How Trellix uses the Open Cybersecurity Framework with Amazon Security Lake

Martin Holste
Trellix CTO, Cloud

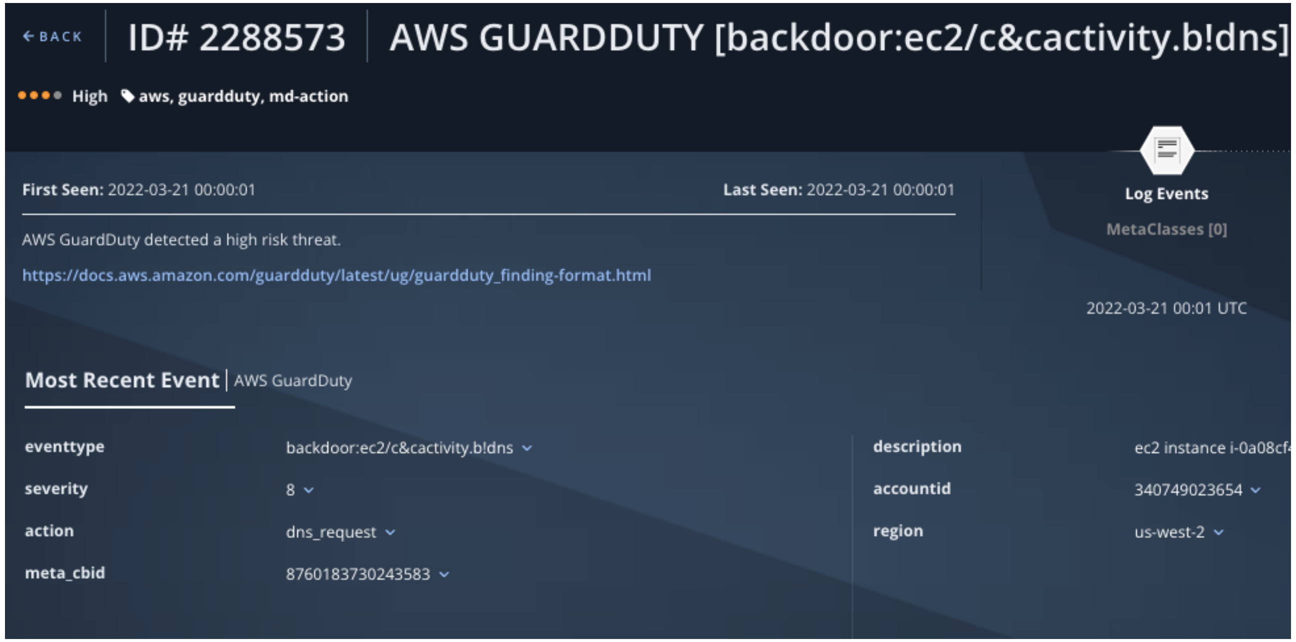
Harrison Holstein
Partner Solutions Architect

Trellix

If you don’t have supporting evidence, alerts aren’t much to go on. For example:

ec2 instance i-0a08cf4dd7dc2beda is querying a domain name associated with a known command & control server.

1. When was this domain declared malicious?
2. What kind of asset is this local IP?
3. What did the communication look like?



ID# 2288573 AWS GUARDDUTY [backdoor:ec2/c&cactivity.b!dns]

●●●● High aws, guardduty, md-action

First Seen: 2022-03-21 00:00:01 **Last Seen:** 2022-03-21 00:00:01

AWS GuardDuty detected a high risk threat.

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-format.html

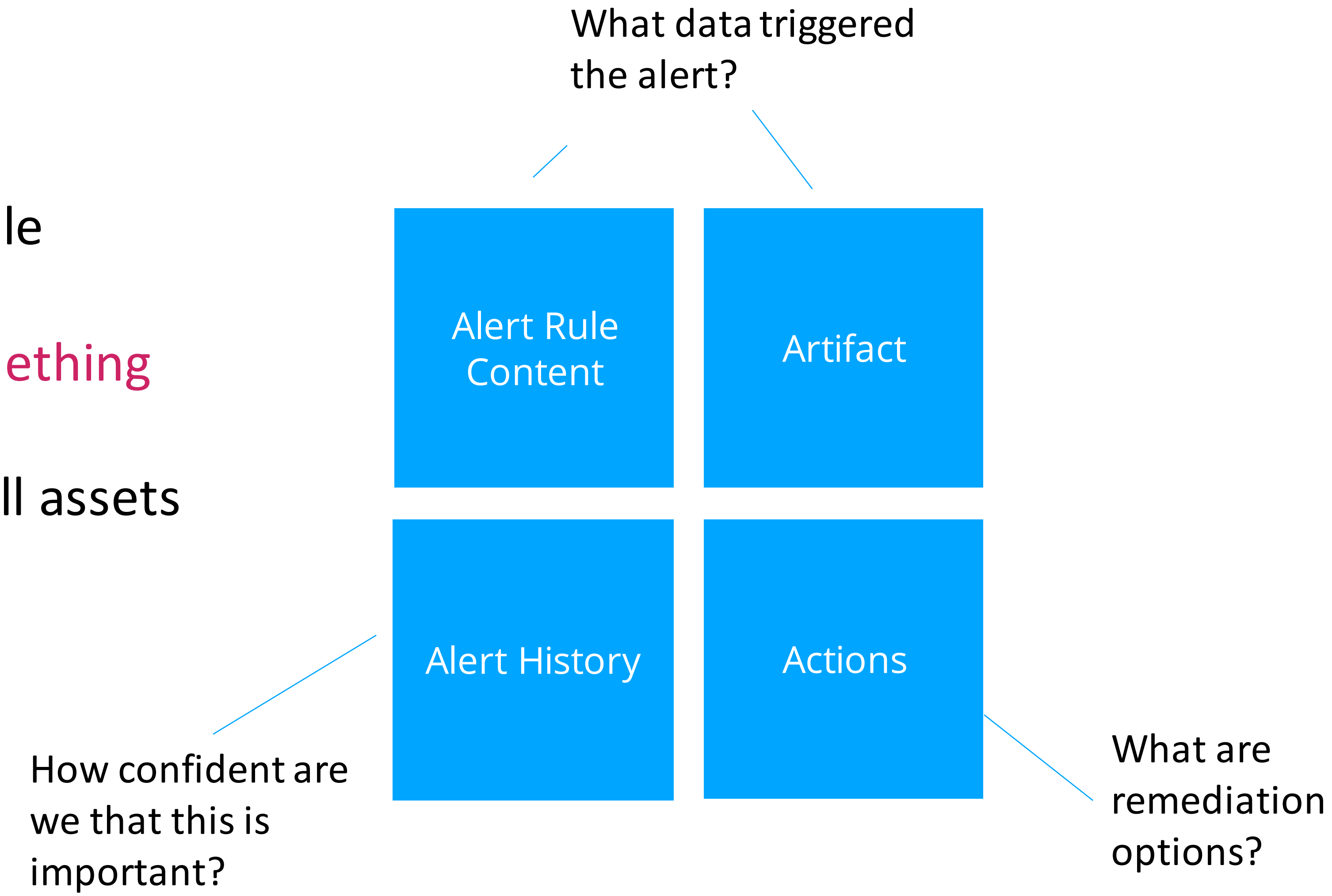
2022-03-21 00:01 UTC

Most Recent Event | AWS GuardDuty

eventtype	backdoor:ec2/c&cactivity.b!dns	**description**	ec2 instance i-0a08cf
severity	8	**accountid**	340749023654
action	dns_request	**region**	us-west-2
meta_cbid	8760183730243583		

Getting answers about the alert

1. What data triggered the alert?
   - Alert triggering rule
   - Artifact (network capture, file sample, or log sample)
2. How confident are we that something bad happened?
   - Rule trigger history across all assets
3. How do we remediate?
   - Is this actionable?


What data triggered the alert?
Alert Rule Content
Artifact
Alert History
Actions
How confident are we that this is important?
What are remediation options?

Introducing the Open Cybersecurity Framework (OCSF)

So many ways to say “IP address”

Analysts waste precious time understanding the nuances of their security data.

- Ip_address
- IP
- Ip_addr
- Srcip
- Source_ip
- Src_ip
- Srchost
- Src_address
- Host
- Hostname
- Target
- Calleraddress
- Sourcecallingip
- Dest
- Dstipv4
- Dest_ip
- Dest_ipv4
- Dst_ip
- Dst_ipv4
- Etc., etc.

The Open Cybersecurity Framework

Solving the inefficiencies of mismatched security data.

The OCSF is a consortium of major players in the security industry that have joined with AWS to declare how we label security data.

- Analysts no longer waste precious time cleaning and understanding data.
- Security telemetry is ensured to contain the same amount of data, regardless of which vendor created it.
- When data is put in the same place, it adds value without becoming an operational burden.

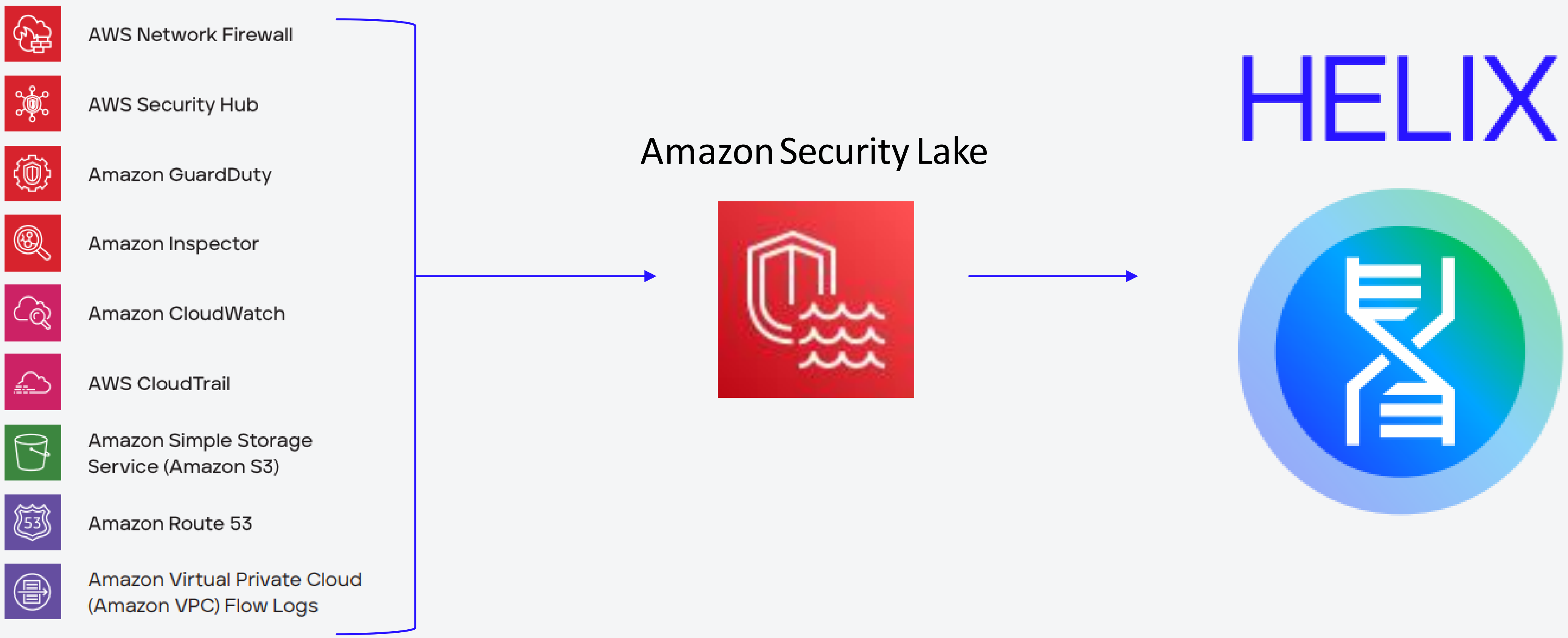
Amazon Security Lake

Powered by the OCSF

The Amazon Security Lake + OCSF creates a new standard for how customers should expect security telemetry: on their terms.

- All security data stored in Amazon Security Lake is guaranteed to conform to OCSF schemas.
- Customers have full control over the data in the lake and grant access to others to use it.
- Security Lake data is stored in commonly used formats (Apache Parquet) on S3, so customers can choose almost any form of indexing and querying.

Trellix + AWS = Security



AWS Network Firewall

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS CloudTrail

Amazon Simple Storage Service (Amazon S3)

Amazon Route 53

Amazon Virtual Private Cloud (Amazon VPC) Flow Logs

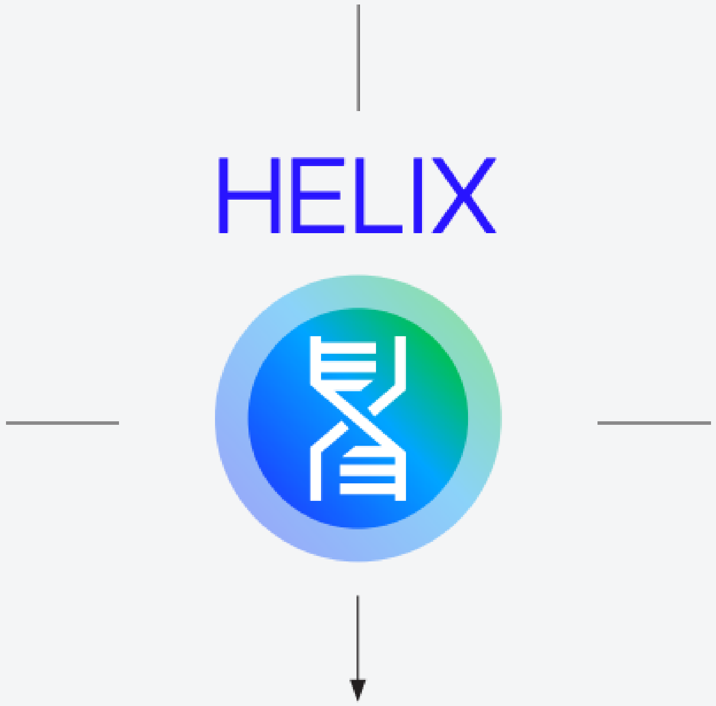
Amazon Security Lake

HELIX

Trellix + AWS = Security

- Endpoint Security
- Email Security
- Network Security and Forensics
- Detection as a Service
- Cloudvisory

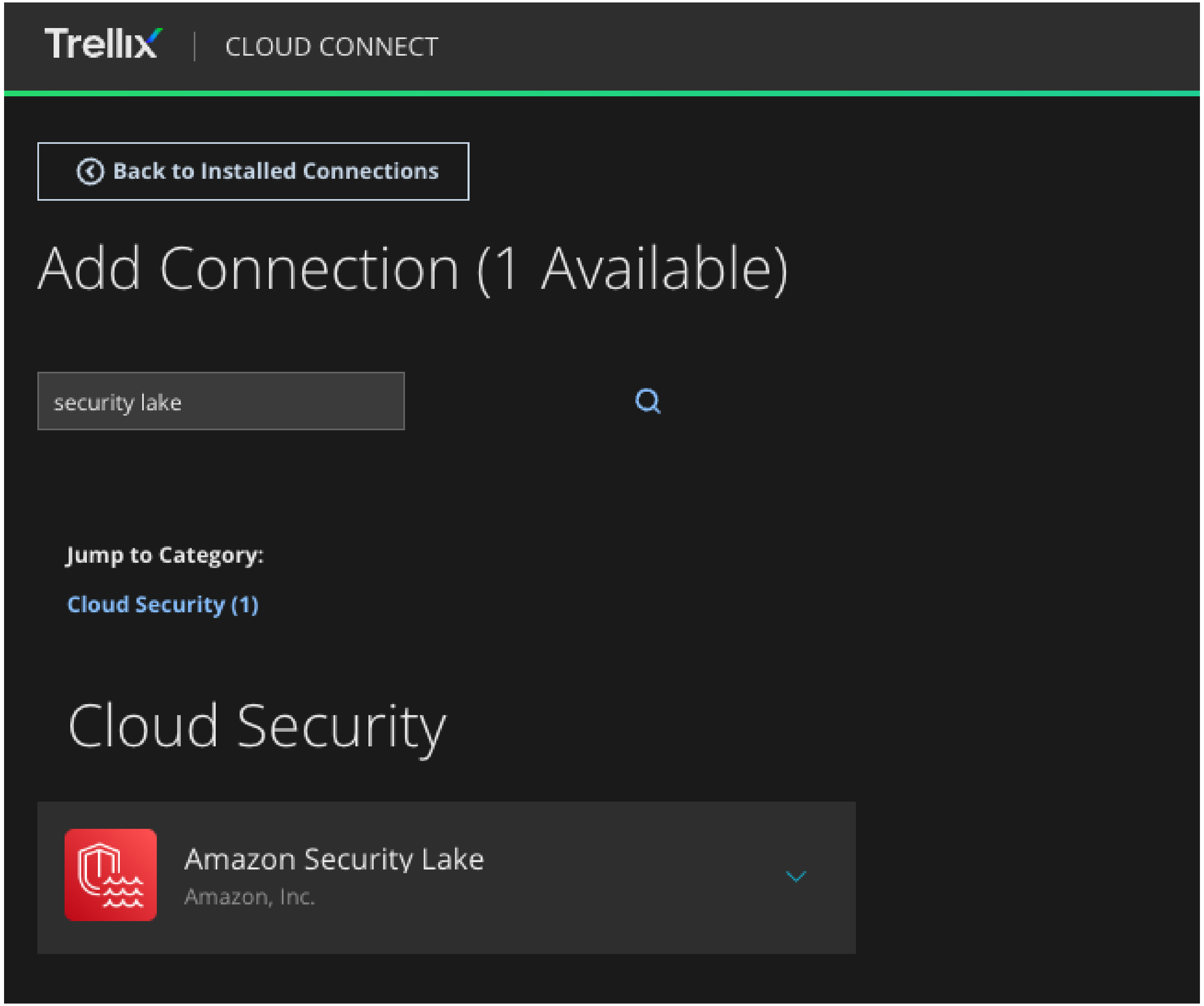
600+ integrations with security tools and applications.



- Prevent data loss and insider threats
- Investigate anomalies faster
- Detect late-stage attacks

- AWS Network Firewall
- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS CloudTrail
- Amazon Simple Storage Service (Amazon S3)
- Amazon Route 53
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs

Get up and running with Trellix Helix and Amazon Security Lake in seconds with our fast and easy setup.



Trellix | CLOUD CONNECT

Back to Installed Connections

Add Connection (1 Available)

security lake

Jump to Category:

Cloud Security (1)

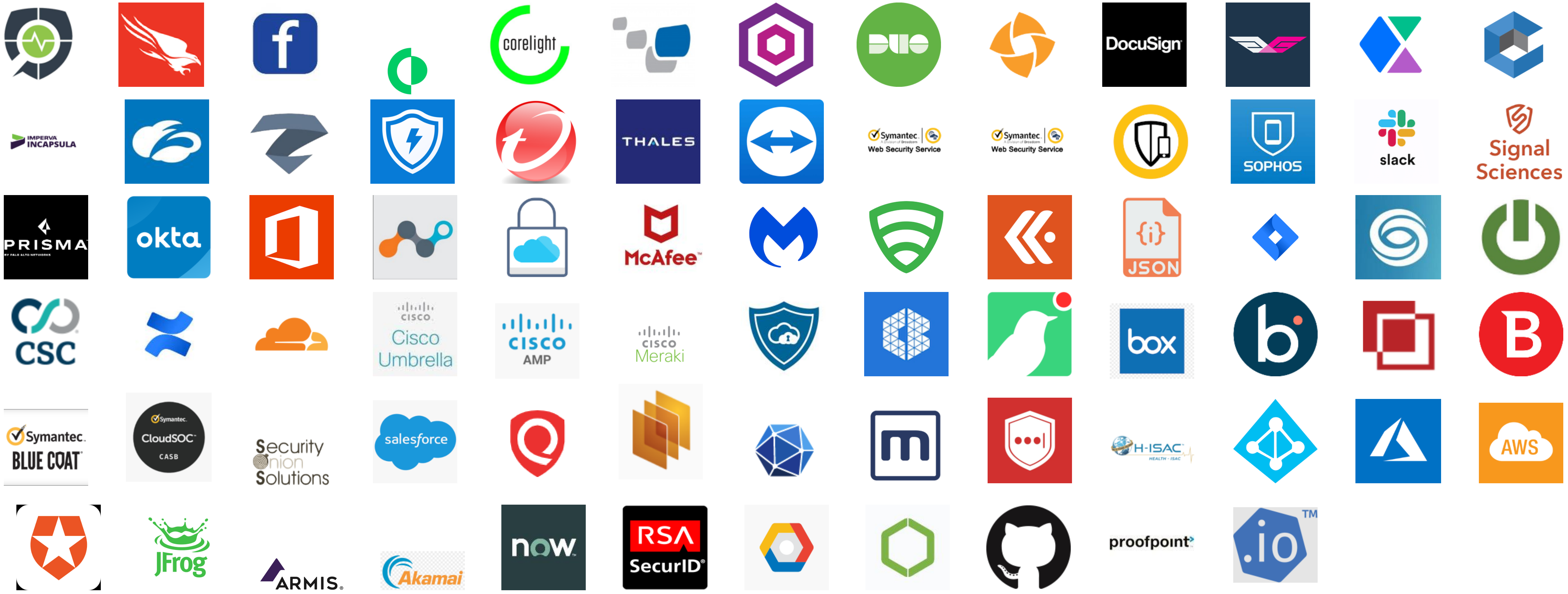
Cloud Security

Amazon Security Lake
Amazon, Inc.

Defending the Cloud with XDR

Trellix

Trellix has 3x more XDR integrations than anyone.

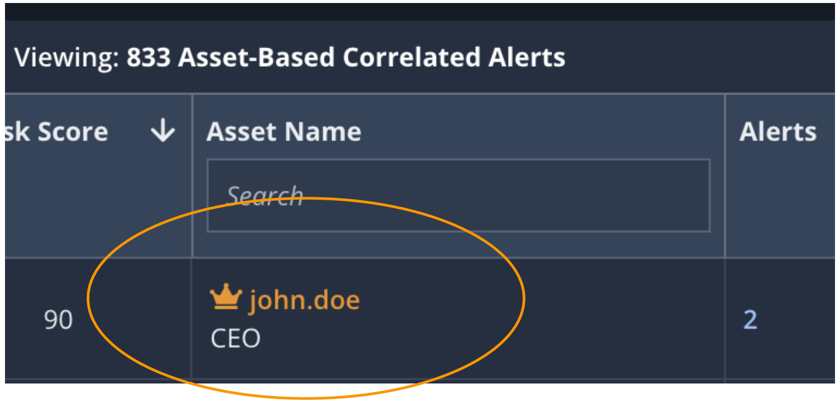


Identity integrations

	Azure Active Directory (For UEBA)
DUO	Duo Auth
	Entrust Intellitrust
okta	Okta

Identity integrations provide identity models which aid in both detection and response. They are the foundation for identity-based risk scoring in XDR.

- ✓ Flag VIP users based on profile for risk scoring
- ✓ Job descriptions aid analysts during investigations
- ✓ Connecting users to roles provides basis for threat hunting



Viewing: 833 Asset-Based Correlated Alerts

sk Score ↓	Asset Name	Alerts
	Search	
90	john.doe CEO	2

Business App Integrations

Most modern threats take advantage of business applications, but getting full access to this data is frequently challenging. Customers need apps that work with the XDR ecosystem to:

✓ Correlate and alert on audit events

✓ Track activities with analytics for anomalies

✓ Quickly react to threats by making policy changes

- Office 365
- Salesforce Events
- Gsuite Admin Logs
- Teamviewer Events
- Microsoft Teams
- Slack

Cloud Storage Integrations

Cloud isn’t just events, there are also many artifacts that need coverage.

- ✓ Malicious file detection
- ✓ Sensitive data identification and control
- ✓ Bulk telemetry integration

- AWS S3
- Azure Blob Storage
- Palo Alto Cortex Data Lake
- Box

Email Integrations

Business email compromise is a serious threat. Understanding how email is being used and correlating alerts with actions is critical.

✓Match phishing alerts with host actions

✓Analyze similar threats and extrapolate for threat hunting

✓Change policies to block threats

Mimecast

Proofpoint

Microsoft Office365

Endpoint Integrations

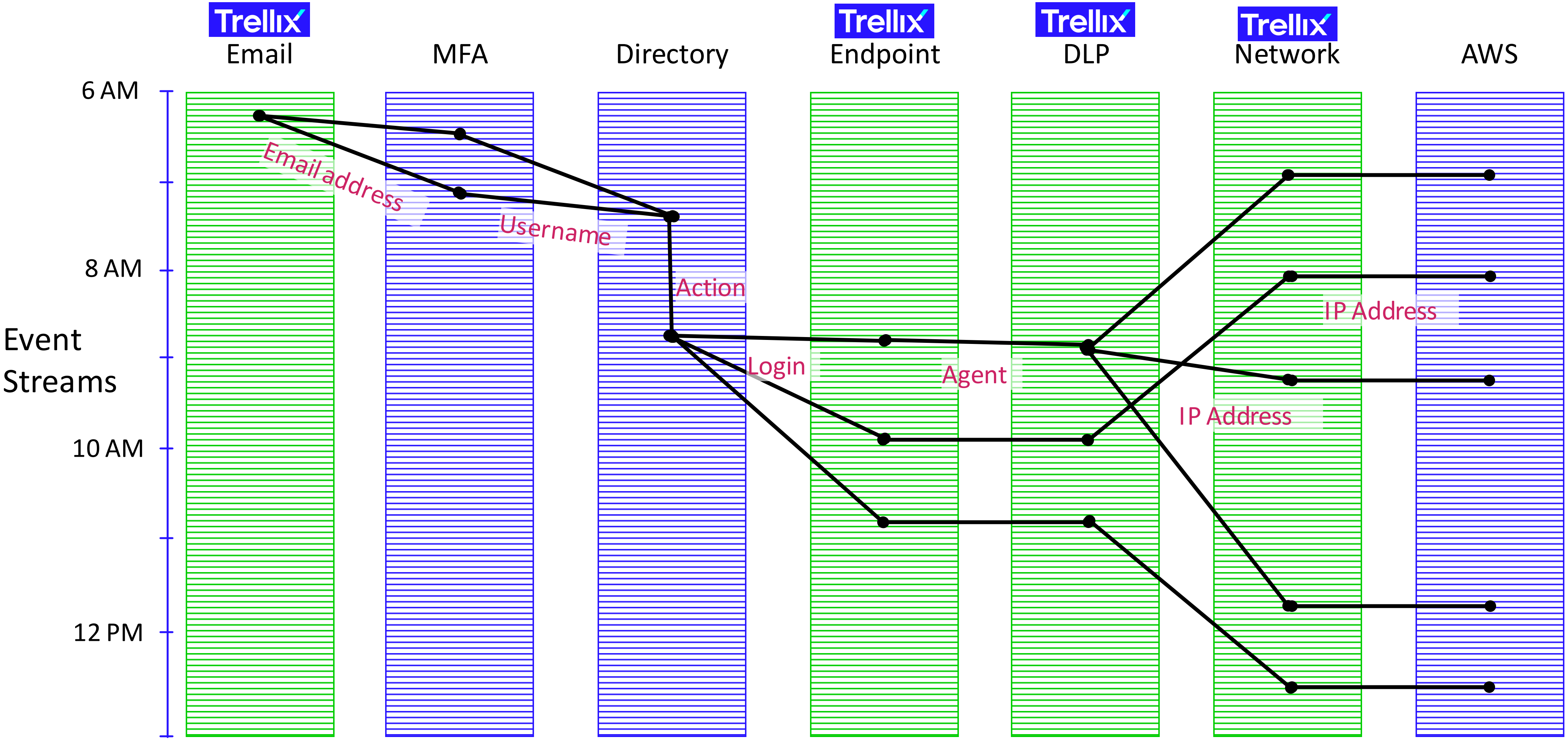
Endpoint plays a crucial role in every enterprise, and the need to integrate it into XDR is self-evident. Here are the key capabilities required:

- ✓ Correlate alerts from multiple hosts
- ✓ Collect EDR trace data for threat hunting
- ✓ Contain compromised hosts
- ✓ Provide offline telemetry

- Cisco
- CyberArk
- CarbonBlack
- Crowdstrike
- Microsoft
- Sophos
- TrendMicro

Our rich XDR platform with partners tells the complete story

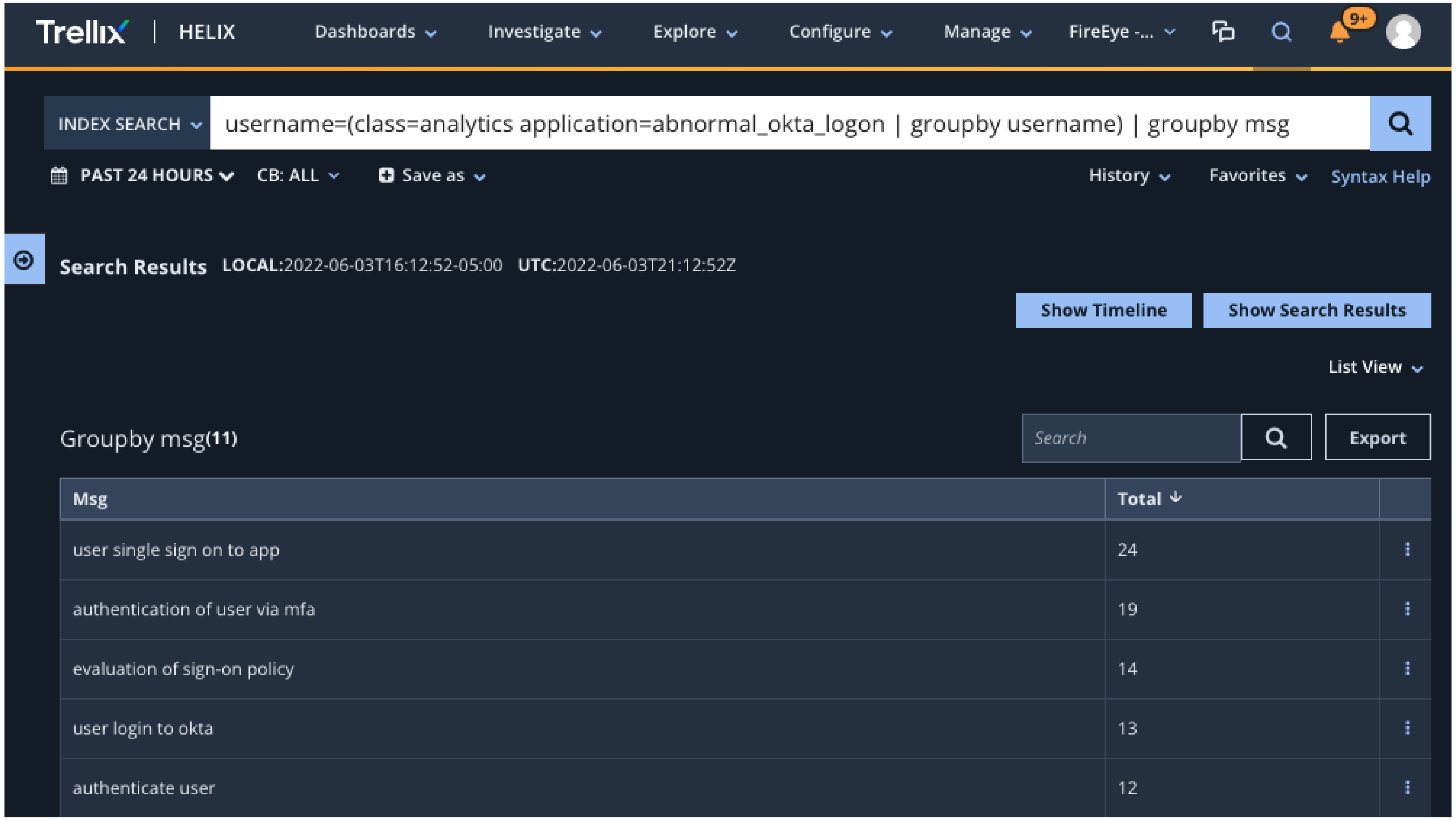
Phishing > 2FA reset > Service account creation > Endpoint compromises > Data theft > AWS account actions



Confidential –Do not distribute

Together, analytics become more powerful

Advanced hunting leverages ML results to go beyond alerting and ML by combining the two across expansive data sets.



```
username=(class=analytics application=abnormal_okta_logon | groupby username) | groupby msg
```

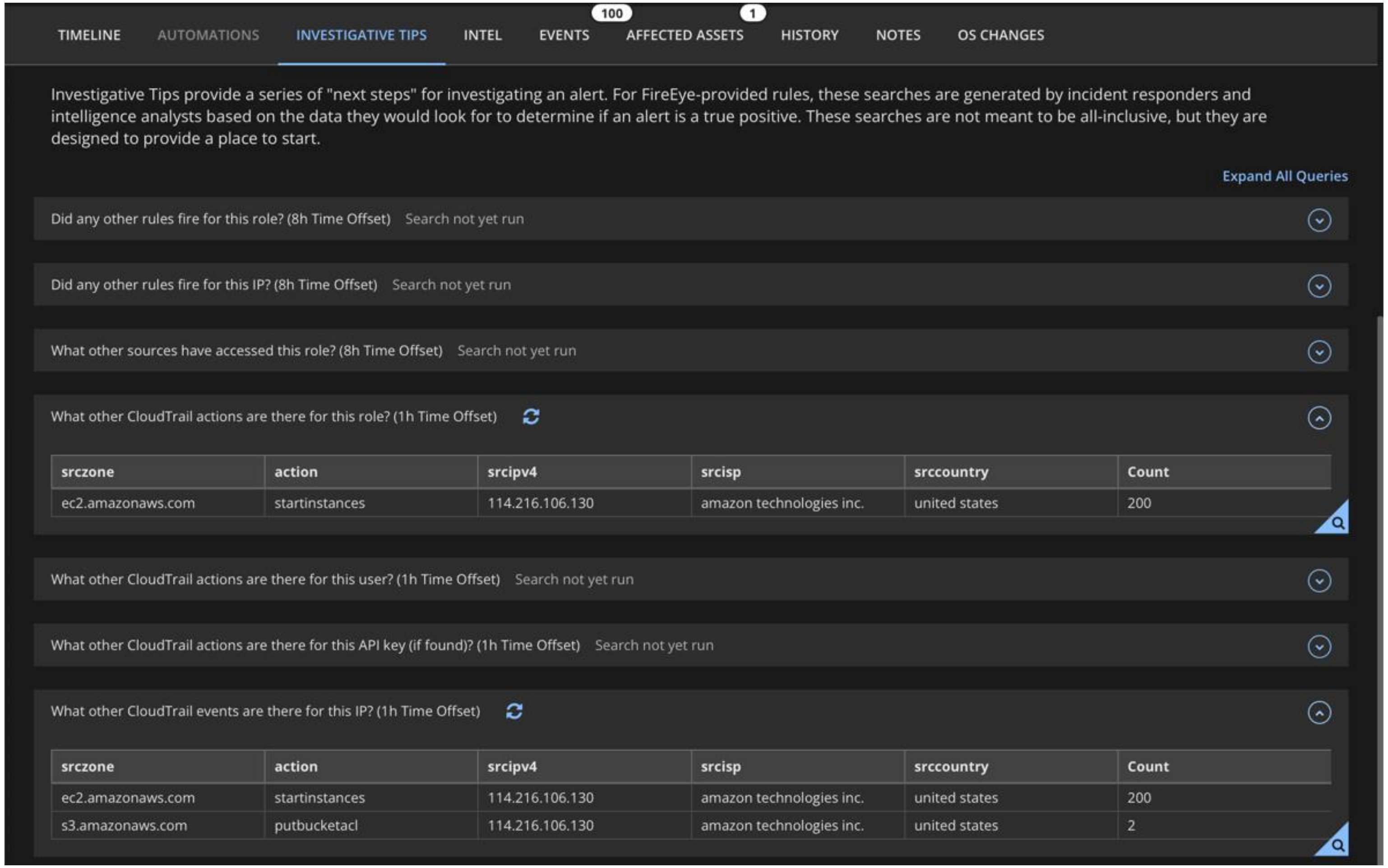
Search Results LOCAL:2022-06-03T16:12:52-05:00 UTC:2022-06-03T21:12:52Z

Groupby msg(11)

Msg	Total ↓
user single sign on to app	24
authentication of user via mfa	19
evaluation of sign-on policy	14
user login to okta	13
authenticate user	12

XDR Investigative Tips

Built-in Expert Investigation



Investigative Tips provide a series of "next steps" for investigating an alert. For FireEye-provided rules, these searches are generated by incident responders and intelligence analysts based on the data they would look for to determine if an alert is a true positive. These searches are not meant to be all-inclusive, but they are designed to provide a place to start.

Did any other rules fire for this role? (8h Time Offset) Search not yet run

Did any other rules fire for this IP? (8h Time Offset) Search not yet run

What other sources have accessed this role? (8h Time Offset) Search not yet run

What other CloudTrail actions are there for this role? (1h Time Offset)

srczone	action	srcipv4	srcisp	srccountry	Count
ec2.amazonaws.com	startinstances	114.216.106.130	amazon technologies inc.	united states	200

What other CloudTrail actions are there for this user? (1h Time Offset) Search not yet run

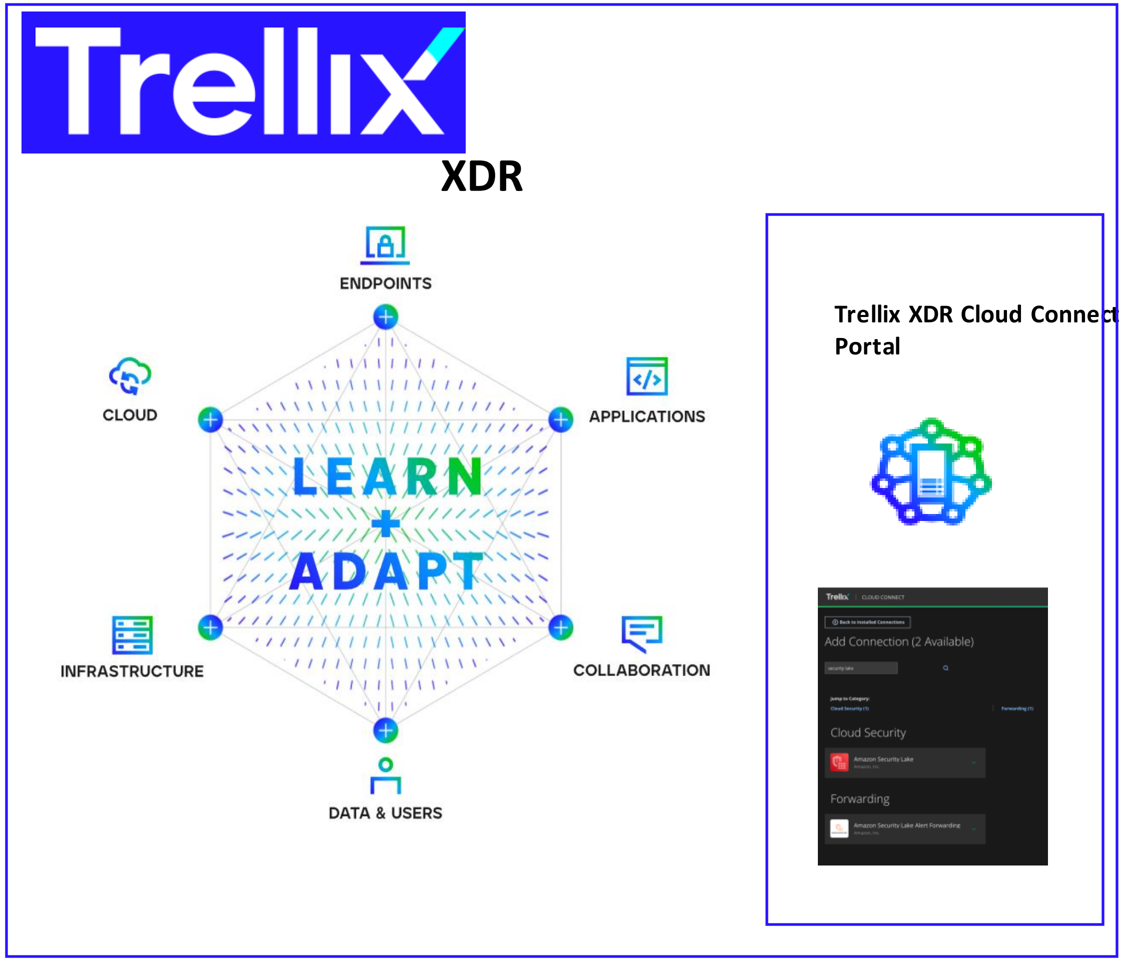
What other CloudTrail actions are there for this API key (if found)? (1h Time Offset) Search not yet run

What other CloudTrail events are there for this IP? (1h Time Offset)

srczone	action	srcipv4	srcisp	srccountry	Count
ec2.amazonaws.com	startinstances	114.216.106.130	amazon technologies inc.	united states	200
s3.amazonaws.com	putbucketacl	114.216.106.130	amazon technologies inc.	united states	2

Trellix Helps Secure Gen AI

Use Trellix XDR to monitor gen AI such as Amazon Bedrock



Trellix | CLOUD CONNECT

Back to Installed Connections

Add Connection (2 Available)

security lake

Jump to Category:
Cloud Security (1) | Forwarding (1)

Cloud Security

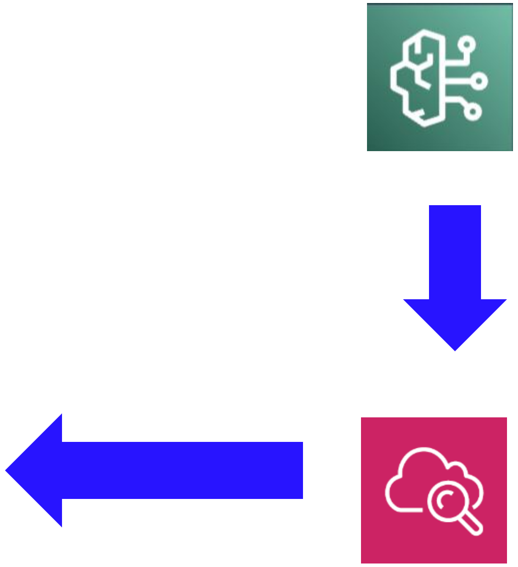
Amazon Security Lake
Amazon, Inc.

Forwarding

Amazon Security Lake Alert Forwarding
Amazon, Inc.

Figure 1: Joint customers can share security events across Trellix XDR and with Amazon Security Lake, getting complete detection and response capabilities for their AWS environments.

Example with LLM02: Insecure output handling



Amazon Bedrock

Malcious prompt from web app:

“Create Javascript that will send the session ID to this URL…”

Amazon CloudWatch

Trellix XDR can tie AI activity together with cloud and other platform events.

THANK YOU!

Trellix