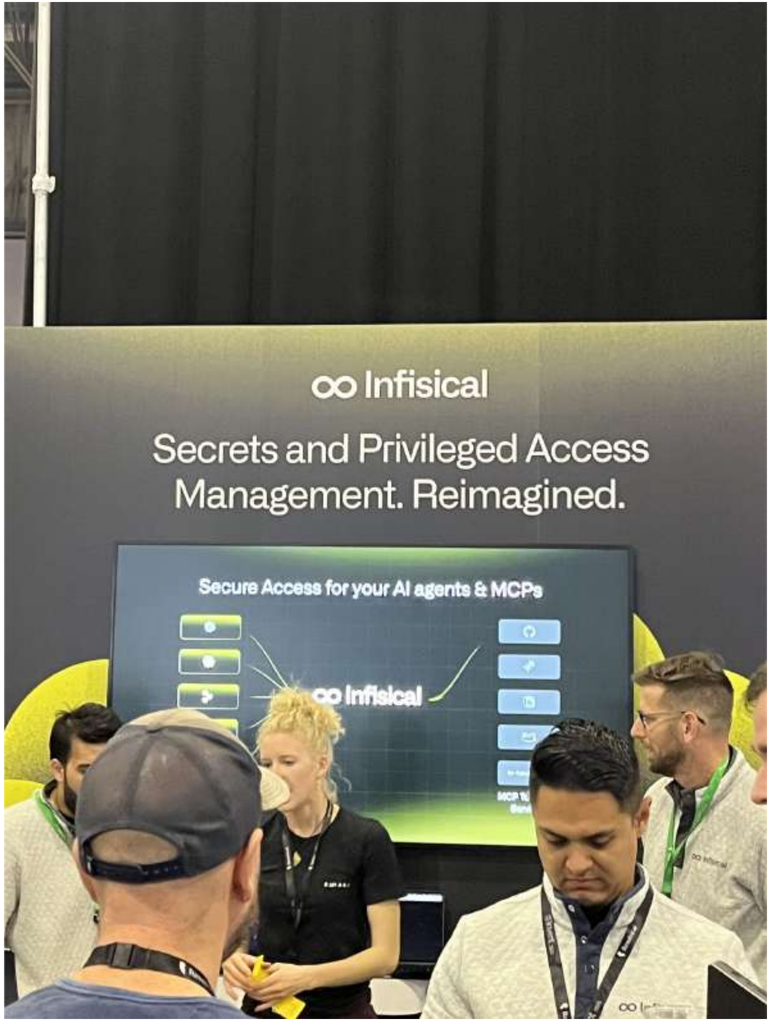
WIZzz
BETTER WITH WIZ
Are your APIs ready for AI?
WIZ

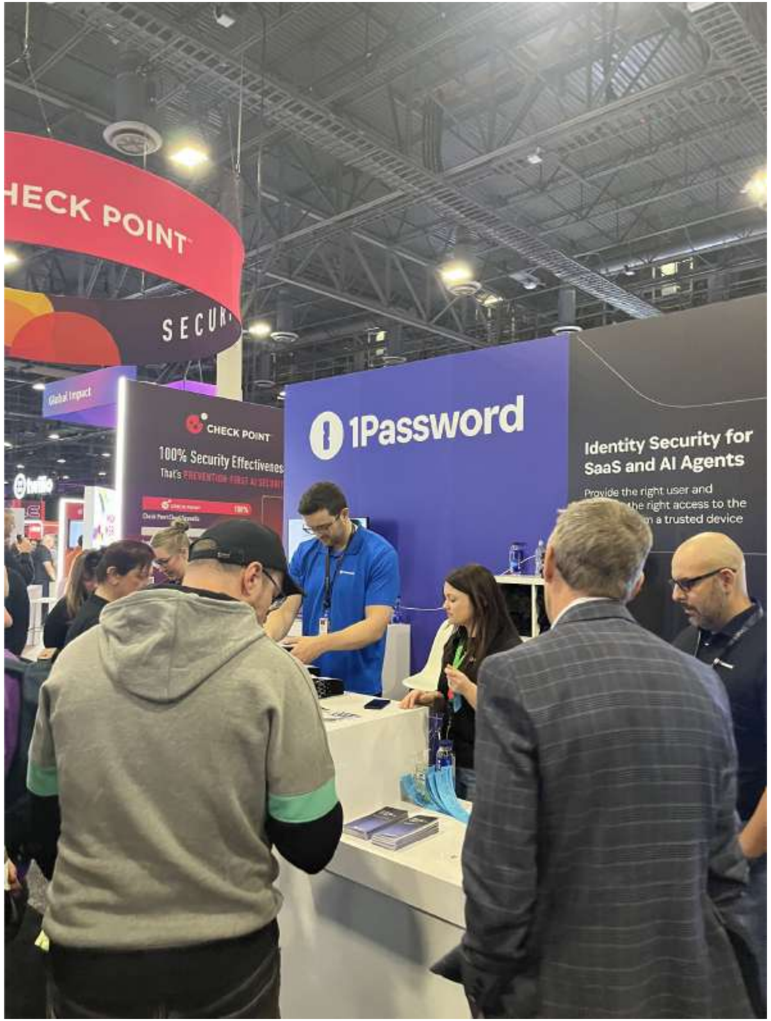
OOMS
sysdig
Cloud security, th
guesswork.
lack boxes.
eal-time defense,
ort.
Cloud defense
without compro
TEST YOUR SKILLS

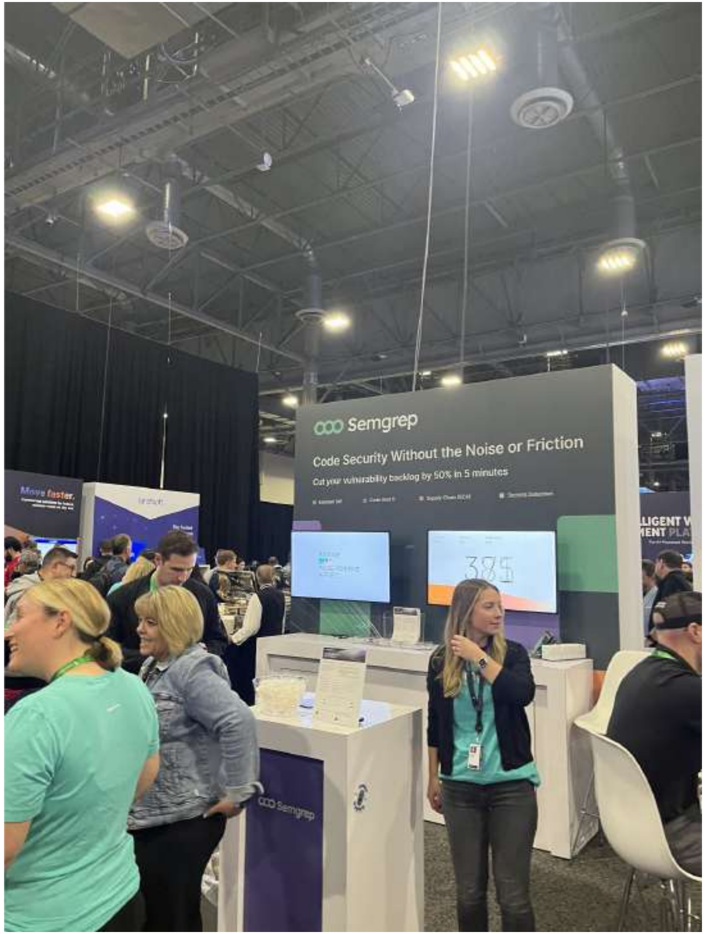

druva
Cyber Resilience, Simpli
Get the ransomware monkey off y
Explore Cyber Resiliency Features
Built in Security
94


SentinelOne
SentinelOne
AI-Powered Cybersecu
Builders' Showcase
SentinelOne
SentinelOne
Builders' Fair


Qualcomm
dynatrace
Vanta
TRUST
GRC
TRUST IS A TEAM SPORT
Automated compliance, Third Party Risk Management, customer trust management, and AI-powered GRC—for teams that play to win.
aws PARTNER
Spend Co


Infisical
Secrets and Privileged Access Management. Reimagined.
Secure Access for your AI agents & MCPs
Infisical

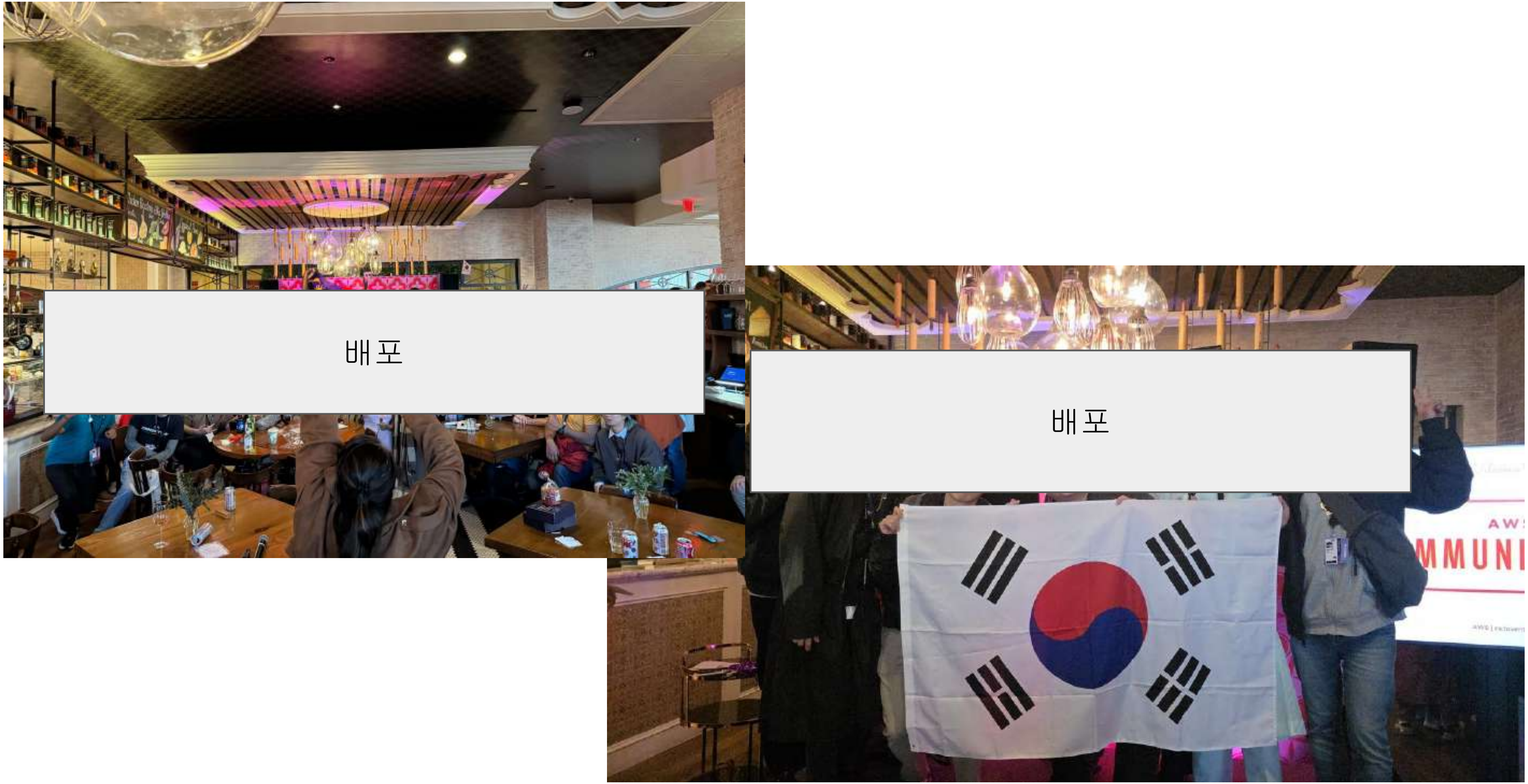

HECK POINT
SECU
Global Impact
CHECK POINT
100% Security Effectivenes
That's PREVENTION FIRST AI SECURI
1Password
Identity Security for SaaS and AI Agents
Provide the right user and
the right access to the
m a trusted device


Semgrep
Code Security Without the Noise or Friction
Cut your vulnerability backlog by 50% in 5 minutes
385
Move faster.
Semgrep

Develop fast.
Stay Secure.
snyk.io
snyk
orca
BORN TO HUNT THREATS
Command your cloud to identify,
prioritize, and remediate risks
Detect Critical
Risks in Your
AWS Environment
Unified
AppSec &
Cloud Security

유저 그룹 & 네트워킹

Eggplant Parm
AWS
COMMUNITY HUB
Welcome
TO THE AWS
COMMUNITY HUB



배포

배포

배포
배포

배포
배포

네버 엔딩 파티!

allegiant stadium

allegiant stadium
allegiant stadium PRIVATE EVENTS
allegiant stadium PRIVATE EVENTS
C134

Tour 25

APJon
Tour 25
LAS VEGAS NEVADA

AWS re:Play
AWS re:Play
aws

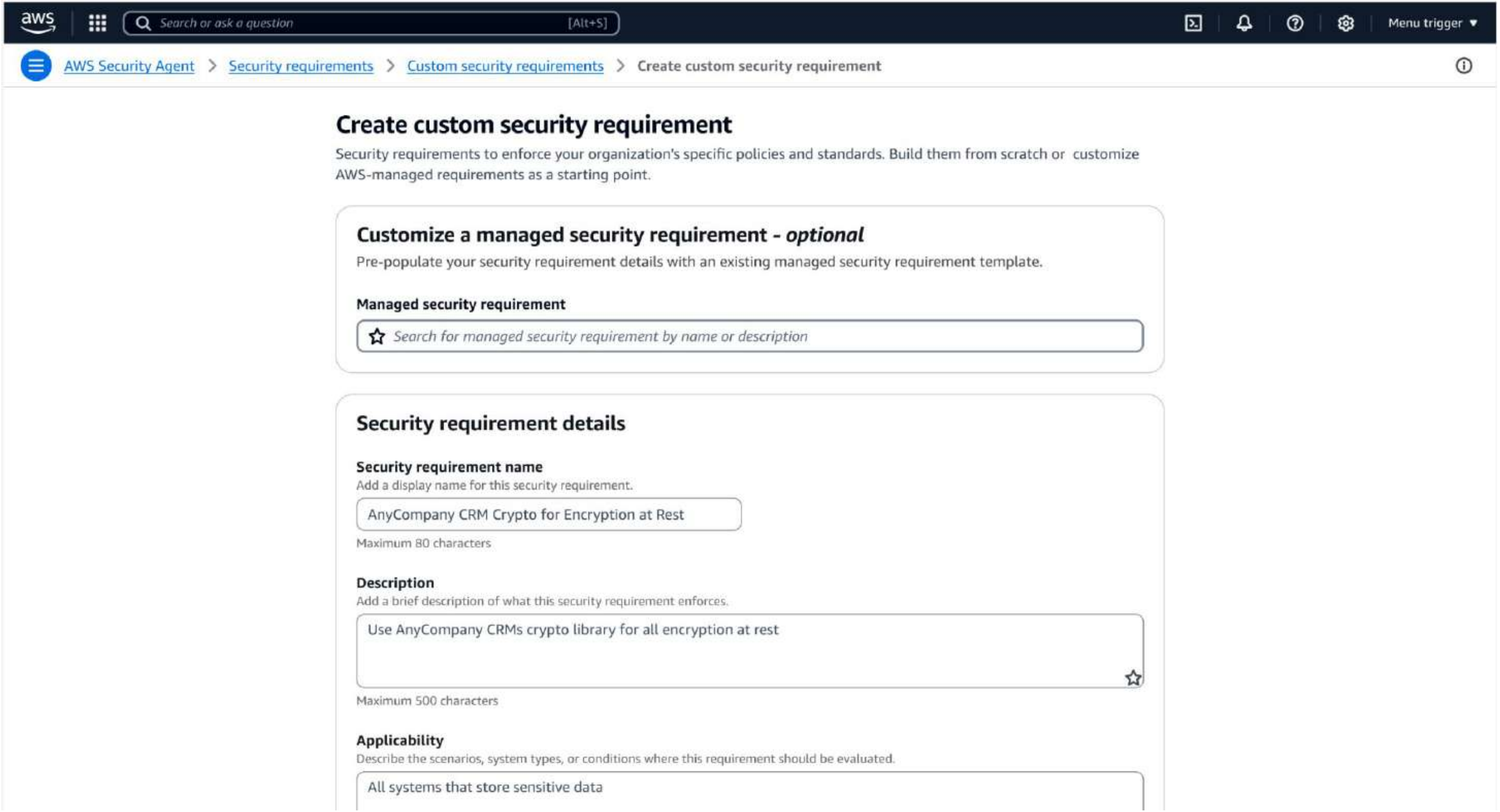
AWS re:Invent에서 공개된 보안 관련 대표 제품/피쳐

- AWS Security Agent (Preview)
- AWS Security Hub (General Availability)
- IAM Policy Autopilot
- GuardDuty Malware Protection for AWS Backup
- Outbound Identity Federation
- Amazon CloudWatch Unified Data Management
- Network Firewall Marketplace Rules
- Aws login - Programmatically access AWS with your console credentials
- Zero-Touch Secret Rotation for your third-party secrets

AWS Security Agent (Preview)

AWS Security Agent는 개발 수명 주기 전반에 걸쳐 애플리케이션을 선제적으로 보호하도록 설계된 프론티어 에이전트입니다. 이 서비스는 조직의 특정 요구 사항에 맞춘 자동화된 애플리케이션 보안 검토를 수행하고, 컨텍스트 인식 침투 테스트(penetration testing)를 온디맨드로 제공합니다

영상: https://www.youtube.com/watch?v=LPo4kI656bY



Create custom security requirement

Security requirements to enforce your organization's specific policies and standards. Build them from scratch or customize AWS-managed requirements as a starting point.

Customize a managed security requirement - *optional*

Pre-populate your security requirement details with an existing managed security requirement template.

Managed security requirement

☆ *Search for managed security requirement by name or description*

Security requirement details

Security requirement name

Add a display name for this security requirement.

AnyCompany CRM Crypto for Encryption at Rest

Maximum 80 characters

Description

Add a brief description of what this security requirement enforces.

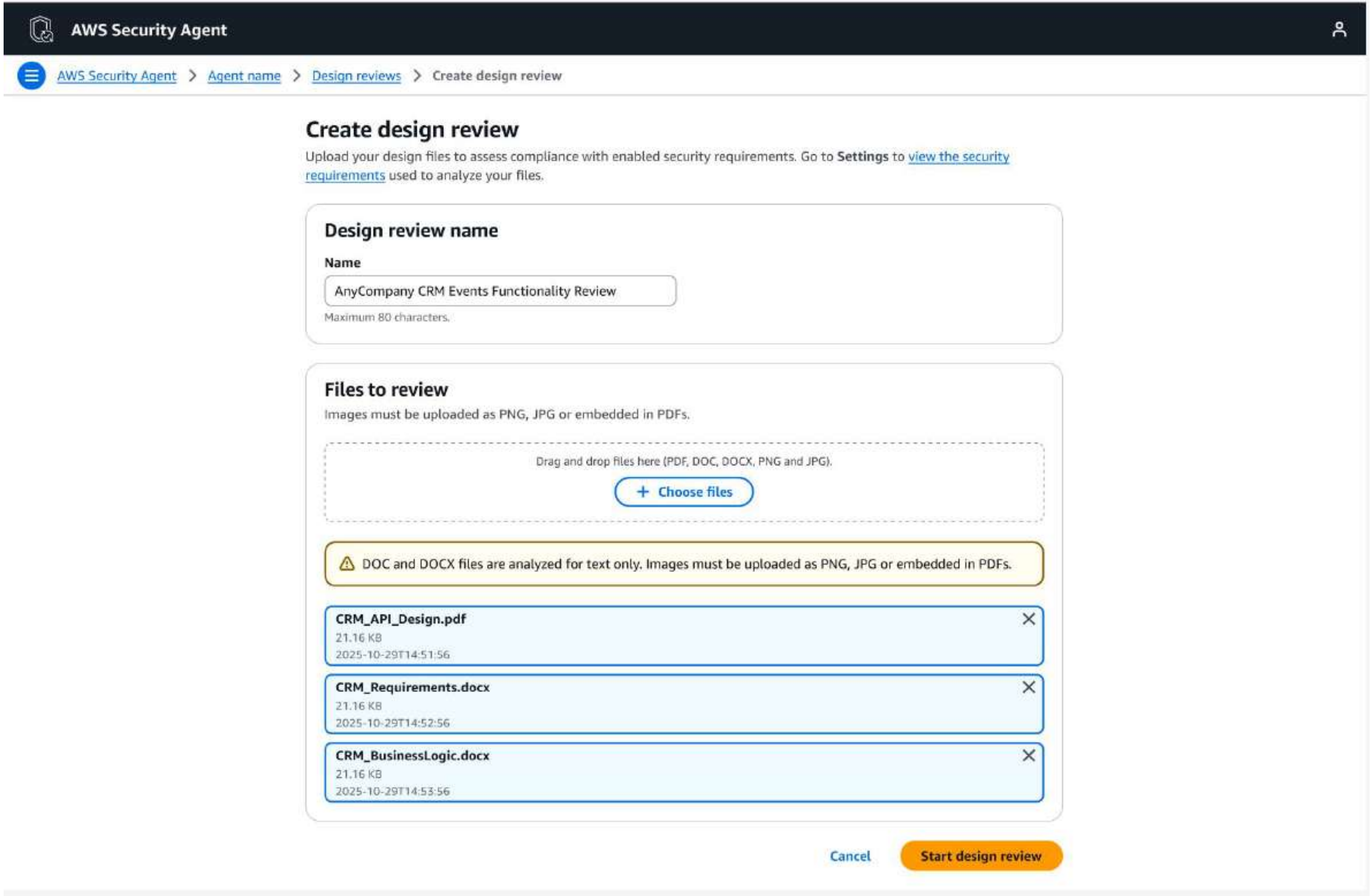
Use AnyCompany CRMs crypto library for all encryption at rest

Maximum 500 characters

Applicability

Describe the scenarios, system types, or conditions where this requirement should be evaluated.

All systems that store sensitive data


AWS Security Agent
AWS Security Agent > Agent name > Design reviews > Create design review

Create design review

Upload your design files to assess compliance with enabled security requirements. Go to **Settings** to view the security requirements used to analyze your files.

Design review name

Name

AnyCompany CRM Events Functionality Review

Maximum 80 characters.

Files to review

Images must be uploaded as PNG, JPG or embedded in PDFs.

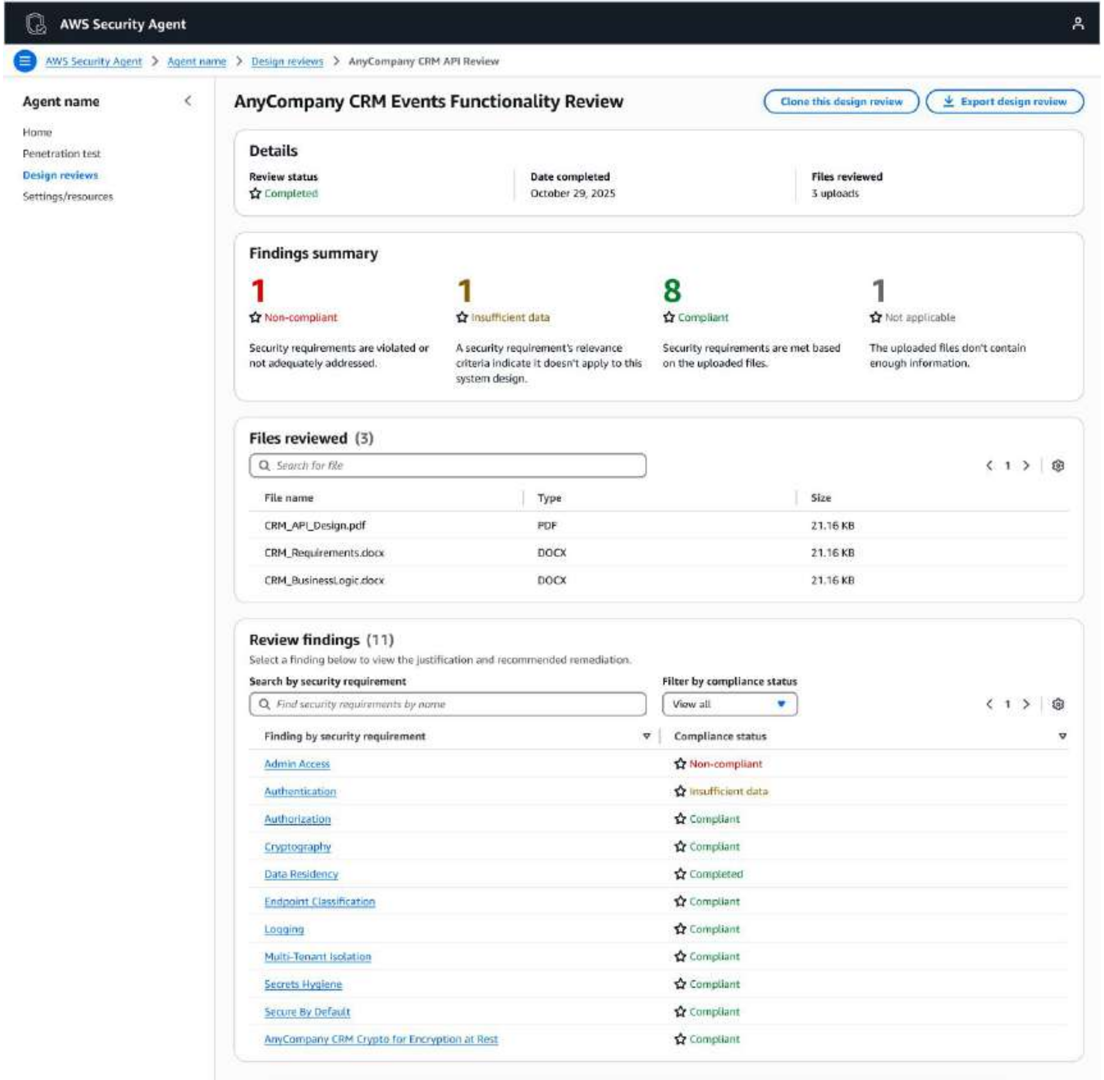
Drag and drop files here (PDF, DOC, DOCX, PNG and JPG).

⚠ DOC and DOCX files are analyzed for text only. Images must be uploaded as PNG, JPG or embedded in PDFs.

CRM_API_Design.pdf
21.16 KB
2025-10-29T14:51:56

CRM_Requirements.docx
21.16 KB
2025-10-29T14:52:56

CRM_BusinessLogic.docx
21.16 KB
2025-10-29T14:53:56



AnyCompany CRM Events Functionality Review

Details

Review status
☆ Completed

Date completed
October 29, 2025

Files reviewed
3 uploads

Findings summary

1
☆ Non-compliant
Security requirements are violated or not adequately addressed.

1
☆ Insufficient data
A security requirement's relevance criteria indicate it doesn't apply to this system design.

8
☆ Compliant
Security requirements are met based on the uploaded files.

1
☆ Not applicable
The uploaded files don't contain enough information.

Files reviewed (3)

File name	Type	Size
CRM_API_Design.pdf	PDF	21.16 KB
CRM_Requirements.docx	DOCX	21.16 KB
CRM_BusinessLogic.docx	DOCX	21.16 KB

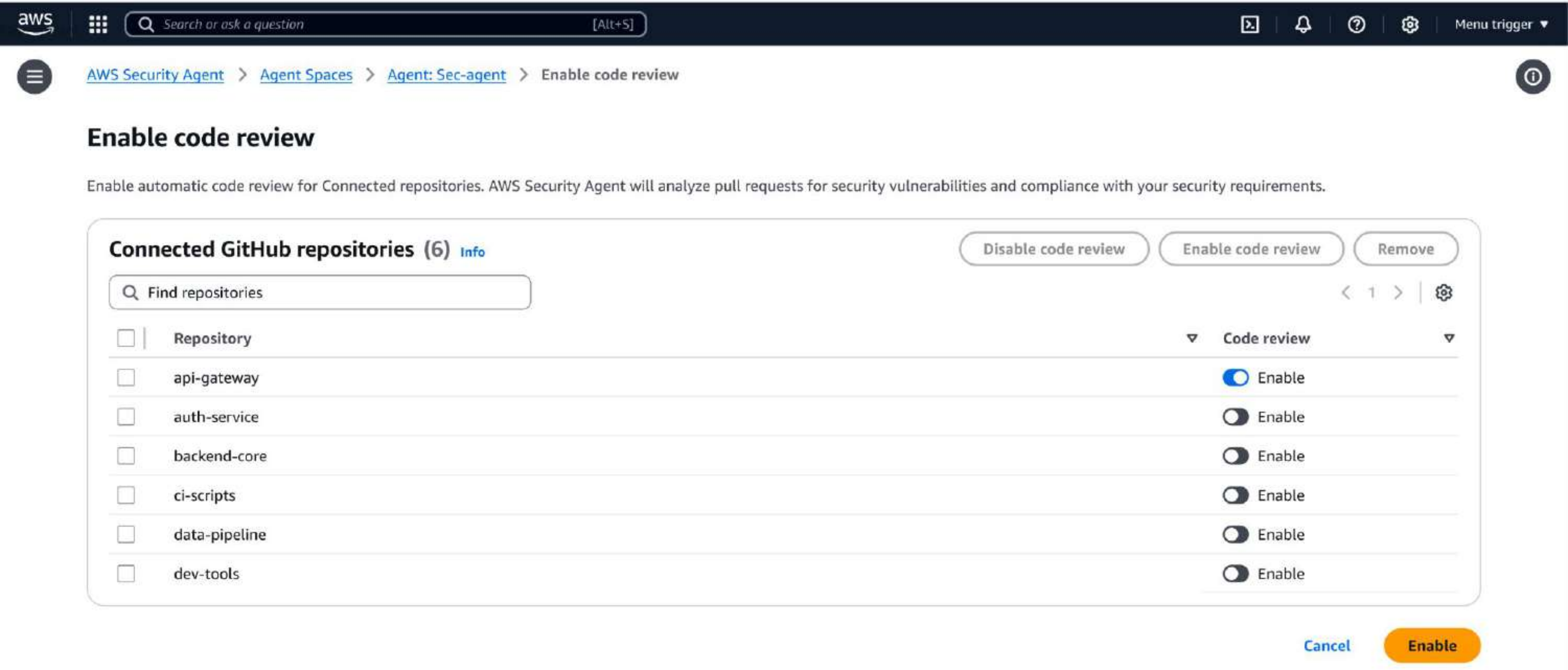
Review findings (11)

Select a finding below to view the justification and recommended remediation.

Search by security requirement

Filter by compliance status

Finding by security requirement	Compliance status
Admin Access	☆ Non-compliant
Authentication	☆ Insufficient data
Authorization	☆ Compliant
Cryptography	☆ Compliant
Data Residency	☆ Completed
Endpoint Classification	☆ Compliant
Logging	☆ Compliant
Multi-Tenant Isolation	☆ Compliant
Secrets Hygiene	☆ Compliant
Secure By Default	☆ Compliant
AnyCompany CRM Crypto for Encryption at Rest	☆ Compliant



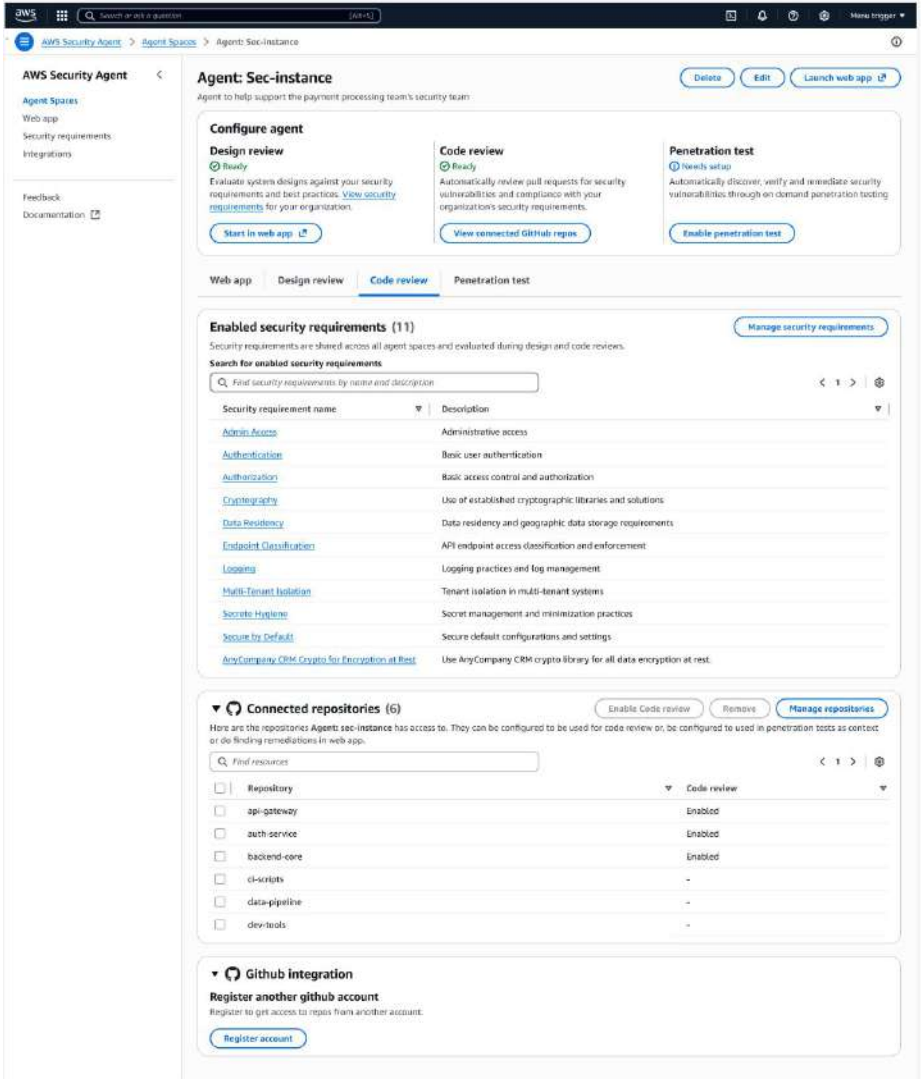
AWS Security Agent > Agent Spaces > Agent: Sec-agent > Enable code review

Enable code review

Enable automatic code review for Connected repositories. AWS Security Agent will analyze pull requests for security vulnerabilities and compliance with your security requirements.

Connected GitHub repositories (6) Info

☐	Repository	Code review
☐	api-gateway	● Enable
☐	auth-service	○ Enable
☐	backend-core	○ Enable
☐	ci-scripts	○ Enable
☐	data-pipeline	○ Enable
☐	dev-tools	○ Enable



Agent: Sec-instance

Agent to help support the payment processing team's security team

Configure agent

Design review

✓ Ready

Evaluate system designs against your security requirements and best practices. View security requirements for your organization.

Code review

✓ Ready

Automatically review pull requests for security vulnerabilities and compliance with your organization's security requirements.

Penetration test

ⓘ Needs setup

Automatically discover, verify and remediate security vulnerabilities through on demand penetration testing

Enabled security requirements (11)

Security requirements are shared across all agent spaces and evaluated during design and code reviews.

Search for enabled security requirements

Find security requirements by name and description

Security requirement name	Description
Admin Access	Administrative access
Authentication	Basic user authentication
Authorization	Basic access control and authorization
Cryptography	Use of established cryptographic libraries and solutions
Data Residency	Data residency and geographic data storage requirements
Endpoint Classification	API endpoint access classification and enforcement
Logging	Logging practices and log management
Multi-Tenant Isolation	Tenant isolation in multi-tenant systems
Secrets Hygiene	Secret management and minimization practices
Secure by Default	Secure default configurations and settings
AnyCompany CRM Crypto for Encryption at Rest	Use AnyCompany CRM crypto library for all data encryption at rest

Connected repositories (6)

Here are the repositories **Agent: sec-instance** has access to. They can be configured to be used for code review or, be configured to used in penetration tests as context or do finding remediations in web app.

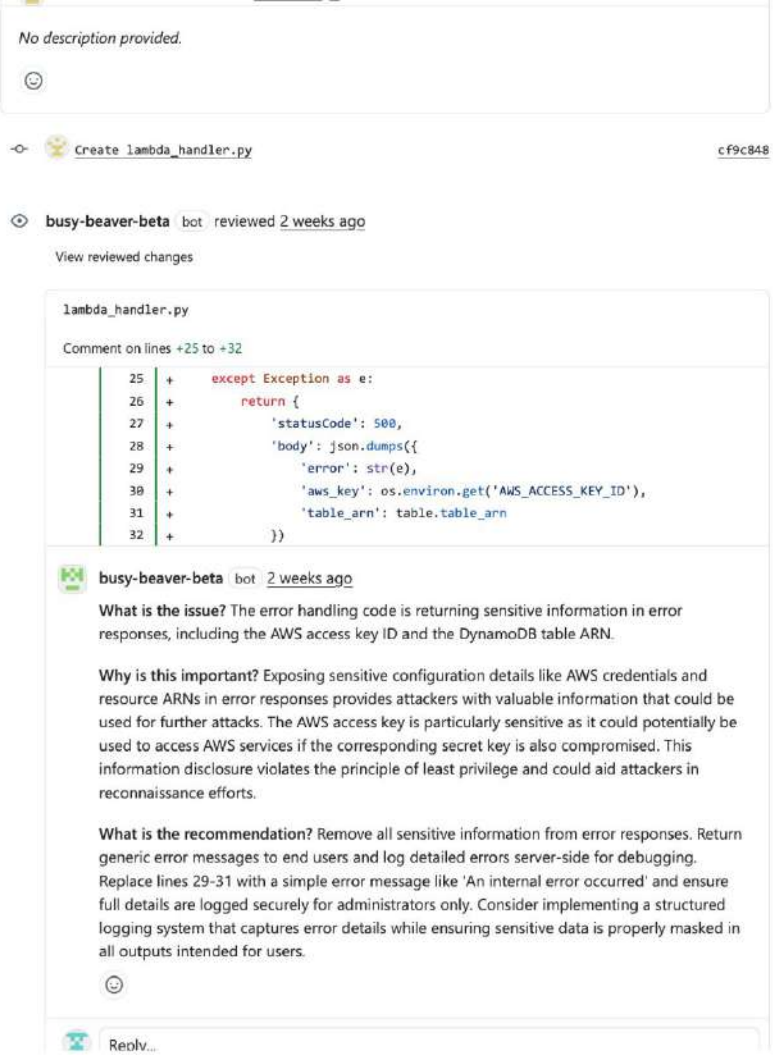
Find resources

☐	Repository	Code review
☐	api-gateway	Enabled
☐	auth-service	Enabled
☐	backend-core	Enabled
☐	ci-scripts	-
☐	data-pipeline	-
☐	dev-tools	-

Github integration

Register another github account

Register to get access to repos from another account.



No description provided.

`Create lambda_handler.py` cf9c848

busy-beaver-beta bot reviewed 2 weeks ago

lambda_handler.py

Comment on lines +25 to +32

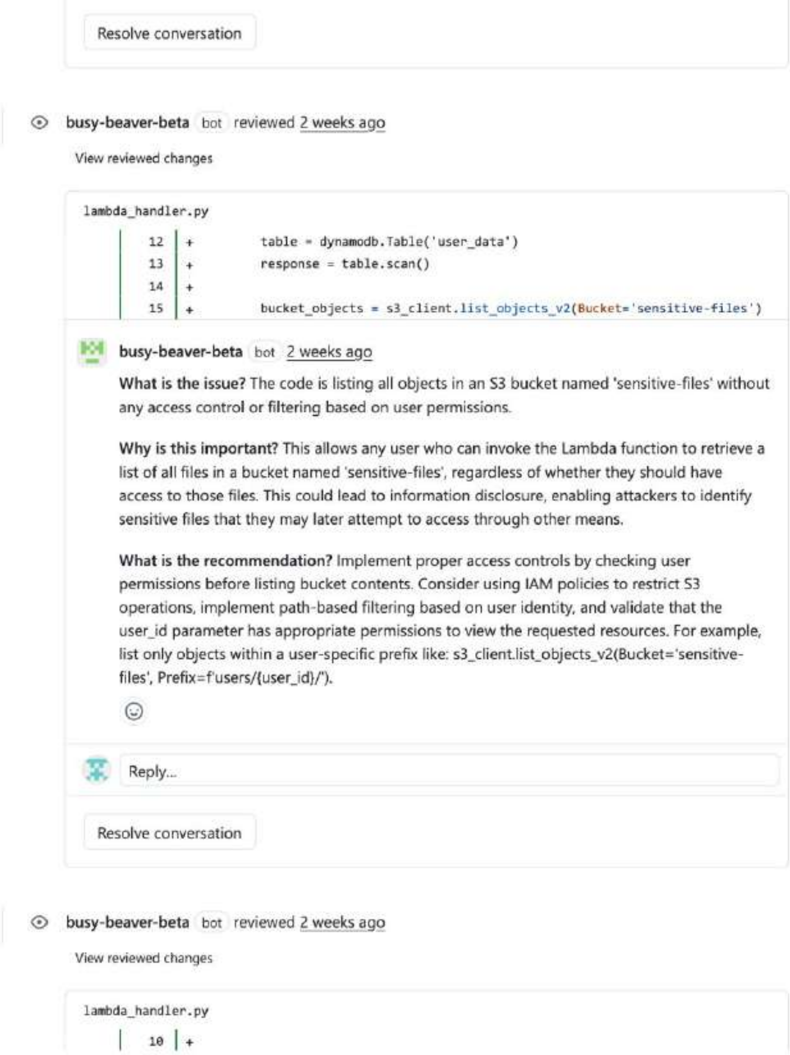
```
25  +     except Exception as e:
26  +         return {
27  +             'statusCode': 500,
28  +             'body': json.dumps({
29  +                 'error': str(e),
30  +                 'aws_key': os.environ.get('AWS_ACCESS_KEY_ID'),
31  +                 'table_arn': table.table_arn
32  +             })
```

busy-beaver-beta bot 2 weeks ago

What is the issue? The error handling code is returning sensitive information in error responses, including the AWS access key ID and the DynamoDB table ARN.

Why is this important? Exposing sensitive configuration details like AWS credentials and resource ARNs in error responses provides attackers with valuable information that could be used for further attacks. The AWS access key is particularly sensitive as it could potentially be used to access AWS services if the corresponding secret key is also compromised. This information disclosure violates the principle of least privilege and could aid attackers in reconnaissance efforts.

What is the recommendation? Remove all sensitive information from error responses. Return generic error messages to end users and log detailed errors server-side for debugging. Replace lines 29-31 with a simple error message like 'An internal error occurred' and ensure full details are logged securely for administrators only. Consider implementing a structured logging system that captures error details while ensuring sensitive data is properly masked in all outputs intended for users.



busy-beaver-beta bot reviewed 2 weeks ago

lambda_handler.py

```
12  +         table = dynamodb.Table('user_data')
13  +         response = table.scan()
14  +
15  +         bucket_objects = s3_client.list_objects_v2(Bucket='sensitive-files')
```

busy-beaver-beta bot 2 weeks ago

What is the issue? The code is listing all objects in an S3 bucket named 'sensitive-files' without any access control or filtering based on user permissions.

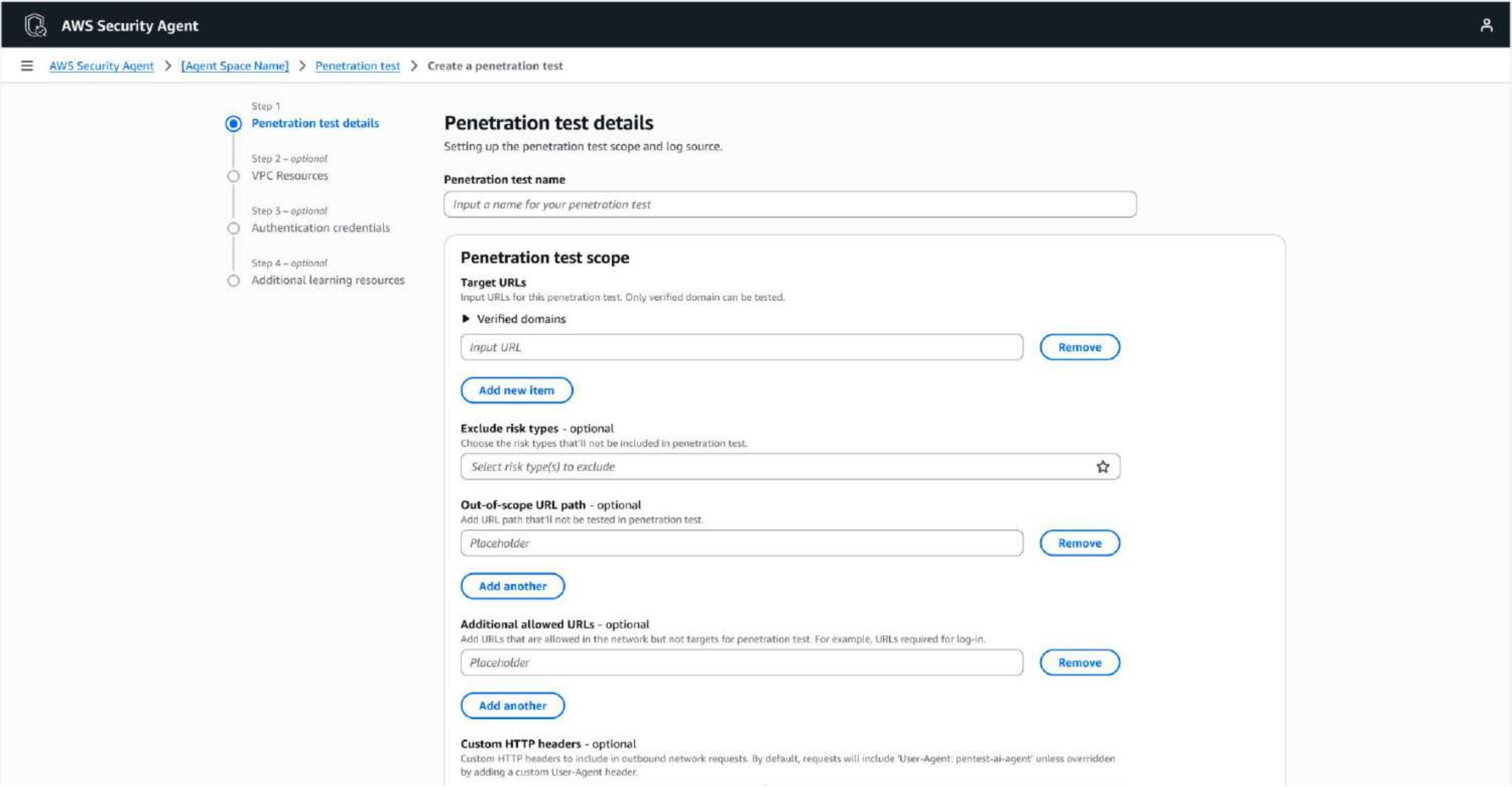
Why is this important? This allows any user who can invoke the Lambda function to retrieve a list of all files in a bucket named 'sensitive-files', regardless of whether they should have access to those files. This could lead to information disclosure, enabling attackers to identify sensitive files that they may later attempt to access through other means.

What is the recommendation? Implement proper access controls by checking user permissions before listing bucket contents. Consider using IAM policies to restrict S3 operations, implement path-based filtering based on user identity, and validate that the user_id parameter has appropriate permissions to view the requested resources. For example, list only objects within a user-specific prefix like: s3_client.list_objects_v2(Bucket='sensitive-files', Prefix=f'users/{user_id}/').

busy-beaver-beta bot reviewed 2 weeks ago

lambda_handler.py

```
10  +
```



Penetration test details

Setting up the penetration test scope and log source.

Penetration test name

Input a name for your penetration test

Penetration test scope

Target URLs

Input URLs for this penetration test. Only verified domain can be tested.

▶ Verified domains

Input URL

Exclude risk types - optional

Choose the risk types that'll not be included in penetration test.

Select risk type(s) to exclude

Out-of-scope URL path - optional

Add URL path that'll not be tested in penetration test.

Placeholder

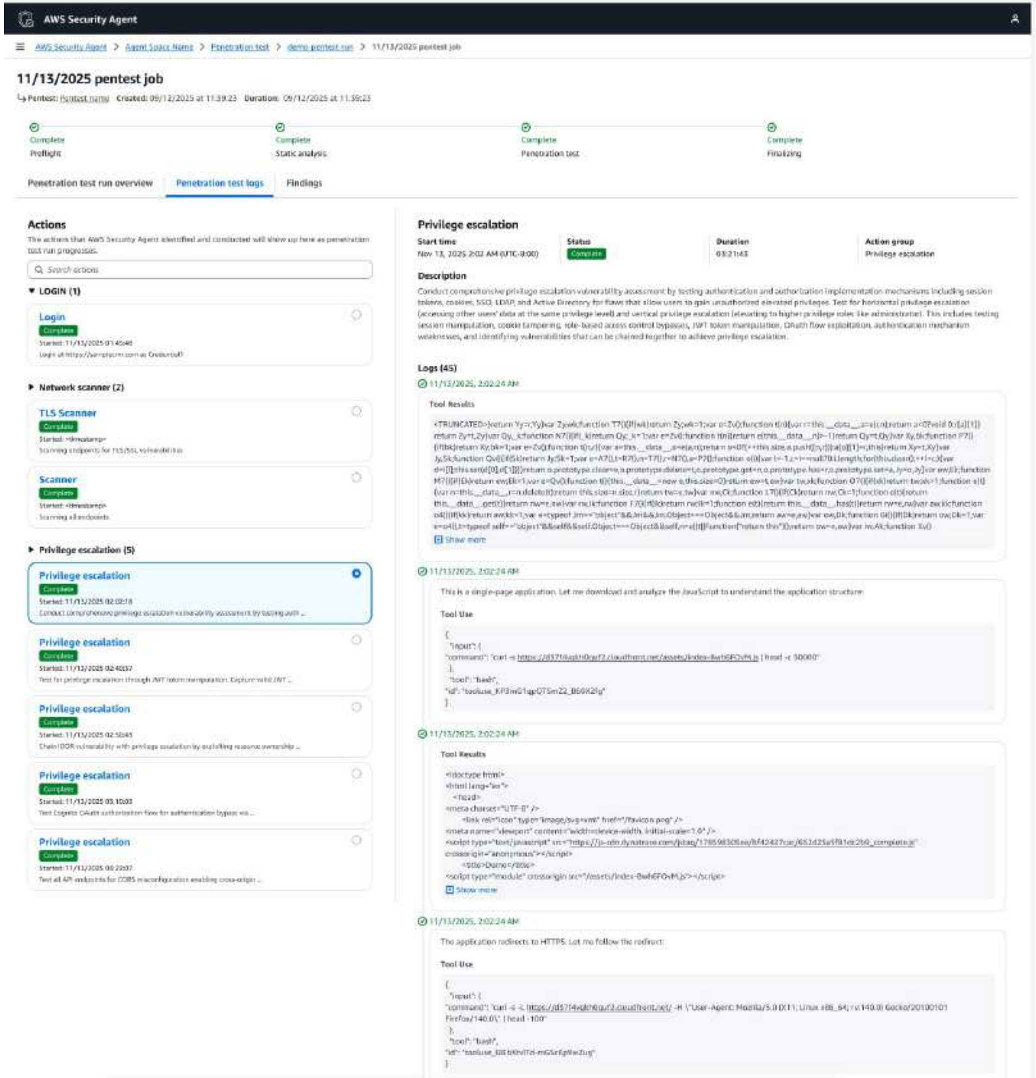
Additional allowed URLs - optional

Add URLs that are allowed in the network but not targets for penetration test. For example, URLs required for log-in.

Placeholder

Custom HTTP headers - optional

Custom HTTP headers to include in outbound network requests. By default, requests will include 'User-Agent: pentest-ai-agent' unless overridden by adding a custom User-Agent header.



AWS Security Agent
AWS Security Agent > Agent Space Name > Penetration test > demo pentest run > 11/13/2025 pentest job

11/13/2025 pentest job

Pentest: Pentest name **Created:** 09/12/2025 at 11:39:23 **Duration:** 09/12/2025 at 11:39:23

Actions

The actions that AWS Security Agent identified and conducted will show up here as penetration test run progresses.

LOGIN (1)

Login
Complete
Started: 11/13/2025 01:45:48
Login at https://samplecrm.com as Credential1

Network scanner (2)

TLS Scanner
Complete
Started: <timestamp>
Scanning endpoints for TLS/SSL vulnerabilities

Scanner
Complete
Started: <timestamp>
Scanning all endpoints

Privilege escalation (5)

Privilege escalation ●
Complete
Started: 11/13/2025 02:02:18
Conduct comprehensive privilege escalation vulnerability assessment by testing auth ...

Privilege escalation ○
Complete
Started: 11/13/2025 02:40:57
Test for privilege escalation through JWT token manipulation. Capture valid JWT ...

Privilege escalation ○
Complete
Started: 11/13/2025 02:52:45
Chain IDOR vulnerability with privilege escalation by exploiting resource ownership ...

Privilege escalation ○
Complete
Started: 11/13/2025 03:10:03
Test Cognito OAuth authorization flow for authentication bypass via ...

Privilege escalation ○
Complete
Started: 11/13/2025 03:22:07
Test all API endpoints for CORS misconfiguration enabling cross-origin ...

Privilege escalation

Start time	Status	Duration	Action group
Nov 13, 2025 2:02 AM (UTC-8:00)	Complete	03:21:45	Privilege escalation

Description

Conduct comprehensive privilege escalation vulnerability assessment by testing authentication and authorization implementation mechanisms including session tokens, cookies, SSO, LDAP, and Active Directory for flaws that allow users to gain unauthorized elevated privileges. Test for horizontal privilege escalation (accessing other users' data at the same privilege level) and vertical privilege escalation (elevating to higher privilege roles like administrator). This includes testing session manipulation, cookie tampering, role-based access control bypasses, JWT token manipulation, OAuth flow exploitation, authentication mechanism weaknesses, and identifying vulnerabilities that can be chained together to achieve privilege escalation.

Logs (45)

11/13/2025, 2:02:24 AM

Tool Results

11/13/2025, 2:02:24 AM

This is a single-page application. Let me download and analyze the JavaScript to understand the application structure.

Tool Use

```
{
 "input": {
"command": "curl -s https://d57f4vqkh0guf2.cloudfront.net/assets/index-BwhGFOvM.js | head -c 50000"
 },
 "tool": "bash",
"id": "tooluse_KP3mG1qpQTSm22_B60R2fg"
}
```

11/13/2025, 2:02:24 AM

Tool Results

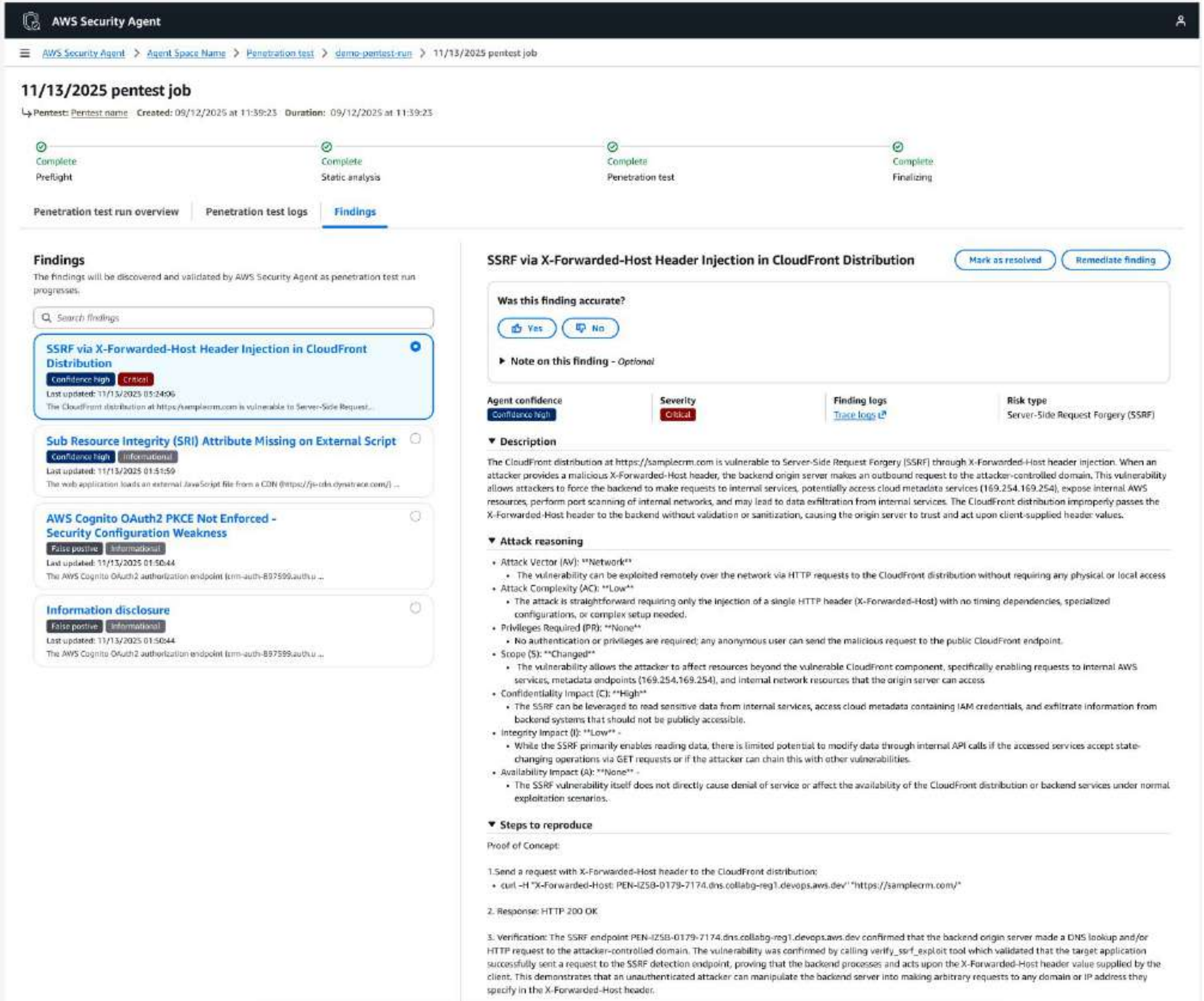
```
<!doctype html>
<html lang="en">
  <head>
<meta charset="UTF-8" />
    <link rel="icon" type="image/svg+xml" href="/favicon.png" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />
<script type="text/javascript" src="https://js-cdn.dynatrace.com/jstag/1765983056e/bf42427cac/652d25a5f81dc2b9_complete.js"
crossorigin="anonymous"></script>
    <title>Demo</title>
<script type="module" crossorigin src="/assets/index-BwhGFOvM.js"></script>
```

11/13/2025, 2:02:24 AM

The application redirects to HTTPS. Let me follow the redirect:

Tool Use

```
{
 "input": {
"command": "curl -s -L https://d57f4vqkh0guf2.cloudfront.net/ -H \"User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
Firefox/140.0\" | head -100"
 },
 "tool": "bash",
"id": "tooluse_l0EbKrvlTd-mGSeEgNwZug"
}
```


AWS Security Agent
AWS Security Agent > Agent Space Name > Penetration test > demo-pentest-run > 11/13/2025 pentest job

11/13/2025 pentest job

Pentest: Pentest name **Created:** 09/12/2025 at 11:39:23 **Duration:** 09/12/2025 at 11:39:23

Findings

The findings will be discovered and validated by AWS Security Agent as penetration test run progresses.

● **SSRF via X-Forwarded-Host Header Injection in CloudFront Distribution**
Confidence high Critical
Last updated: 11/13/2025 03:24:06
The CloudFront distribution at https://samplecrm.com is vulnerable to Server-Side Request...

○ **Sub Resource Integrity (SRI) Attribute Missing on External Script**
Confidence high Informational
Last updated: 11/13/2025 01:51:59
The web application loads an external JavaScript file from a CDN (https://js-cdn.dynatrace.com/) ...

○ **AWS Cognito OAuth2 PKCE Not Enforced - Security Configuration Weakness**
False postive Informational
Last updated: 11/13/2025 01:50:44
The AWS Cognito OAuth2 authorization endpoint (crm-auth-897599.auth.u ...

○ **Information disclosure**
False postive Informational
Last updated: 11/13/2025 01:50:44
The AWS Cognito OAuth2 authorization endpoint (crm-auth-897599.auth.u ...

SSRF via X-Forwarded-Host Header Injection in CloudFront Distribution

Was this finding accurate?

▶ **Note on this finding** - *Optional*

Agent confidence	**Severity**	**Finding logs**	**Risk type**
Confidence high	Critical	Trace logs	Server-Side Request Forgery (SSRF)

▼ **Description**

The CloudFront distribution at https://samplecrm.com is vulnerable to Server-Side Request Forgery (SSRF) through X-Forwarded-Host header injection. When an attacker provides a malicious X-Forwarded-Host header, the backend origin server makes an outbound request to the attacker-controlled domain. This vulnerability allows attackers to force the backend to make requests to internal services, potentially access cloud metadata services (169.254.169.254), expose internal AWS resources, perform port scanning of internal networks, and may lead to data exfiltration from internal services. The CloudFront distribution improperly passes the X-Forwarded-Host header to the backend without validation or sanitization, causing the origin server to trust and act upon client-supplied header values.

▼ **Attack reasoning**

- Attack Vector (AV): **Network**
  - The vulnerability can be exploited remotely over the network via HTTP requests to the CloudFront distribution without requiring any physical or local access
- Attack Complexity (AC): **Low**
  - The attack is straightforward requiring only the injection of a single HTTP header (X-Forwarded-Host) with no timing dependencies, specialized configurations, or complex setup needed.
- Privileges Required (PR): **None**
  - No authentication or privileges are required; any anonymous user can send the malicious request to the public CloudFront endpoint.
- Scope (S): **Changed**
  - The vulnerability allows the attacker to affect resources beyond the vulnerable CloudFront component, specifically enabling requests to internal AWS services, metadata endpoints (169.254.169.254), and internal network resources that the origin server can access
- Confidentiality Impact (C): **High**
  - The SSRF can be leveraged to read sensitive data from internal services, access cloud metadata containing IAM credentials, and exfiltrate information from backend systems that should not be publicly accessible.
- Integrity Impact (I): **Low** -
  - While the SSRF primarily enables reading data, there is limited potential to modify data through internal API calls if the accessed services accept state-changing operations via GET requests or if the attacker can chain this with other vulnerabilities.
- Availability Impact (A): **None** -
  - The SSRF vulnerability itself does not directly cause denial of service or affect the availability of the CloudFront distribution or backend services under normal exploitation scenarios.

▼ **Steps to reproduce**

Proof of Concept:

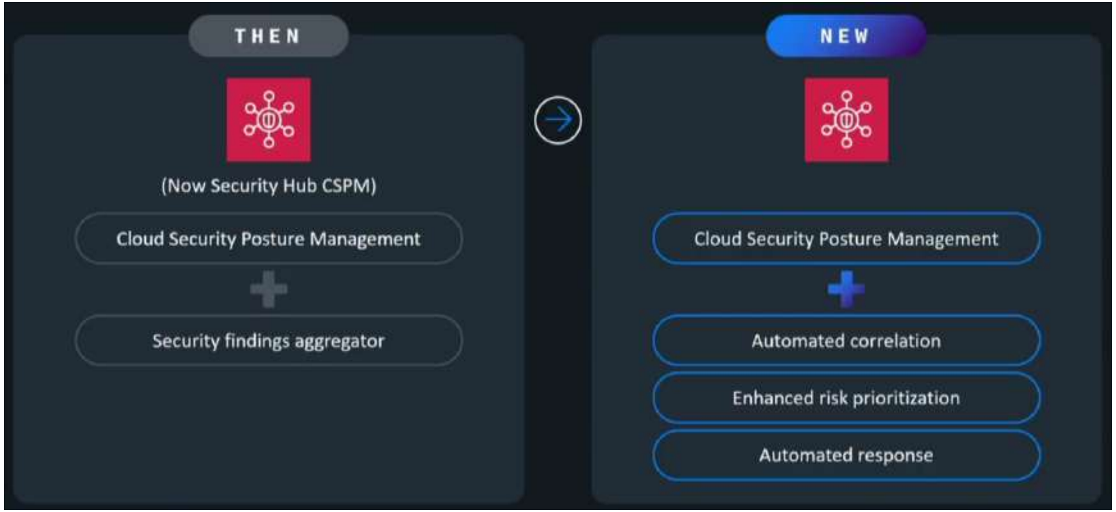
1.Send a request with X-Forwarded-Host header to the CloudFront distribution:
- curl -H "X-Forwarded-Host: PEN-IZ5B-0179-7174.dns.collabg-reg1.devops.aws.dev" "https://samplecrm.com/"

2. Response: HTTP 200 OK

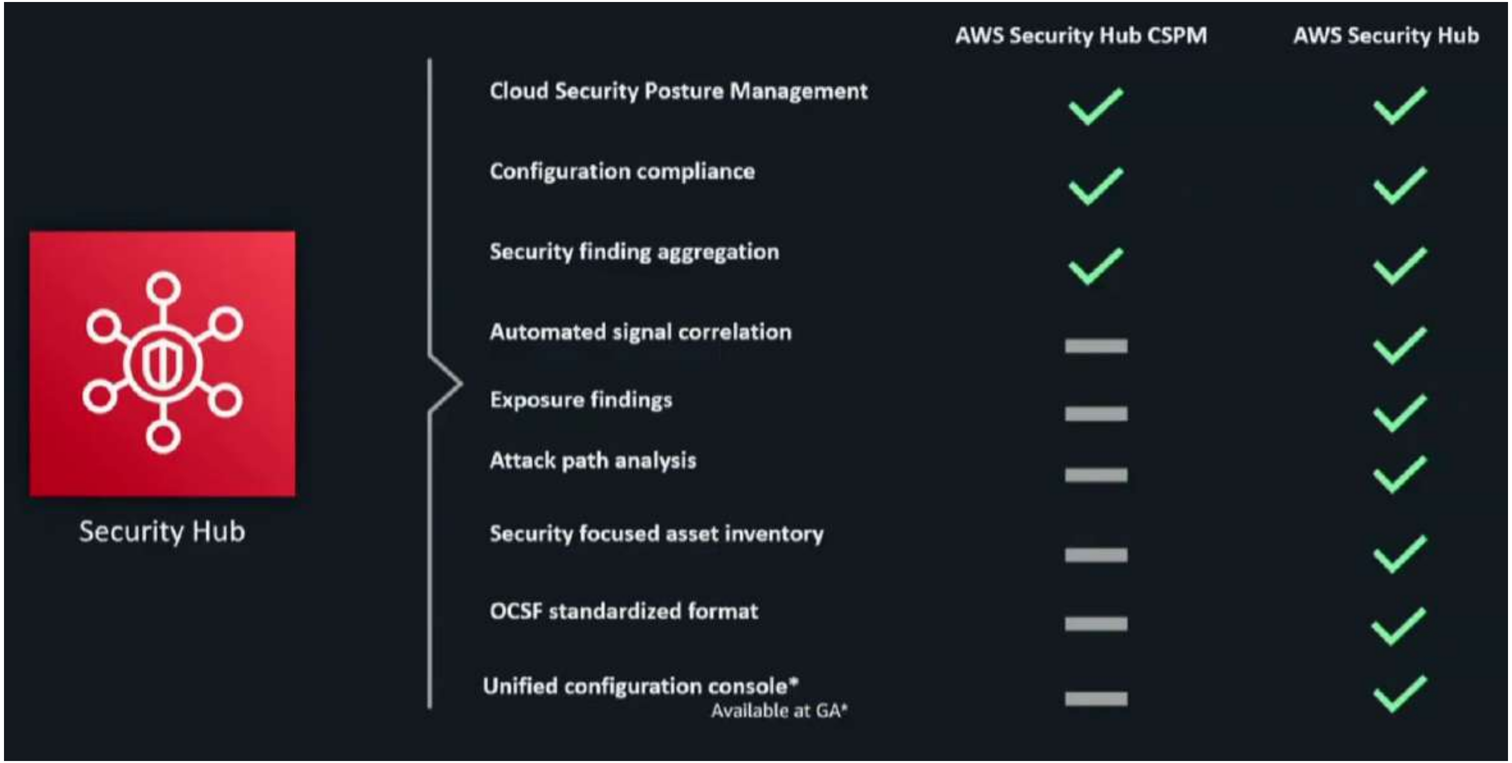
3. Verification: The SSRF endpoint PEN-IZ5B-0179-7174.dns.collabg-reg1.devops.aws.dev confirmed that the backend origin server made a DNS lookup and/or HTTP request to the attacker-controlled domain. The vulnerability was confirmed by calling verify_ssrf_exploit tool which validated that the target application successfully sent a request to the SSRF detection endpoint, proving that the backend processes and acts upon the X-Forwarded-Host header value supplied by the client. This demonstrates that an unauthenticated attacker can manipulate the backend server into making arbitrary requests to any domain or IP address they specify in the X-Forwarded-Host header.

AWS Security Hub (General Availability)

Security Hub는 완전 관리형 통합 보안 운영 서비스로 발전하여, 여러 AWS 보안 서비스와 파트너 도구의 탐지 결과를 하나의 중앙화된 뷰로 통합합니다. AI/ML 기반 준실시간 위협 상관관계 분석, 노출(Exposure) 탐지 및 공격 경로 시각화, 간소화된 다중 계정/리전 활성화, 지라(등) 연동 동 그리고 통합 가격 정책(GuardDuty, Inspector, Security Hub 통합)이 있습니다.

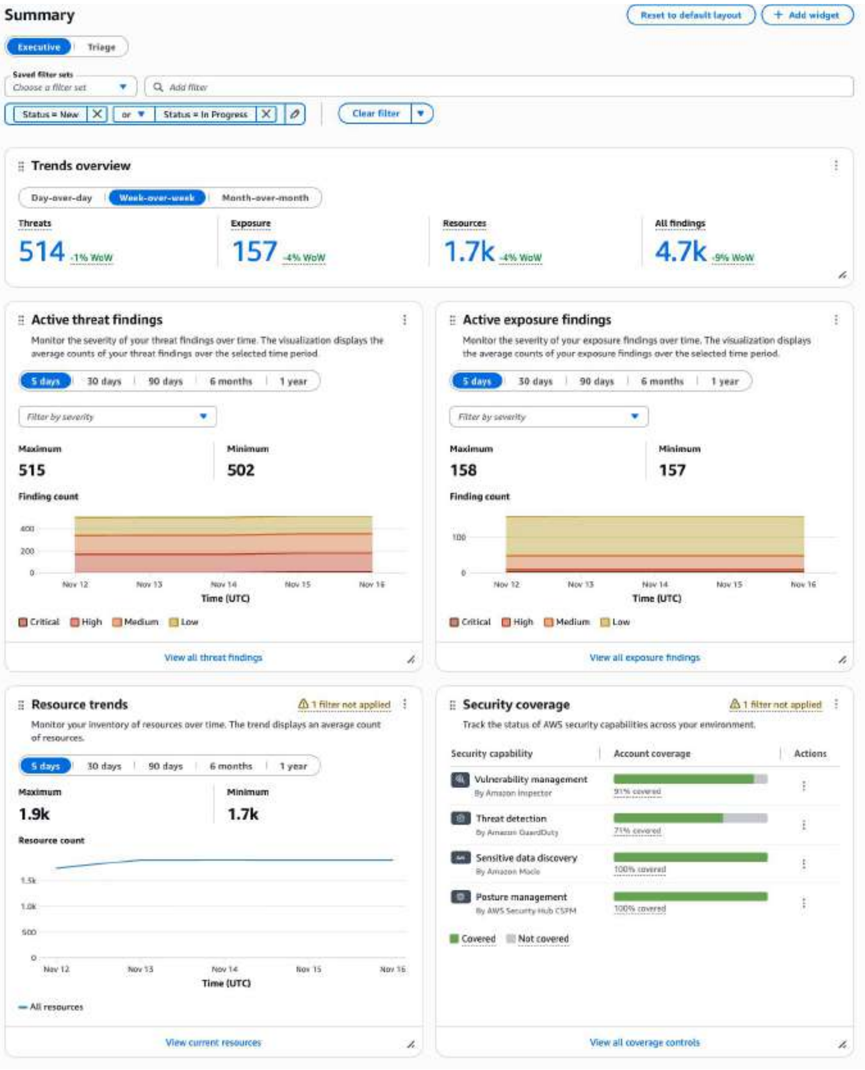

THEN
(Now Security Hub CSPM)
Cloud Security Posture Management
Security findings aggregator
NEW
Cloud Security Posture Management
Automated correlation
Enhanced risk prioritization
Automated response

영상: https://www.youtube.com/watch?v=mYyBQYIeJzk



Security Hub

	AWS Security Hub CSPM	AWS Security Hub
Cloud Security Posture Management	✓	✓
Configuration compliance	✓	✓
Security finding aggregation	✓	✓
Automated signal correlation	—	✓
Exposure findings	—	✓
Attack path analysis	—	✓
Security focused asset inventory	—	✓
OCSF standardized format	—	✓
Unified configuration console* Available at GA*	—	✓



Summary

Saved filter sets

Status = New or Status = In Progress

Trends overview

Day-over-day | Week-over-week | Month-over-month

Threats	Exposure	Resources	All findings
514 -1% WoW	157 -4% WoW	1.7k -4% WoW	4.7k -9% WoW

Active threat findings

Monitor the severity of your threat findings over time. The visualization displays the average counts of your threat findings over the selected time period.

5 days | 30 days | 90 days | 6 months | 1 year

Filter by severity

Maximum	Minimum
515	502

View all threat findings

Active exposure findings

Monitor the severity of your exposure findings over time. The visualization displays the average counts of your exposure findings over the selected time period.

5 days | 30 days | 90 days | 6 months | 1 year

Filter by severity

Maximum	Minimum
158	157

View all exposure findings

Resource trends

⚠ 1 filter not applied

Monitor your inventory of resources over time. The trend displays an average count of resources.

5 days | 30 days | 90 days | 6 months | 1 year

Maximum	Minimum
1.9k	1.7k

View current resources

Security coverage

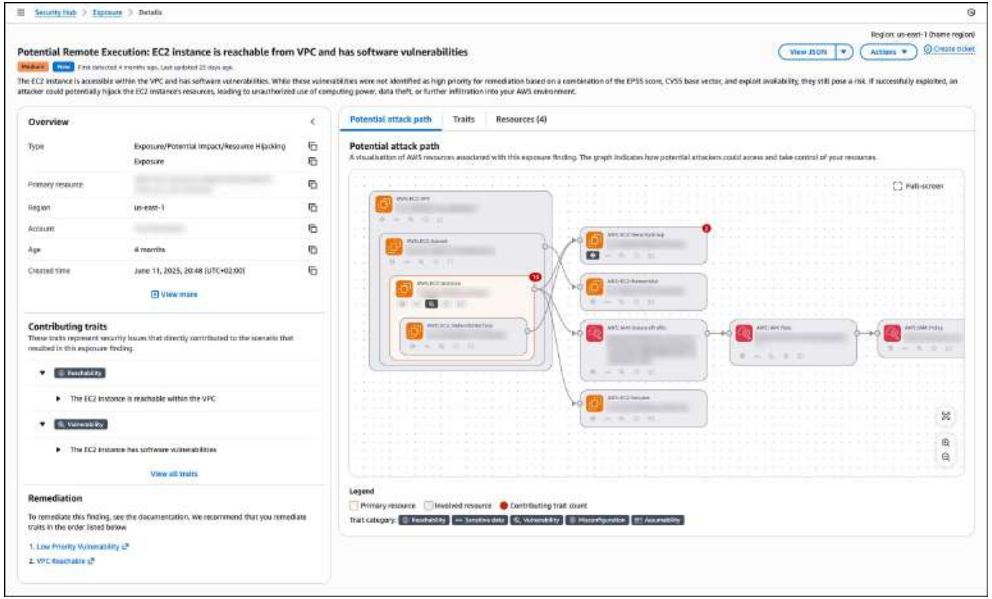
⚠ 1 filter not applied

Track the status of AWS security capabilities across your environment.

Security capability	Account coverage	Actions
Vulnerability management By Amazon Inspector	91% covered	⋮
Threat detection By Amazon GuardDuty	71% covered	⋮
Sensitive data discovery By Amazon Macie	100% covered	⋮
Posture management By AWS Security Hub CSPM	100% covered	⋮

🟩 Covered ▨ Not covered

View all coverage controls



Potential Remote Execution: EC2 instance is reachable from VPC and has software vulnerabilities

Medium New First detected 4 months ago. Last updated 22 days ago.

The EC2 instance is accessible within the VPC and has software vulnerabilities. While these vulnerabilities were not identified as high priority for remediation based on a combination of the EPSS score, CVSS base vector, and exploit availability, they still pose a risk. If successfully exploited, an attacker could potentially hijack the EC2 instance's resources, leading to unauthorized use of computing power, data theft, or further infiltration into your AWS environment.

Overview

Type	Exposure/Potential Impact/Resource Hijacking Exposure
Primary resource	
Region	us-east-1
Account	
Age	4 months
Created time	June 11, 2025, 20:48 (UTC+02:00)

View more

Contributing traits

These traits represent security issues that directly contributed to the scenario that resulted in this exposure finding.

- Reachability
  - The EC2 instance is reachable within the VPC
- Vulnerability
  - The EC2 instance has software vulnerabilities

View all traits

Remediation

To remediate this finding, see the documentation. We recommend that you remediate traits in the order listed below.

1. Low Priority Vulnerability
2. VPC Reachable

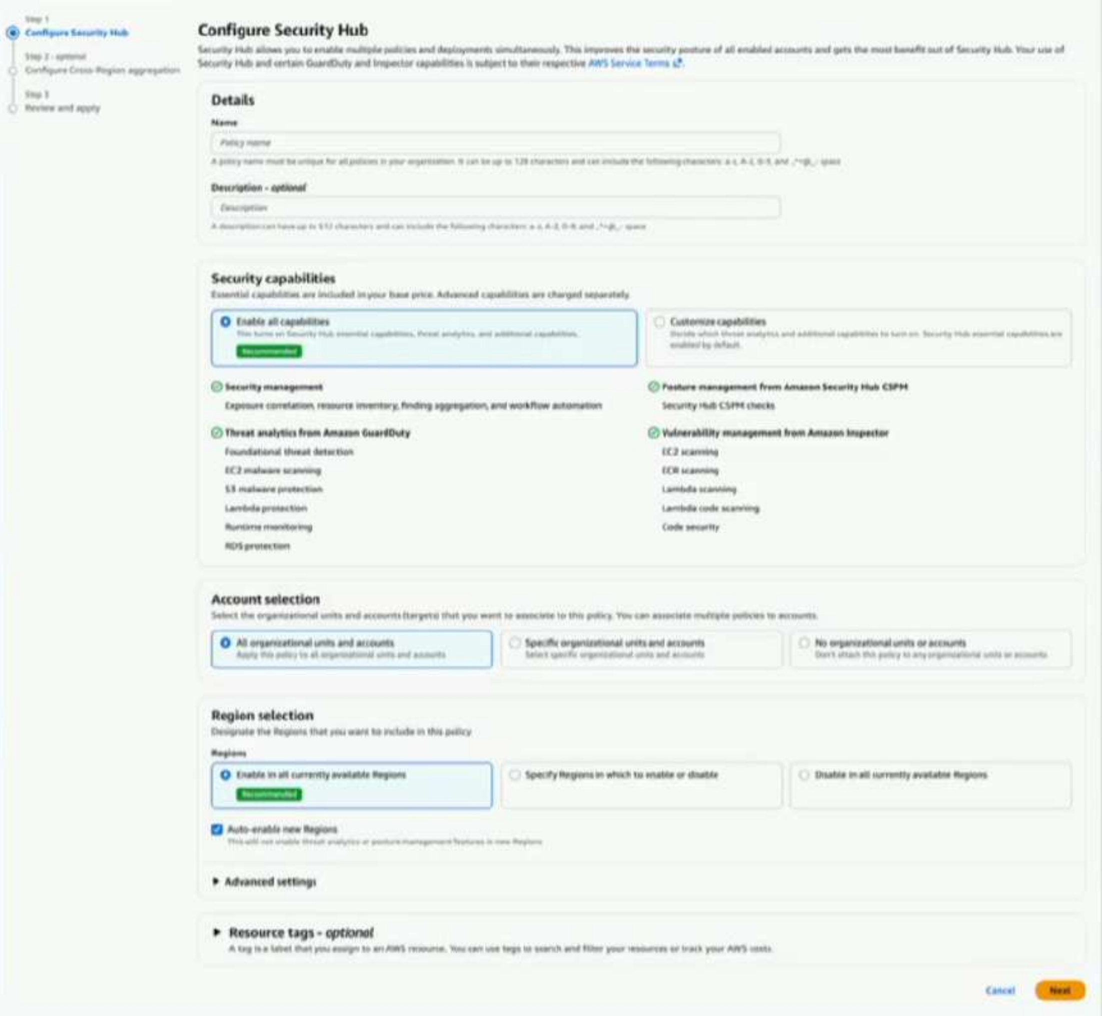
Potential attack path

A visualization of AWS resources associated with this exposure finding. The graph indicates how potential attackers could access and take control of your resources.

Legend

☐ Primary resource ☐ Involved resource ● Contributing trait count

Trait category: Reachability | Sensitive data | Vulnerability | Misconfiguration | Assumability



Configure Security Hub

Security Hub allows you to enable multiple policies and deployments simultaneously. This improves the security posture of all enabled accounts and gets the most benefit out of Security Hub. Your use of Security Hub and certain GuardDuty and Inspector capabilities is subject to their respective AWS Service Terms.

Details

Name

Policy name

A policy name must be unique for all policies in your organization. It can be up to 128 characters and can include the following characters: a-z, A-Z, 0-9, and .:+=@_/- space

Description - *optional*

Description

A description can have up to 512 characters and can include the following characters: a-z, A-Z, 0-9, and .:+=@_/- space

Security capabilities

Essential capabilities are included in your base price. Advanced capabilities are charged separately.

● Enable all capabilities
This turns on Security Hub essential capabilities, threat analytics, and additional capabilities.
Recommended

○ Customize capabilities
Decide which threat analytics and additional capabilities to turn on. Security Hub essential capabilities are enabled by default.

✓ **Security management**
Exposure correlation, resource inventory, finding aggregation, and workflow automation

✓ **Threat analytics from Amazon GuardDuty**
Foundational threat detection
EC2 malware scanning
S3 malware protection
Lambda protection
Runtime monitoring
RDS protection

✓ **Posture management from Amazon Security Hub CSPM**
Security Hub CSPM checks

✓ **Vulnerability management from Amazon Inspector**
EC2 scanning
ECR scanning
Lambda scanning
Lambda code scanning
Code security

Account selection

Select the organizational units and accounts (targets) that you want to associate to this policy. You can associate multiple policies to accounts.

● All organizational units and accounts
Apply this policy to all organizational units and accounts

○ Specific organizational units and accounts
Select specific organizational units and accounts

○ No organizational units or accounts
Don't attach this policy to any organizational units or accounts.

Region selection

Designate the Regions that you want to include in this policy

Regions

● Enable in all currently available Regions
Recommended

○ Specify Regions in which to enable or disable

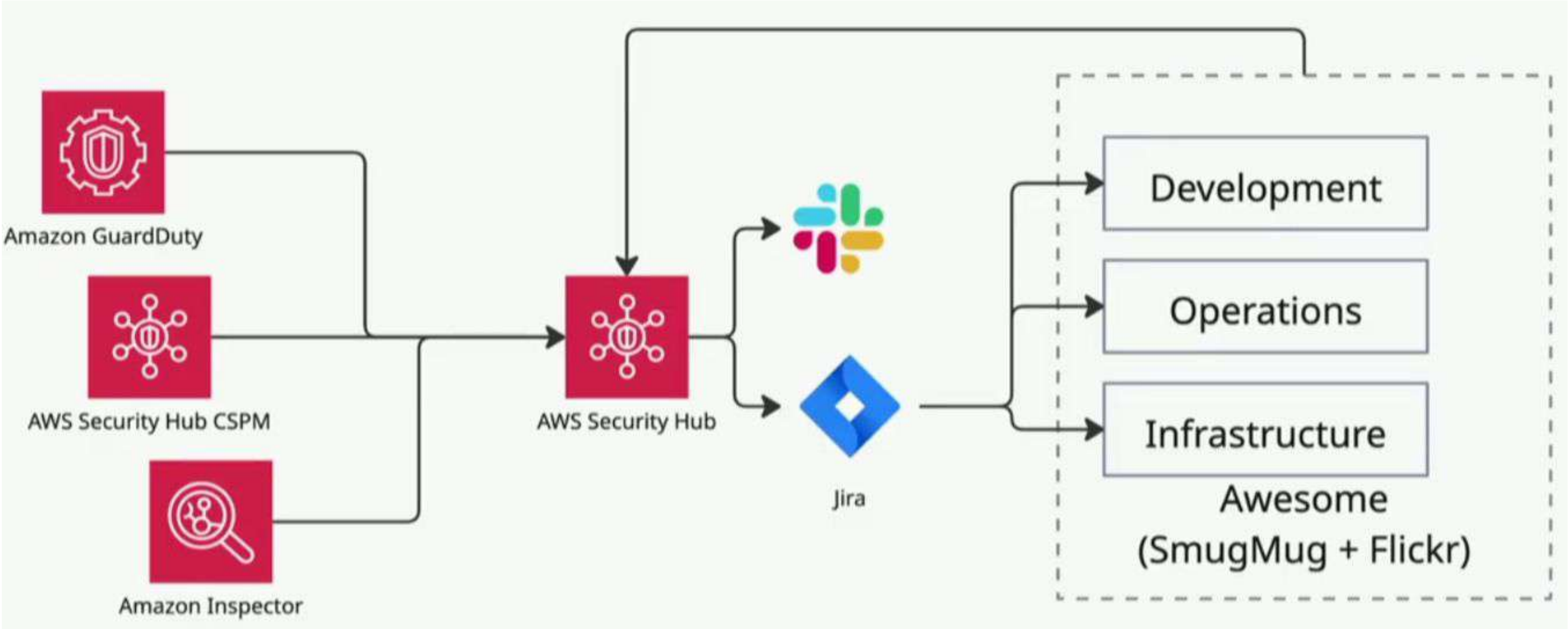
○ Disable in all currently available Regions

☑ Auto-enable new Regions
This will not enable threat analytics or posture management features in new Regions

▸ **Advanced settings**

▸ Resource tags - *optional*

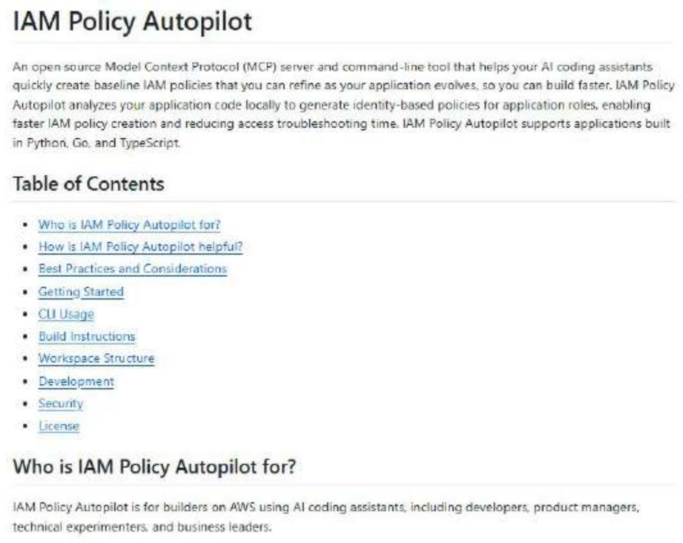
A tag is a label that you assign to an AWS resource. You can use tags to search and filter your resources or track your AWS costs.



Amazon GuardDuty
AWS Security Hub CSPM
Amazon Inspector
AWS Security Hub
Jira
Development
Operations
Infrastructure
Awesome
(SmugMug + Flickr)

IAM Policy Autopilot

IAM Policy Autopilot은 도구는 정적 코드 분석을 통해 개발자의 코드에서 필요한 IAM 권한을 자동으로 생성하는 CLI 도구이자 MCP 서버입니다. IAM Policy Autopilot은 결정론적(deterministic, 같은 결과를 출력력)이고 최신 상태를 유지하며 신뢰할 수 있는 정책 생성을 제공하여, 내부 데이터 분석 결과 기존 개발자 정책 대비 97% 적은 권한만을 부여하면서도 필요한



IAM Policy Autopilot

An open source Model Context Protocol (MCP) server and command-line tool that helps your AI coding assistants quickly create baseline IAM policies that you can refine as your application evolves, so you can build faster. IAM Policy Autopilot analyzes your application code locally to generate identity-based policies for application roles, enabling faster IAM policy creation and reducing access troubleshooting time. IAM Policy Autopilot supports applications built in Python, Go, and TypeScript.

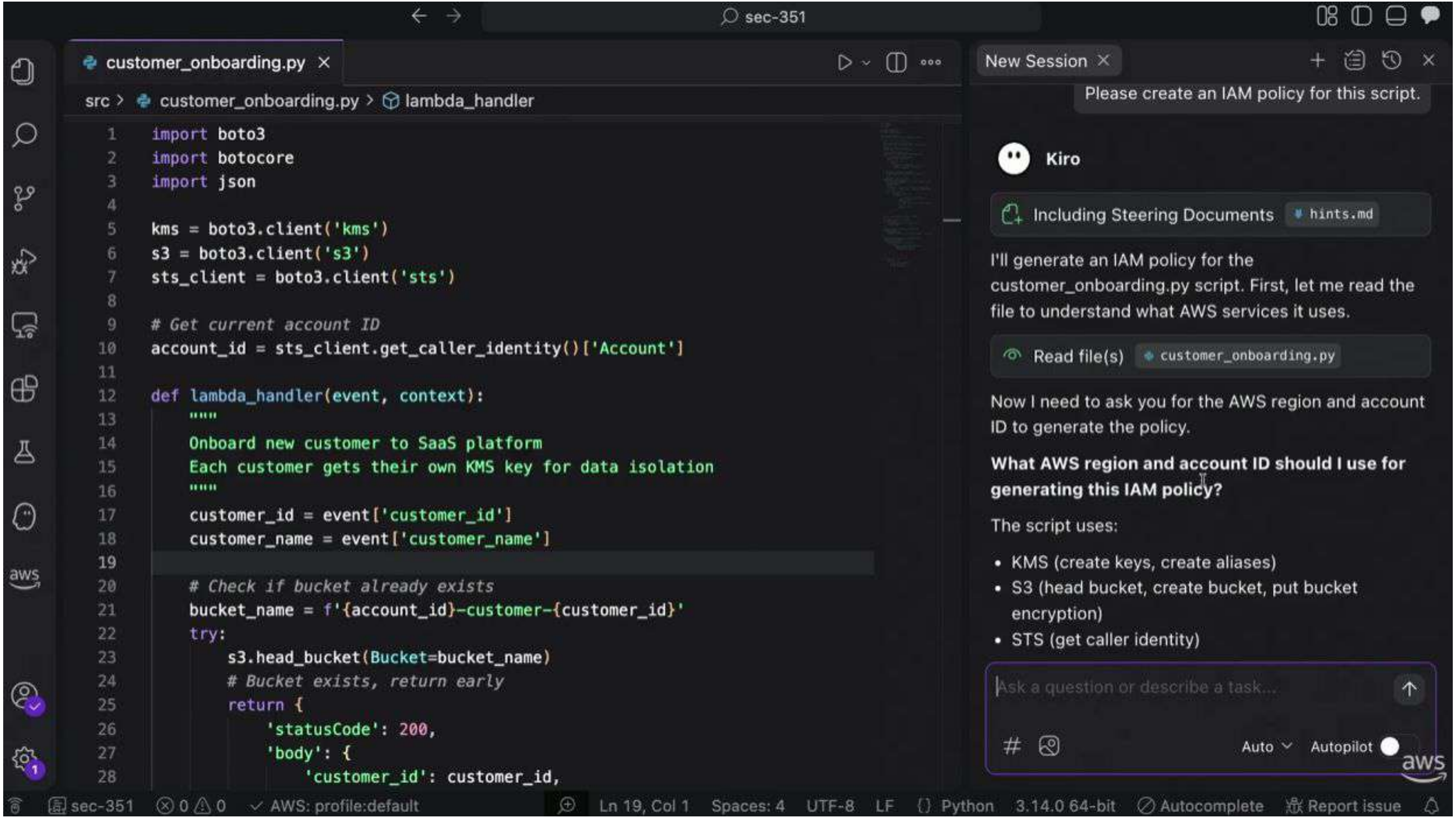
Table of Contents

- Who is IAM Policy Autopilot for?
- How is IAM Policy Autopilot helpful?
- Best Practices and Considerations
- Getting Started
- CLI Usage
- Build Instructions
- Workspace Structure
- Development
- Security
- License

Who is IAM Policy Autopilot for?

IAM Policy Autopilot is for builders on AWS using AI coding assistants, including developers, product managers, technical experimenters, and business leaders.

영상: https://www.youtube.com/watch?v=vgA_sq99Kas



```
import boto3
import botocore
import json

kms = boto3.client('kms')
s3 = boto3.client('s3')
sts_client = boto3.client('sts')

# Get current account ID
account_id = sts_client.get_caller_identity()['Account']

def lambda_handler(event, context):
    """
    Onboard new customer to SaaS platform
    Each customer gets their own KMS key for data isolation
    """
    customer_id = event['customer_id']
    customer_name = event['customer_name']

    # Check if bucket already exists
    bucket_name = f'{account_id}-customer-{customer_id}'
    try:
        s3.head_bucket(Bucket=bucket_name)
        # Bucket exists, return early
        return {
            'statusCode': 200,
            'body': {
                'customer_id': customer_id,
```

Please create an IAM policy for this script.

Kiro

Including Steering Documents `hints.md`

I'll generate an IAM policy for the customer_onboarding.py script. First, let me read the file to understand what AWS services it uses.

Read file(s) `customer_onboarding.py`

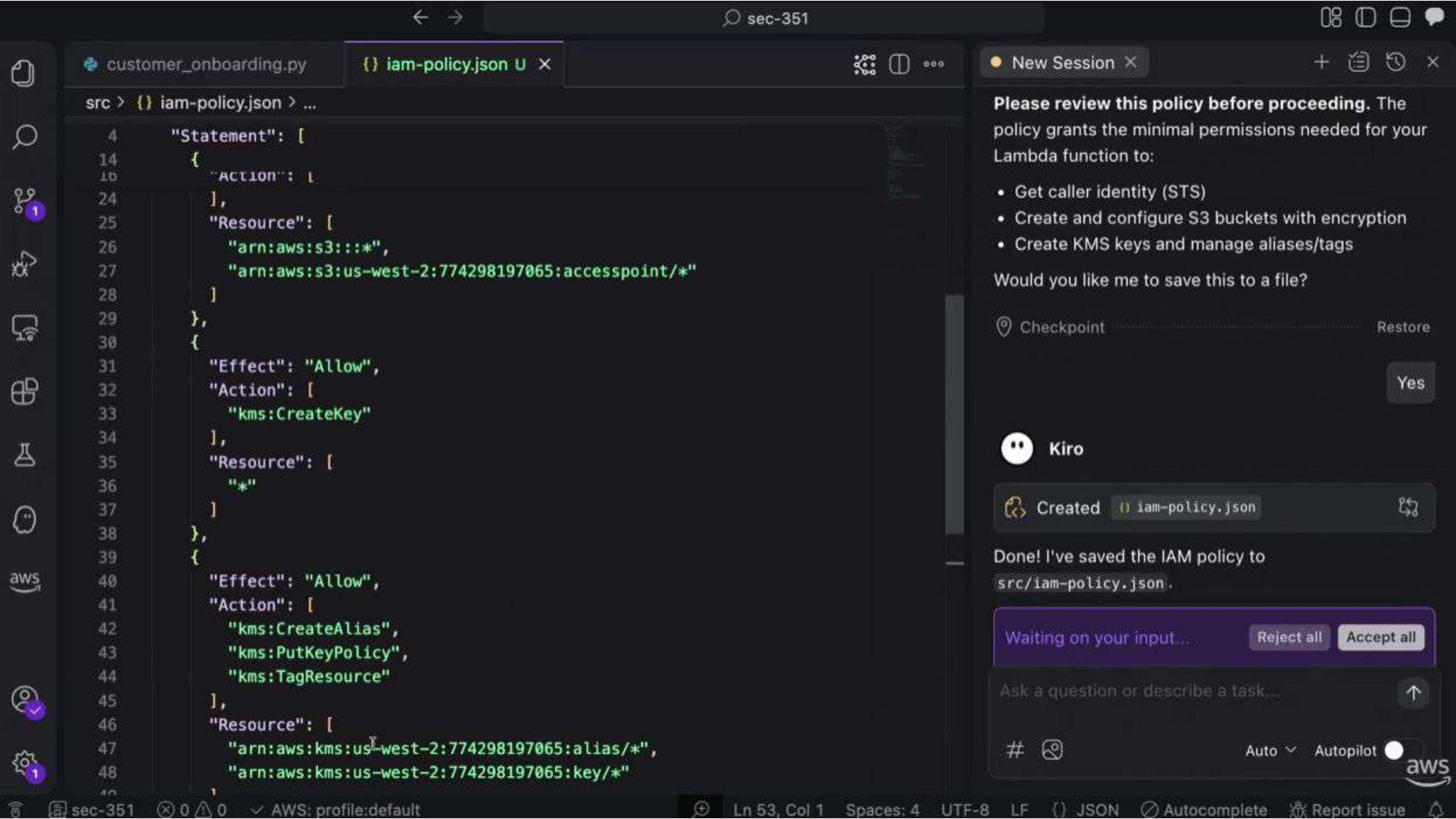
Now I need to ask you for the AWS region and account ID to generate the policy.

What AWS region and account ID should I use for generating this IAM policy?

The script uses:

- KMS (create keys, create aliases)
- S3 (head bucket, create bucket, put bucket encryption)
- STS (get caller identity)

Ask a question or describe a task...



```
    "Statement": [
      {
        "Action": [
        ],
        "Resource": [
          "arn:aws:s3:::*",
          "arn:aws:s3:us-west-2:774298197065:accesspoint/*"
        ]
      },
      {
        "Effect": "Allow",
        "Action": [
          "kms:CreateKey"
        ],
        "Resource": [
          "*"
        ]
      },
      {
        "Effect": "Allow",
        "Action": [
          "kms:CreateAlias",
          "kms:PutKeyPolicy",
          "kms:TagResource"
        ],
        "Resource": [
          "arn:aws:kms:us-west-2:774298197065:alias/*",
          "arn:aws:kms:us-west-2:774298197065:key/*"
```

Please review this policy before proceeding. The policy grants the minimal permissions needed for your Lambda function to:

- Get caller identity (STS)
- Create and configure S3 buckets with encryption
- Create KMS keys and manage aliases/tags

Would you like me to save this to a file?

Yes

Kiro

Created `iam-policy.json`

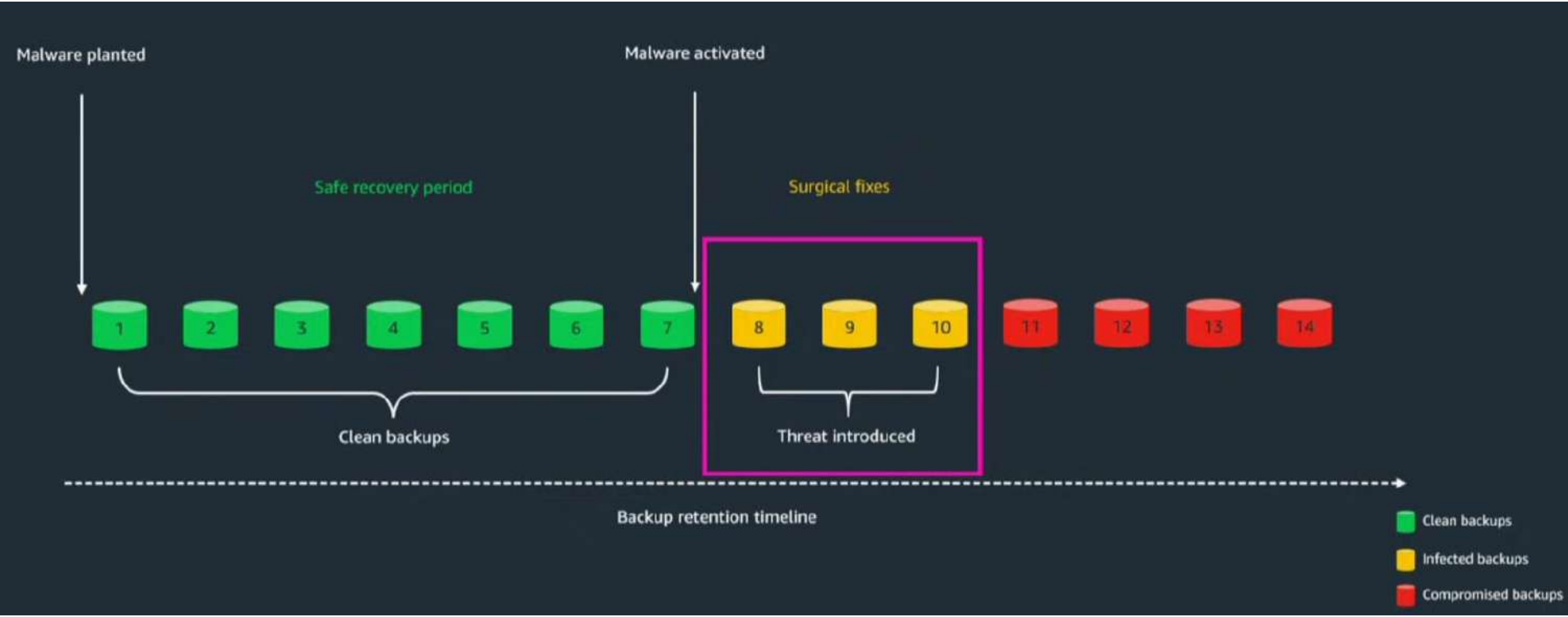
Done! I've saved the IAM policy to `src/iam-policy.json`.

GuardDuty Malware Protection for AWS Backup

GuardDuty는 완전 관리형 위협 탐지 서비스로, 수백만 개의 EC2 인스턴스와 S3 버킷을 모니터링합니다. 이제 EC2, S3를 넘어 AWS Backup에 대한 멀웨어 스캔 기능을 제공합니다.

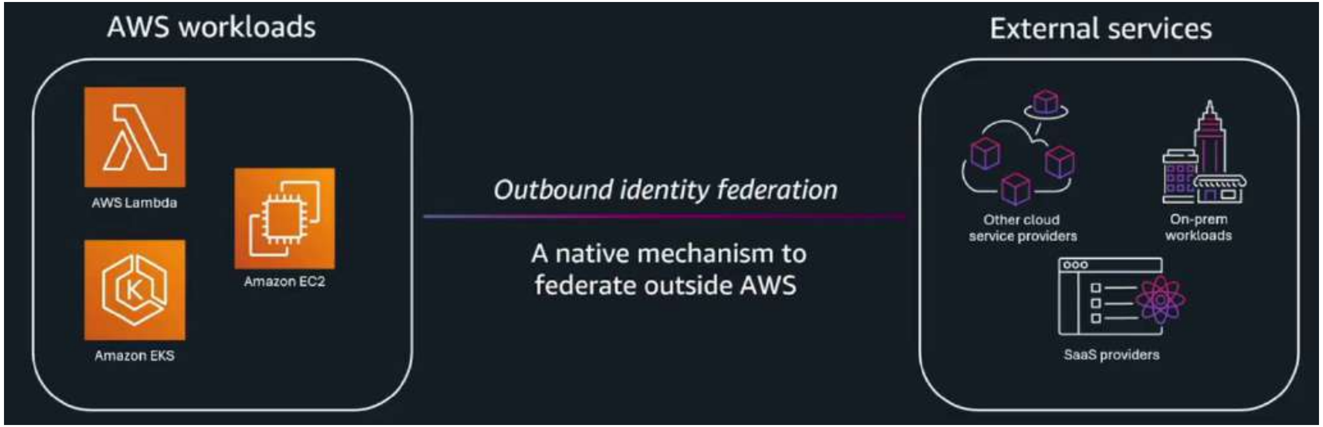
❤

영상: https://www.youtube.com/watch?v=E5p_WnP4pw8

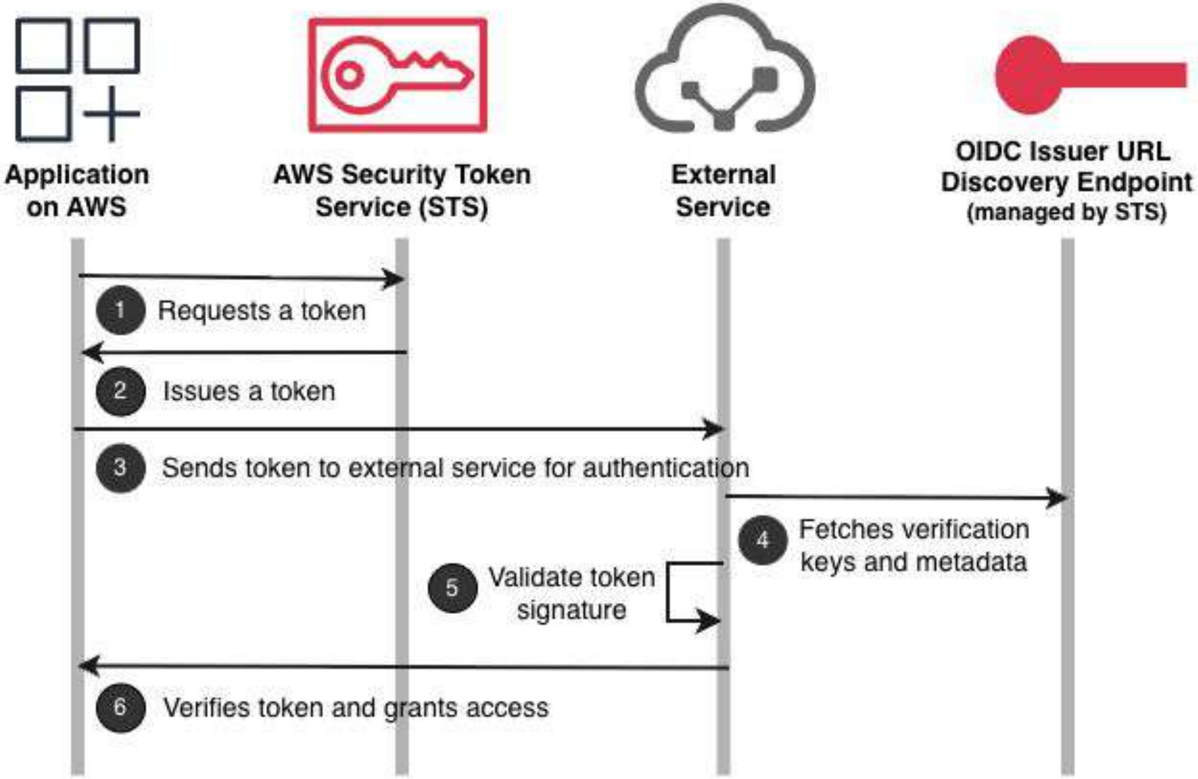

Malware planted
Malware activated
Safe recovery period
Surgical fixes
1
2
3
4
5
6
7
8
9
10
11
12
13
14
Clean backups
Threat introduced
Backup retention timeline
🟩 Clean backups
🟨 Infected backups
🟥 Compromised backups

AWS Outbound Identity Federation

외부 서비스의 장기 증명(api key, access token 등)을 관리하지 않아도 AWS 워크로드에서 외부 서비스의 권한을 위임 받아서 호출할 수 있습니다.

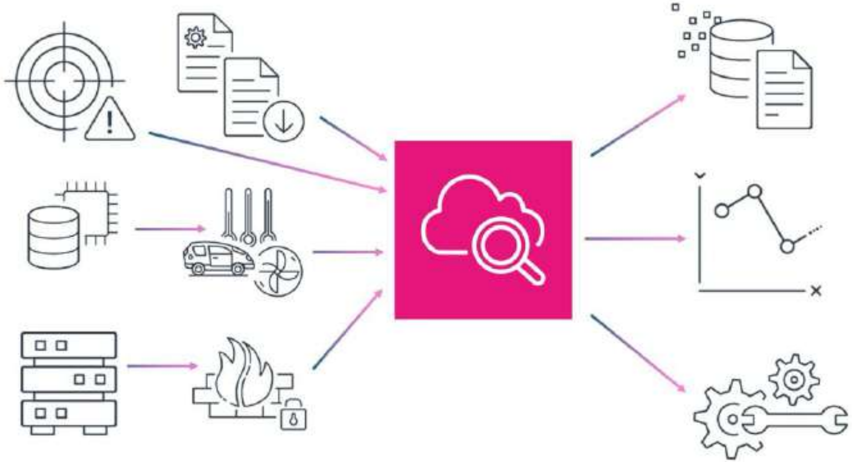

AWS workloads
AWS Lambda
Amazon EC2
Amazon EKS
Outbound identity federation
A native mechanism to federate outside AWS
External services
Other cloud service providers
On-prem workloads
SaaS providers

영상: https://www.youtube.com/watch?v=gkMnYCMJmBI

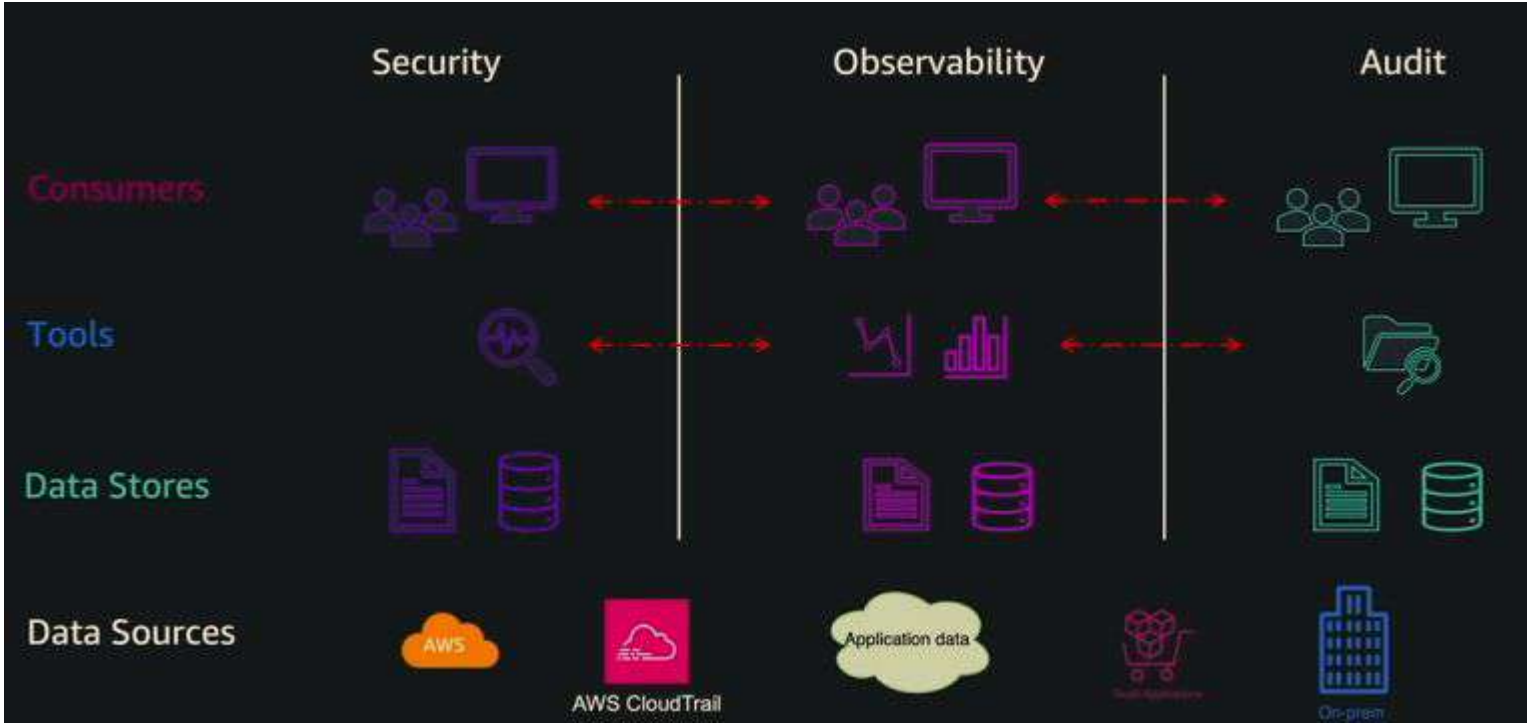

Application on AWS
AWS Security Token Service (STS)
External Service
OIDC Issuer URL Discovery Endpoint (managed by STS)
1 Requests a token
2 Issues a token
3 Sends token to external service for authentication
4 Fetches verification keys and metadata
5 Validate token signature
6 Verifies token and grants access

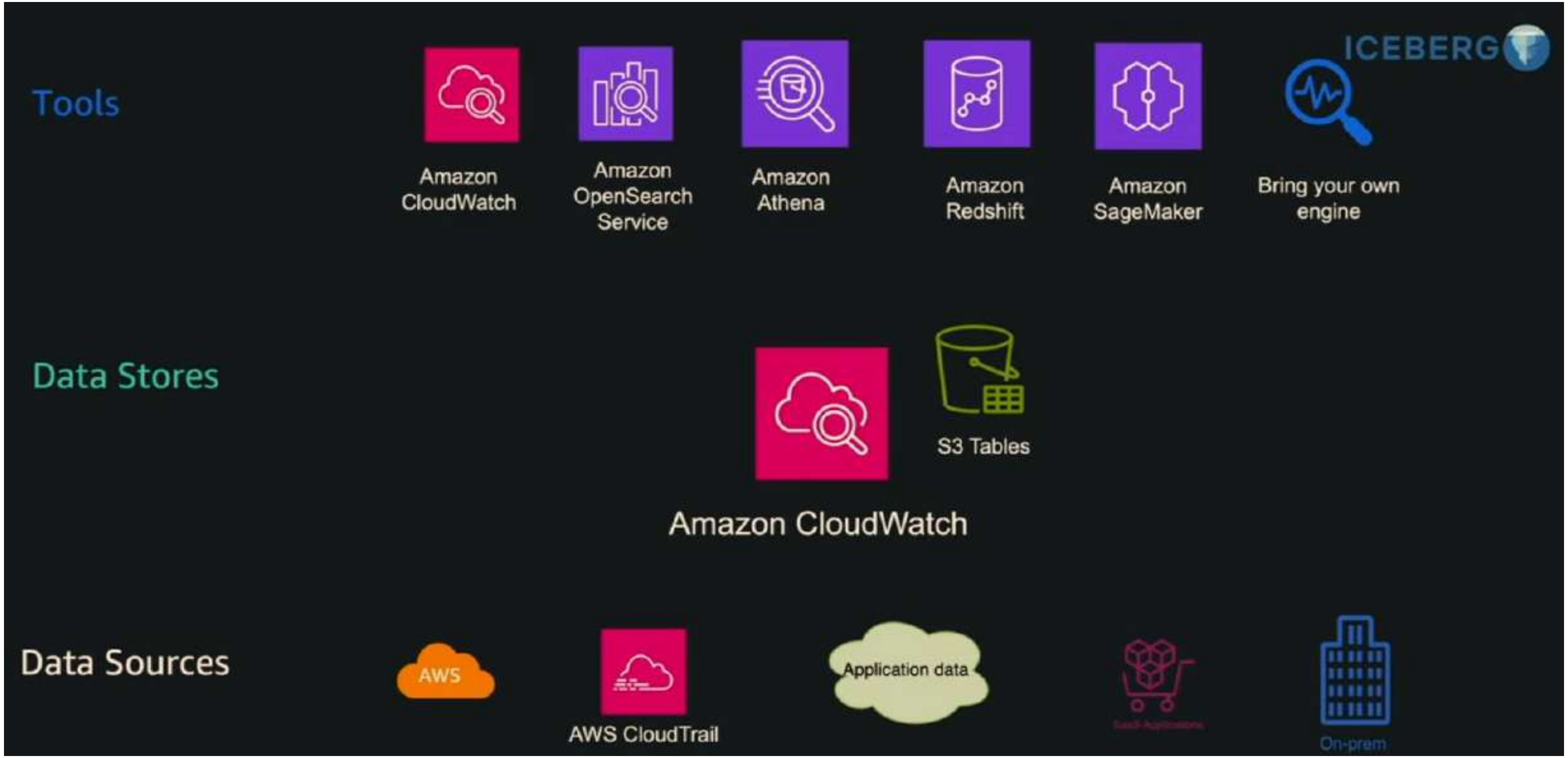
Amazon CloudWatch Unified Data Management

보안 팀, 감사 팀, DevOps 팀간의 데이터 수집 경계를 허물기 위해 로그 중앙화, S3 Tables 통합, 서드파티 커넥터, 그리고 강력한 분석 기능을 제공하는 관리형 서비스.



영상: https://www.youtube.com/watch?v=5-_I3MYJdLs


Security
Observability
Audit
Consumers
Tools
Data Stores
Data Sources
AWS
AWS CloudTrail
Application data
On-prem



ICEBERG

Tools

Amazon CloudWatch

Amazon OpenSearch Service

Amazon Athena

Amazon Redshift

Amazon SageMaker

Bring your own engine

Data Stores

Amazon CloudWatch

S3 Tables

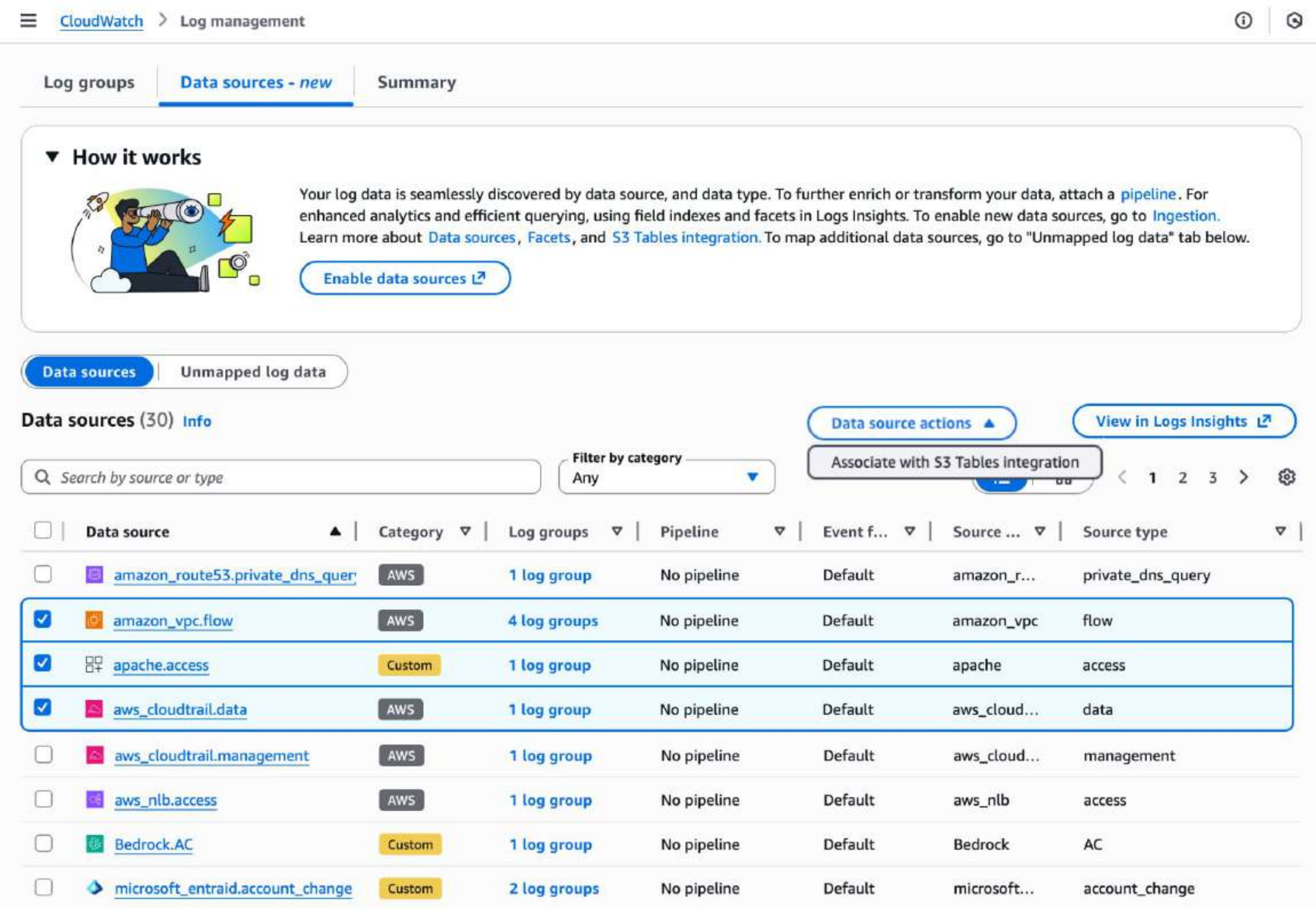
Data Sources

AWS CloudTrail

Application data

SaaS Applications

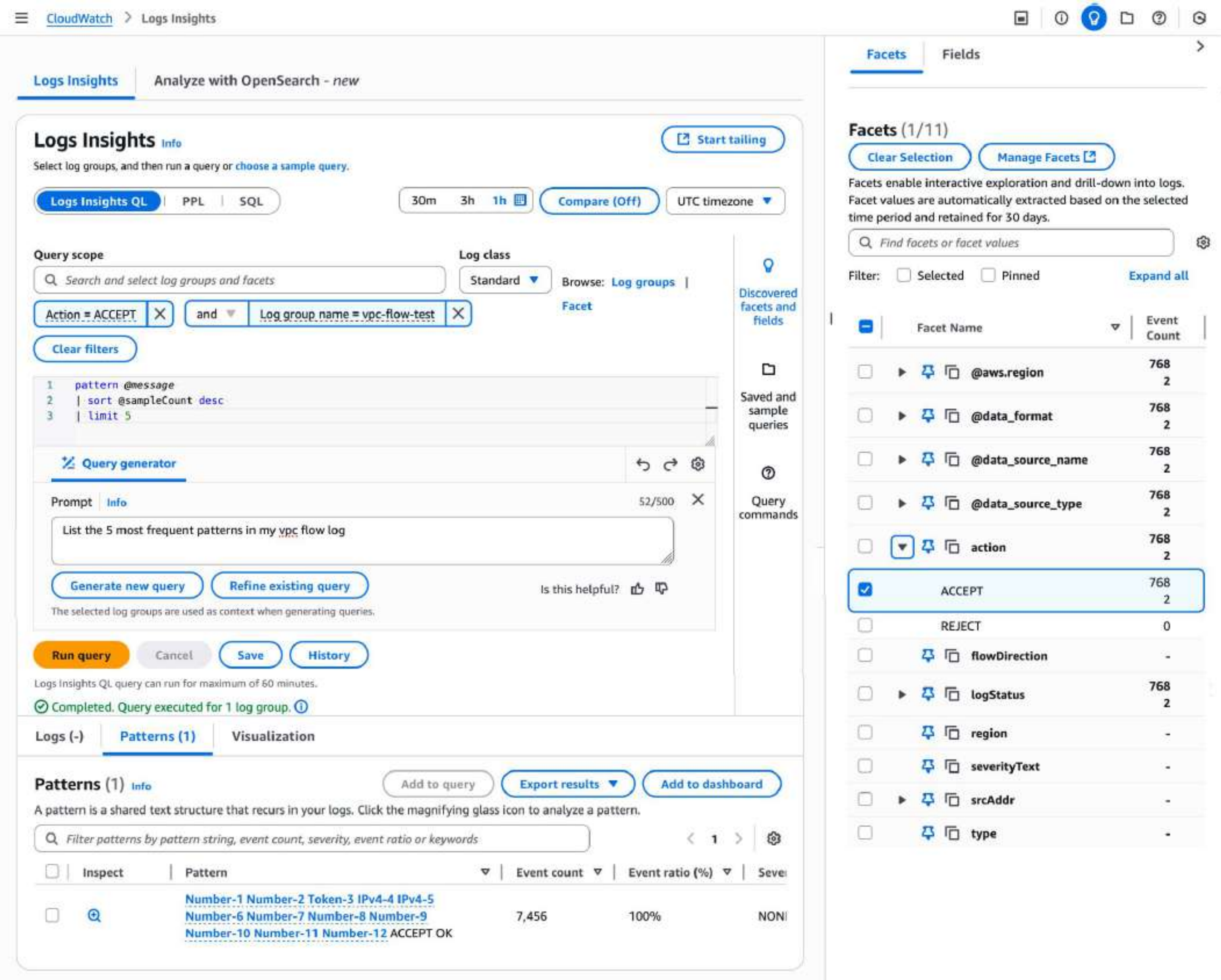
On-prem



Your log data is seamlessly discovered by data source, and data type. To further enrich or transform your data, attach a pipeline. For enhanced analytics and efficient querying, using field indexes and facets in Logs Insights. To enable new data sources, go to Ingestion. Learn more about Data sources, Facets, and S3 Tables integration. To map additional data sources, go to "Unmapped log data" tab below.

Data sources (30) Info

☐	Data source ▲	Category	Log groups	Pipeline	Event f...	Source ...	Source type
☐	amazon_route53.private_dns_quer	AWS	1 log group	No pipeline	Default	amazon_r...	private_dns_query
☑	amazon_vpc.flow	AWS	4 log groups	No pipeline	Default	amazon_vpc	flow
☑	apache.access	Custom	1 log group	No pipeline	Default	apache	access
☑	aws_cloudtrail.data	AWS	1 log group	No pipeline	Default	aws_cloud...	data
☐	aws_cloudtrail.management	AWS	1 log group	No pipeline	Default	aws_cloud...	management
☐	aws_nlb.access	AWS	1 log group	No pipeline	Default	aws_nlb	access
☐	Bedrock.AC	Custom	1 log group	No pipeline	Default	Bedrock	AC
☐	microsoft_entraid.account_change	Custom	2 log groups	No pipeline	Default	microsoft...	account_change



Logs Insights

Select log groups, and then run a query or choose a sample query.

Query scope

Search and select log groups and facets

Log class: Standard

Browse: Log groups | Facet

Action = ACCEPT   and   Log group name = vpc-flow-test

```
pattern @message
| sort @sampleCount desc
| limit 5
```

Prompt Info 52/500

List the 5 most frequent patterns in my vpc flow log

The selected log groups are used as context when generating queries.

Logs Insights QL query can run for maximum of 60 minutes.

Completed. Query executed for 1 log group.

Patterns (1)

A pattern is a shared text structure that recurs in your logs. Click the magnifying glass icon to analyze a pattern.

Filter patterns by pattern string, event count, severity, event ratio or keywords

☐	Inspect	Pattern	Event count	Event ratio (%)	Seve
☐	🔍	Number-1 Number-2 Token-3 IPv4-4 IPv4-5 Number-6 Number-7 Number-8 Number-9 Number-10 Number-11 Number-12 ACCEPT OK	7,456	100%	NON

Facets (1/11)

Facets enable interactive exploration and drill-down into logs. Facet values are automatically extracted based on the selected time period and retained for 30 days.

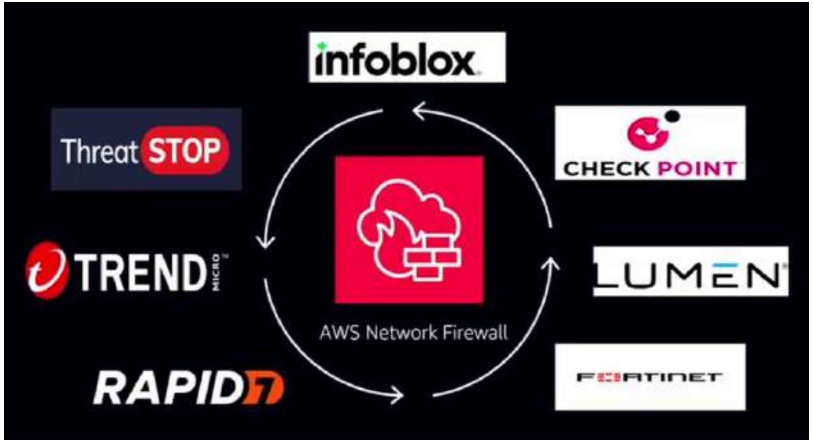
Find facets or facet values

Filter: ☐ Selected ☐ Pinned   Expand all

☐	Facet Name	Event Count
☐	@aws.region	7682
☐	@data_format	7682
☐	@data_source_name	7682
☐	@data_source_type	7682
☐	action	7682
☑	ACCEPT	7682
☐	REJECT	0
☐	flowDirection	-
☐	logStatus	7682
☐	region	-
☐	severityText	-
☐	srcAddr	-
☐	type	-

Network Firewall Marketplace Rules

Network Firewall에서 Active Threat Defense(MadPot 인프라 기반 위협 인텔)와 7개 주요 파트너(Checkpoint, Fortinet, Infoblox, Lumen, Rapid7, Trend Micro, ThreatSTOP)의 관리형 규칙을 사용(구매)할 수 있습니다.



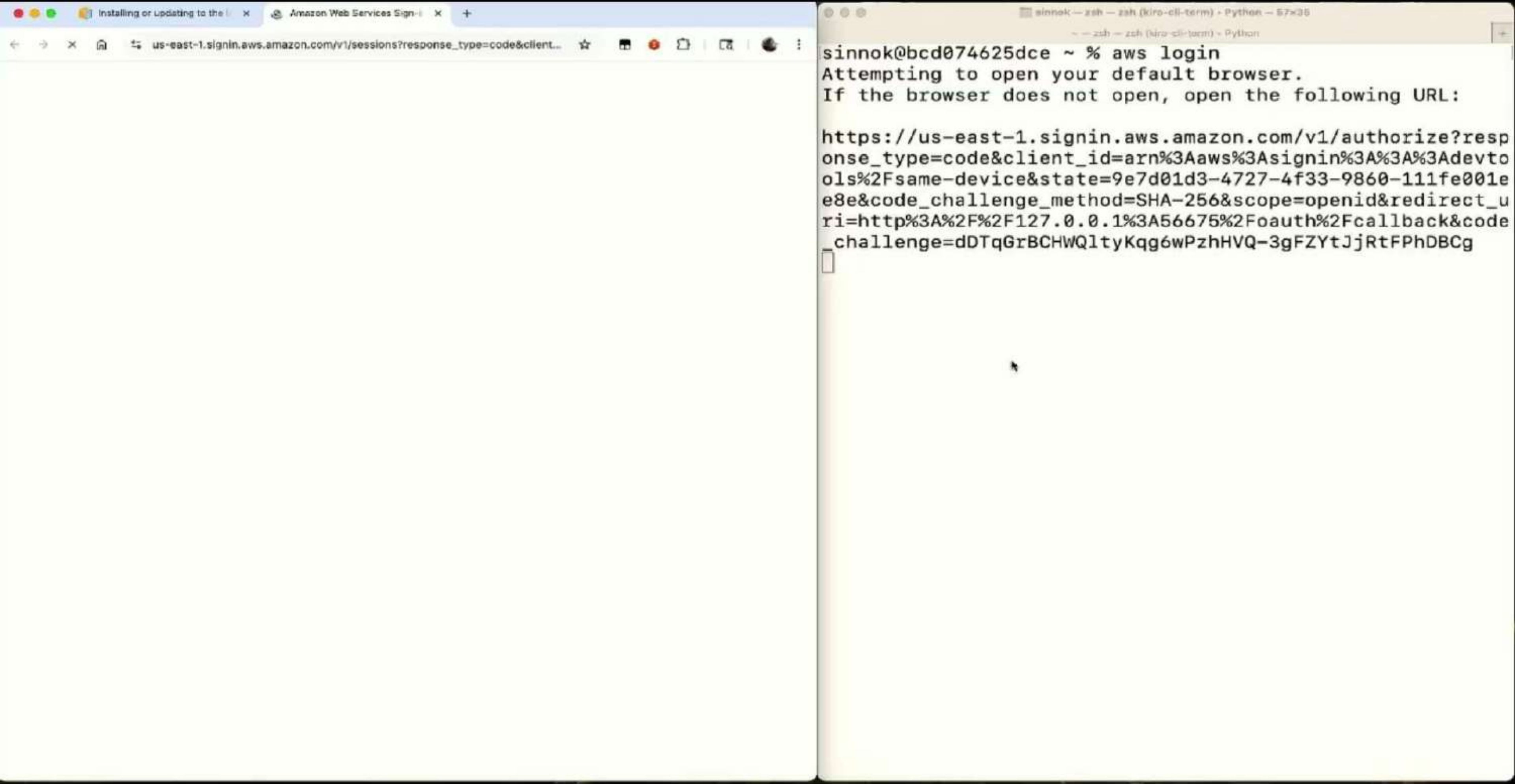
영상: https://www.youtube.com/watch?v=iyT2TJrZhC8

AWS login - Programmatically access AWS with your console credentials

개발자들이 콘솔 로그인 자격 증명을 사용하여 자격 증명 키를 장기 저장하지 않고도 AWS에 접근할 수 있는 방법을 다룹니다

```
$ aws login
```

영상: https://www.youtube.com/watch?v=BI9kWS-UxR0

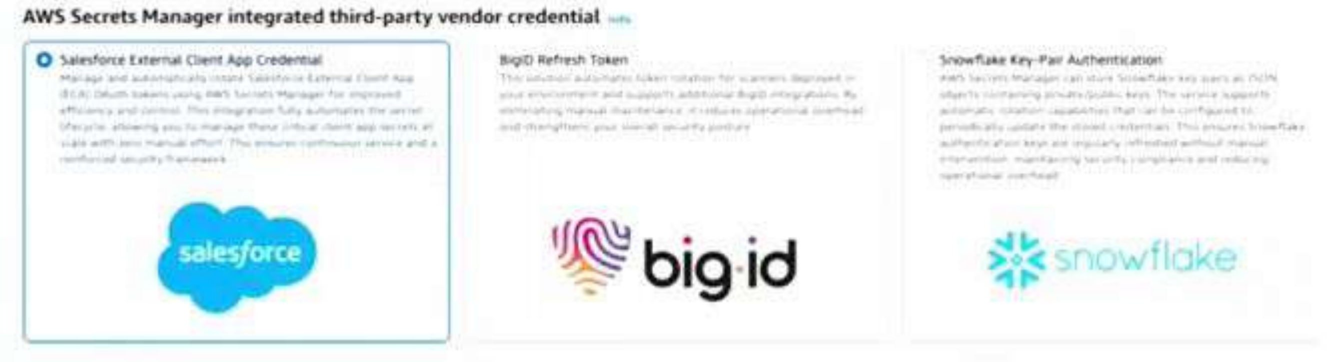

Installing or updating to the l
Amazon Web Services Sign-i
us-east-1.signin.aws.amazon.com/v1/sessions?response_type=code&client...
sinnok — zsh — zsh (kiro-cli-term) · Python — 57×35
~ — zsh — zsh (kiro-cli-term) · Python

```
sinnok@bcd074625dce ~ % aws login
Attempting to open your default browser.
If the browser does not open, open the following URL:

https://us-east-1.signin.aws.amazon.com/v1/authorize?resp
onse_type=code&client_id=arn%3Aaws%3Asignin%3A%3A%3Adevto
ols%2Fsame-device&state=9e7d01d3-4727-4f33-9860-111fe001e
e8e&code_challenge_method=SHA-256&scope=openid&redirect_u
ri=http%3A%2F%2F127.0.0.1%3A56675%2Foauth%2Fcallback&code
_challenge=dDTqGrBCHWQltyKqg6wPzhHVQ-3gFZYtJjRtFPhDBCg
```

Zero-Touch Secret Rotation for your third-party secrets

AWS Secrets Manager가 비 AWS 서비스(서드파티)를 에서도 시크릿을 로테이션 할 수 있는 기능을 제공합니다. (람다 안쓰고! 네이티브하게)



AWS Secrets Manager integrated third-party vendor credential

● Salesforce External Client App Credential

BigID Refresh Token

Snowflake Key-Pair Authentication

영상: https://www.youtube.com/watch?v=BI9kWS-UxR0

Thank you!