

# Become a Sumo Security User

Security Certification



# Become a Sumo Security Power User

1. Learn How **Security Analytics** works for you
2. Develop a **Toolset** for Basic and Advanced Analytics
3. **Monitor** Trends & Critical Events
4. Learn about Sumo's **Security and Compliance Apps**
5. **Next steps:** where do you go from here?

# Tutorial: Hands-on Exercises

## Training Environment:

1. [service.sumologic.com](https://service.sumologic.com)
2. The username and password is on your handout

## Security Hands-on Labs:

- [sumologic.com/learn/certifications](https://sumologic.com/learn/certifications)



ONLINE EXAM: 30 QUESTIONS | 60  
MINUTES  
PREP: SECURITY ANALYTICS WEBINAR  
& HANDS-ON LABS ←

# Sumo Logic Security Analytics

## Real-time insights for streamlined **Compliance and Security**

- Meet compliance deadlines
- Reduce security risks
- Identify potential security breaches
- Neutralize new threat patterns
- Transform reactive/manual processes into integrated/proactive/automated

## Automate Threat Detection

- Detect threats across microservices, container services, cloud-based technology, operating systems, applications, storage devices, servers, workstations, and more.

# Examples of Security Use Cases



- Monitor “Root” Logins
- Monitor Multiple Failed Logins
- Monitor Web Activity
- Monitor Ingress/Outgress Rules
- Identify publicly exposed Security Group (0.0.0.0/0 with <open port>)
- Identify Services out of Compliance (no patches in “n” days)
- Identify Application Threats (Libraries, Botnets, compromised credentials)
- Monitor Malicious Threats and IOCs

➤ What's your use case?

# Search and Parse

Filter and Provide Structure

sumo logic®



# Search and Parse

## Search and Filter your data

### Search and Filter your data

- \_metadata
- Keywords
- Live Tail

```
_sourceCategory=Labs/AWS/CloudTrail and root  
| json "eventType", "sourceIPAddress", "userIdentity" nodrop  
| json field=userIdentity "type", "arn" nodrop
```

## Parse fields to provide structure to your data

- Query Parsing
- Implement your Field Extraction Rules



# Security Certification: Hands-on Labs

## Security Analytics

### Labs 1-3: Search and Parse

- Search Basics: Metadata and Keywords
- Parsing Operators and Options
- Grouping Results
- Field Extraction Rules

# Simple Analytics

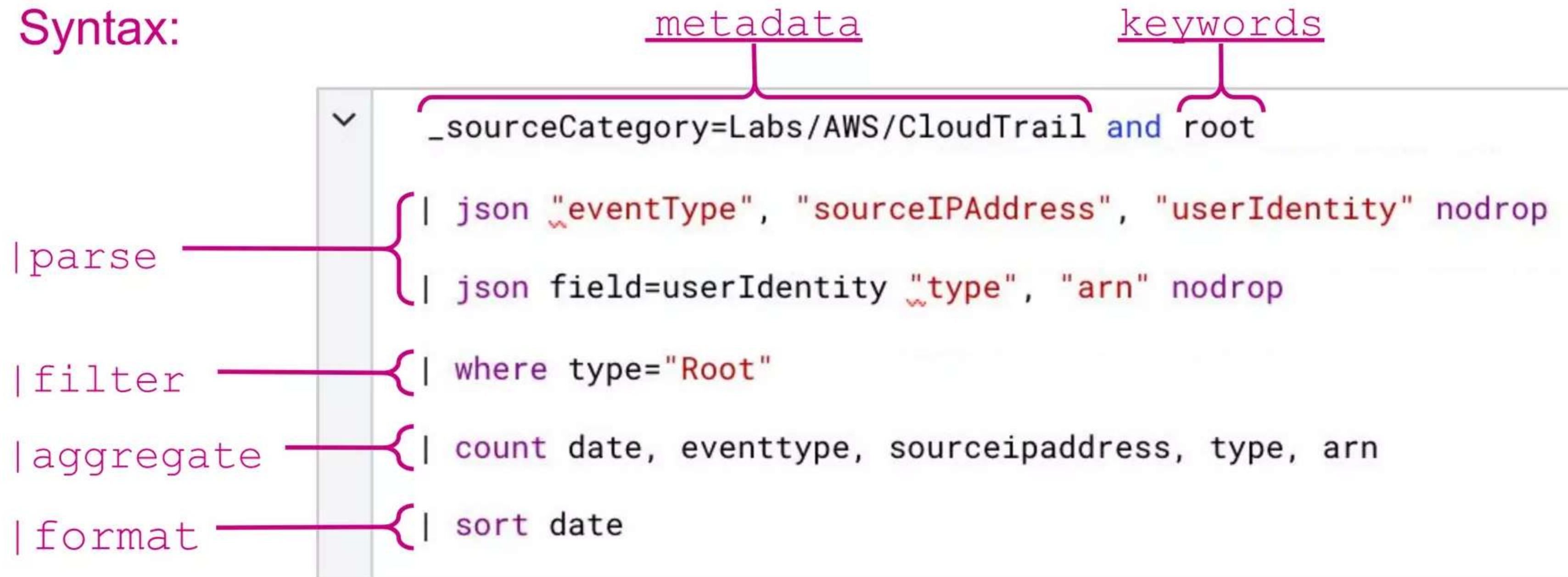
Conditional Logic, Filtering,  
Formatting Results



# Review ➔ Query Syntax

Keywords and operators, separated by pipes, that build on top of each other

Syntax:



# Simple Analytics

Aggregation	Conditional	Formatting
<b>count</b> [ ]   <b>sum</b>   <b>avg</b>   <b>min</b> ( )   <b>max</b> ( )	<b>if</b> ( )   [ ] <b>matches</b> [ ]   <> <b>in</b> ( )   <b>filter</b>   <b>where</b>	<b>transpose</b>   <b>fields</b>   <b>limit</b>   <b>sort by</b>   <b>top</b>

Home **Learn** + New

**Learn Tab**

Quick Start Videos

- Sumo Logic Quickstart
- Introduction to Search
- Building Dashboards
- Simplifying Search with Search Templates
- Introduction to Metrics in Sumo

Sumo Logic QuickStart Webinar - August 2018      Introduction to Search      Building Dashboards      Simplifying Search with Search Templates      Introduction to Metrics in Sumo

Using Sumo Logic Tutorial

- Part 1: Viewing Data
- Part 2: Search for Log Data
- Part 3: Chart your data
- Part 4: Create and share a dashboard
- Part 5: Modify your dashboard
- Part 6: Create an alert
- Part 7: Get help

Set Up Sumo Logic Tutorial

- Part 1: Install a Collector
- Part 2: Add a Source
- Part 3: Install an App and View Data
- Part 4: Try Simple Analytics
- Part 5: Collect and Visualize Host Metrics

Cheat Sheet      Docs      What's New

Community      Ask for Support      Get Training

Cheat Sheet

Community

# Security Certification: Hands-On Labs

## Security Analytics

### Lab 4A: Monitor AWS Root Account Usage

Community > Query Library > Security-related Queries for AWS

```
_sourceCategory=Labs/AWS/CloudTrail and root
| json "eventType", "eventName", "eventSource", "sourceIPAddress", "userIdentity", "responseElements" nodrop
| json field=userIdentity "type", "arn" nodrop
| where type="Root"
| where !(sourceipaddress matches "*amazonaws*")
| formatDate(_messageTime, "yy-MM-dd HH:mm:ss") as date
| count date, eventname, eventtype, sourceipaddress, type, arn
| sort date
```

## Filter using metadata and keywords



# Security Certification: Hands-On Labs

## Security Analytics

### Lab 4B: Monitor Security Groups Created

Community > Query Library > Security-related Queries for AWS

```
✓ _sourceCategory=Labs/AWS/CloudTrail and authorizesecuritygroupingress
| json "requestParameters", "userIdentity"
| json "errorCode" nodrop
| json field=useridentity "type" nodrop
| json field=useridentity "arn" nodrop
| json field=requestParameters "ipPermissions"
| json field=requestParameters "groupId"
| json field=ipPermissions "items[*].ipRanges.items[*].cidrIp" as cidrIp nodrop
| json field=ipPermissions "items[*].ipv6Ranges.items[*].cidrIpv6" as cidrIpv6 nodrop
| json field=ipPermissions "items[*].fromPort" as fromPort nodrop
| json field=ipPermissions "items[*].toPort" as toPort nodrop
| json field=ipPermissions "items[*].ipProtocol" as ipProtocol nodrop
// Uncomment the next line to identify "Permit Any" Ingress Security Groups
//| where (ipProtocol matches "*-1*" or (fromPort="[0]" and toPort="[65535]")) or cidrip matches
"0.0.0.0*" or cidripv6 matches "*::*"
```

# Security Certification: Hands-On Labs

## Security Analytics

### Lab 4C: Monitor “Impossible Travel” scenario

Community > Query Library > Security-related Queries for AWS

```
✓ _sourceCategory=Labs/AWS/CloudTrail and consolelogin
| json "eventType", "eventName", "eventSource", "sourceIPAddress", "userIdentity", "responseElements",
"additionalEventData"
| json field=userIdentity "type", "arn"
| json field=responseElements "ConsoleLogin"
| json field=additionalEventData "MFAUsed", "SamlProviderArn" nodrop
| where consolelogin="Success"
| count arn, sourceipaddress
| sort by arn
| 1 as rownum
| total rownum by arn
| where _total > 1
| fields -_count, rownum|
| formatDate(_messageTime, "yy-MM-dd HH:mm:ss") as date
| count date, cidrip, fromport, toport, groupid, ipprotocol, arn, type, errorcode|
```

# Advanced Analytics

Outliers, Trends,  
Needle in the Haystack



# Advanced Analytics

**LogReduce** → New security attacks/breaches.

Find the "needle in the haystack" by identifying patterns.

```
_sourceCategory=Labs/security/snort  
| logreduce
```

**LogCompare** → Compare attacks/breaches to other time periods.

Compare today's patterns with patterns in the past.

```
_sourceCategory=Labs/security/snort  
| logcompare -24h
```

#	Select	Count	Relevance	Actions	Signature
1	<input type="checkbox"/>	<a href="#">469</a>	9.53		\$DATE WEB-MISC BugPort config 2] {TCP} ***** -> 10.*****
2	<input type="checkbox"/>	<a href="#">389</a>	9.53		\$DATE WEB-PHP Typo3 transla 1] {TCP} ***** :**-> *10. *
3	<input type="checkbox"/>	<a href="#">350</a>	9.53		\$DATE WEB-MISC BugPort config 2] {TCP} ***** -> 10.*****
4	<input type="checkbox"/>	<a href="#">174</a>	9.53		\$DATE SENSITIVE-DATA Email Ad > *10. *****

#	Select	Count	Score	Actions	Signature
1	<input type="checkbox"/>	<a href="#">473</a> -1.5%	0.00		\$DATE WEB-MISC BugPort config {TCP} ***** -> 10.*****
2	<input type="checkbox"/>	<a href="#">388</a> -7.1%	0.07		\$DATE WEB-PHP Typo3 translati {TCP} ***** :**-> *10. *****
3	<input type="checkbox"/>	<a href="#">358</a> -0.01%	0.00		\$DATE WEB-MISC BugPort config {TCP} ***** -> 10.***.206.*
4	<input type="checkbox"/>	<a href="#">178</a> +25%	0.25		\$DATE SENSITIVE-DATA Email Ad > *10. *****

# Advanced Analytics

**Outlier → Anomalies in number of Failed Logins**

```
_sourceCategory=Labs/AWS/CloudTrail  
| parse "\"eventName\":\"*\"" as eventName nodrop  
| parse "\"responseElements\":{\"ConsoleLogin\":\"*\"}" as loginResult nodrop  
| where eventName="ConsoleLogin" and loginresult="Failure"  
| timeslice 30m  
| count(eventName) as failed_login_attempts by _timeslice  
| outlier failed_login_attempts
```

**Predict → Traffic from a Rogue Country/State**

```
_sourceCategory=Labs/security/Proofpoint and Mexico  
| timeslice 5m  
| count as rogue_traffic by _timeslice  
| predict rogue_traffic by 5m forecast=12
```

# Advanced Analytics

**Time Compare → Identify a 5-fold increase in Denied Traffic**

```
_sourceCategory=Labs/PaloAltoNetworks and ",TRAFFIC,"  
| where action="deny"  
| count action  
| compare with timeshift 15m 4 avg  
| if(isNull(_count), 0, _count) as _count  
| if(isNull(_count_60m_avg), 0, _count_60m_avg) as _count_60m_avg  
| where _count > (5 * _count_60m_avg)
```

**Geo Lookup → Traffic Destinations outside the US**

```
_sourceCategory=Labs/PaloAltoNetworks and ",TRAFFIC,"  
| lookup latitude, longitude, country_code, country_name, city from geo://location on ip=dest_ip  
| where country_code <> "US"  
| count by latitude, longitude, country_code, country_name, city
```

# Security Certification: Hands-On Labs

## Security Analytics

---

### Lab 5-8: Advanced Analytics

- Finding the needle in the haystack
- Comparing time periods
- Identifying Outliers

# Advanced Analytics

## Transactionize → Follow a Transaction

```
((_sourceCategory=Labs/PaloAltoNetworks ",THREAT,") or (_sourceCategory=Labs/PaloAltoNetworks ",TRAFFIC,"  
action=allow)  
| concat(dest_ip,":", dest_port) as destination  
| transactionize src_ip (merge type, destination, src_ip takeFirst)  
| where type matches "*TRAFFIC*" and type matches "*THREAT*"  
| count src_ip, type, destination  
| fields - _count
```

## Transaction → Correlate Traffic Data

```
((_sourceCategory=Labs/security/snort "[Classification: Web Application Attack]") or  
_sourceCategory=Labs/Apache/Access)  
| parse "{TCP} *:* -> *:" as src_ip, src_port, dest_ip, dest_port nodrop  
| parse regex "(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"  
| transaction on src_ip  
  with states %"Labs/security/snort", %"Labs/Apache/Access" in _sourceCategory  
| where %"Labs/security/snort">0 and %"Labs/Apache/Access">0
```

# Security Certification: Hands-On Labs

## Security Analytics

---

### Labs 9-14: Lookups and Data Correlation

- Using Threat Intel Lookup
- Creating Query Templates
- Creating Custom Lookups
- Correlating Data
  - Transaction
  - Transactionize
  - Subqueries

# Monitoring your Data

## Dashboards and Alerts



# Monitoring Your Data

---

## Visualize your data through Dashboards

- Chart your Data
- Create Panels
- Share your Content!

## Receive notification of your Critical Events

- Schedule Your Searches
- Use Webhook Connections to reach your audience
- Create Meaningful Alerts

# Security Certification: Hands-On Labs

## Security Analytics

---

### Labs 15-18: Visualizing and Monitoring

- Create a Dashboard
- Add Panels to an Existing Dashboard
- Create Meaningful Alerts

# Security and Compliance Apps

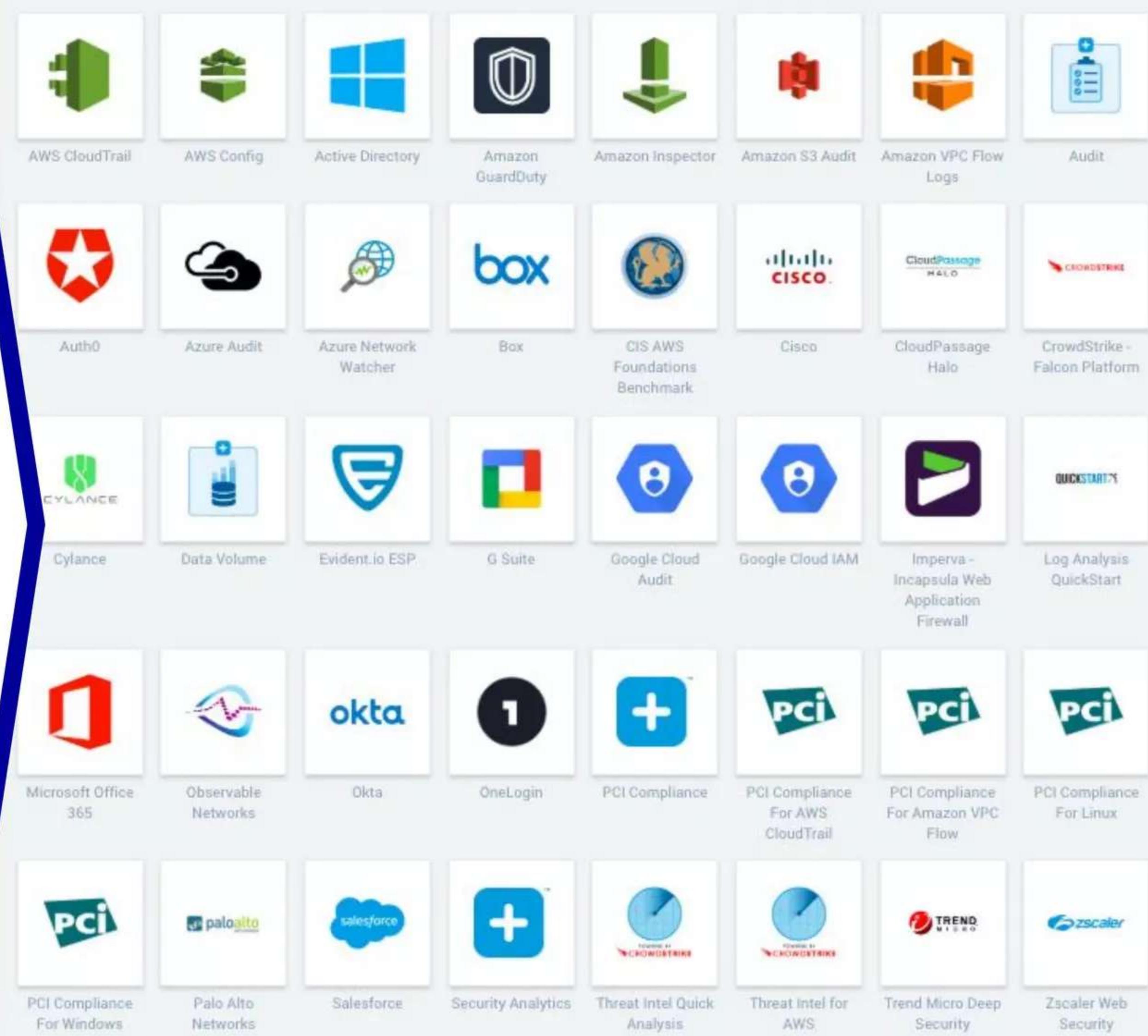
## Out-of-the-Box Content

sumo logic®



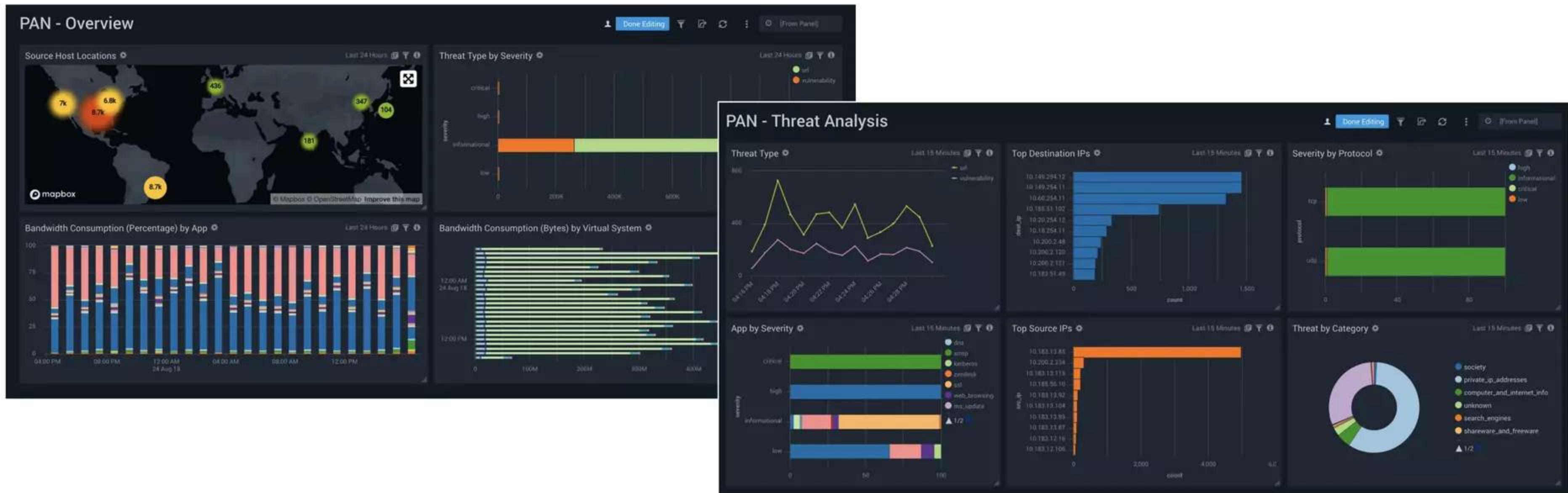
# Security and Compliance Apps

- Simplify Compliance Management
- Set up Real-time monitoring and Alerts
- Security Analytics with Threat Intelligence



# Apps: Palo Alto Networks

Discover threats, consumption, traffic patterns, and other security-driven issues, providing additional insight for investigations.



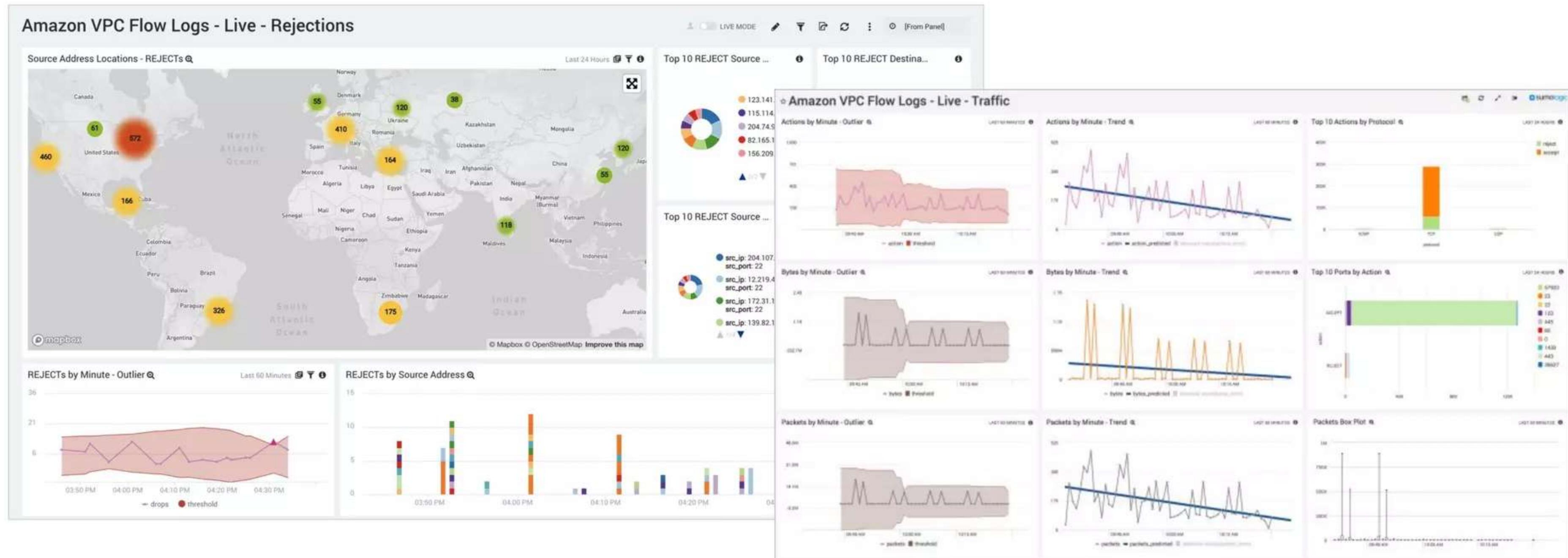
# Apps: AWS CloudTrail

Track user behavior patterns, administrator activity, or correlate with other data sets to get a broader understanding of events from operating systems, intrusion detection systems or application logs.



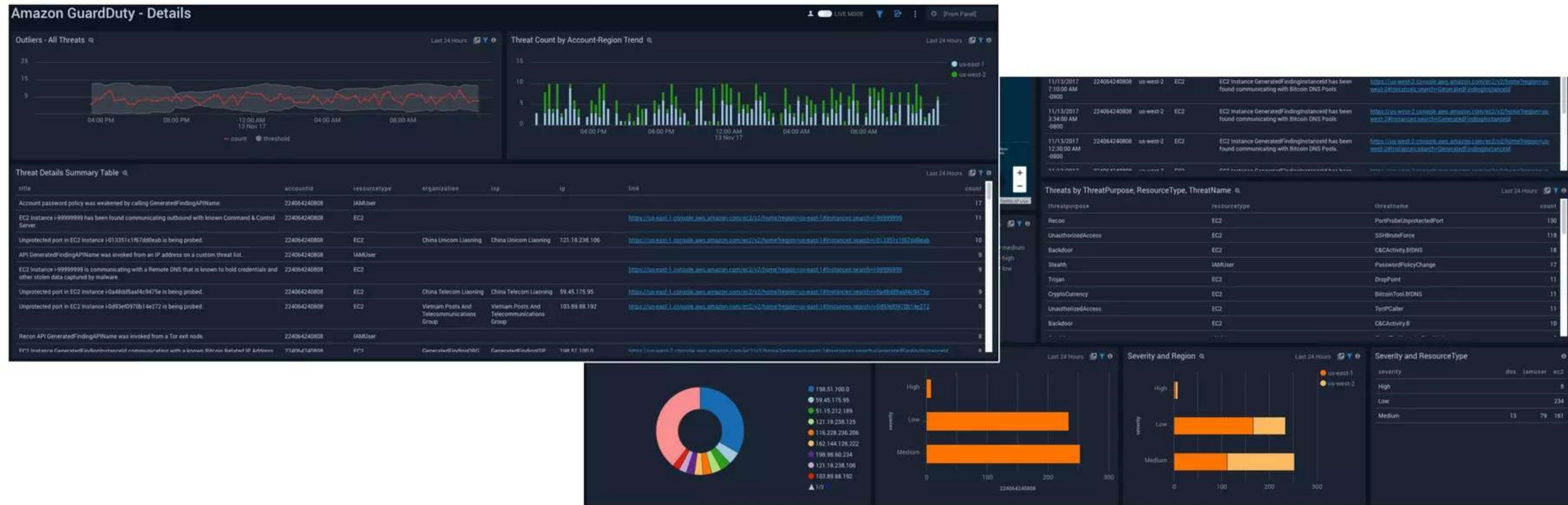
# Apps: AWS VPC Flow Logs

Track your IP network traffic and troubleshoot security issues with real-time visibility and analysis of your environment.



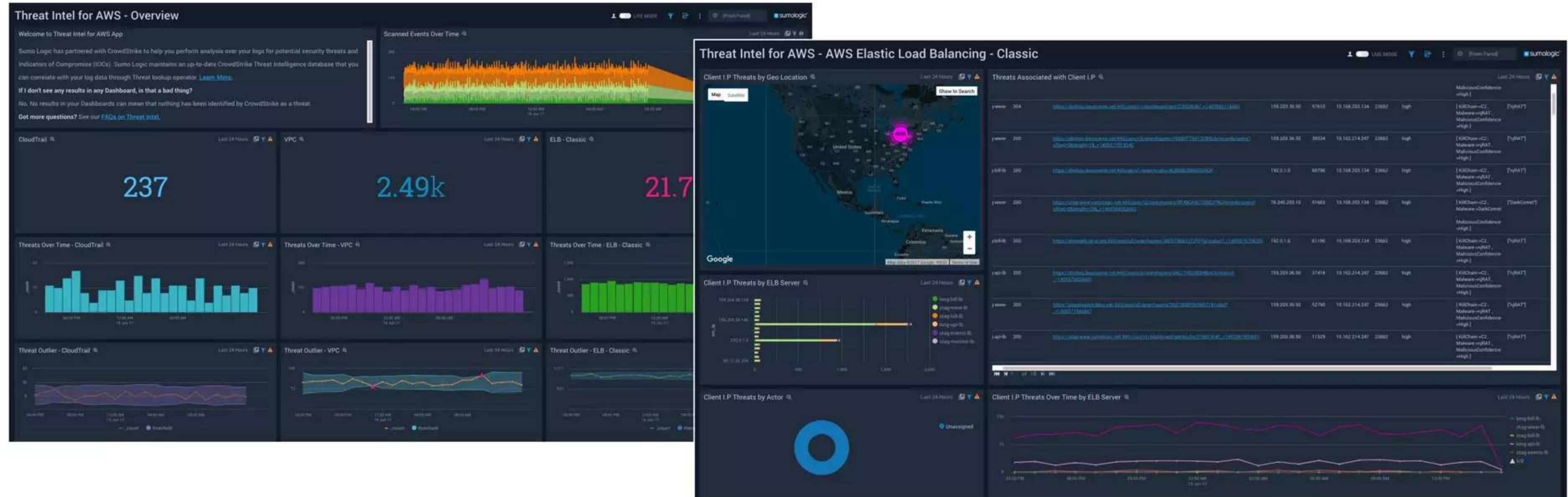
# Apps: AWS GuardDuty

Detect unexpected and potentially malicious activities in your AWS account. Analyze threats by severity, VPC, IP, account ID, region, and resource type. GuardDuty analyzes and processes VPC Flow Logs and AWS CloudTrail event logs.



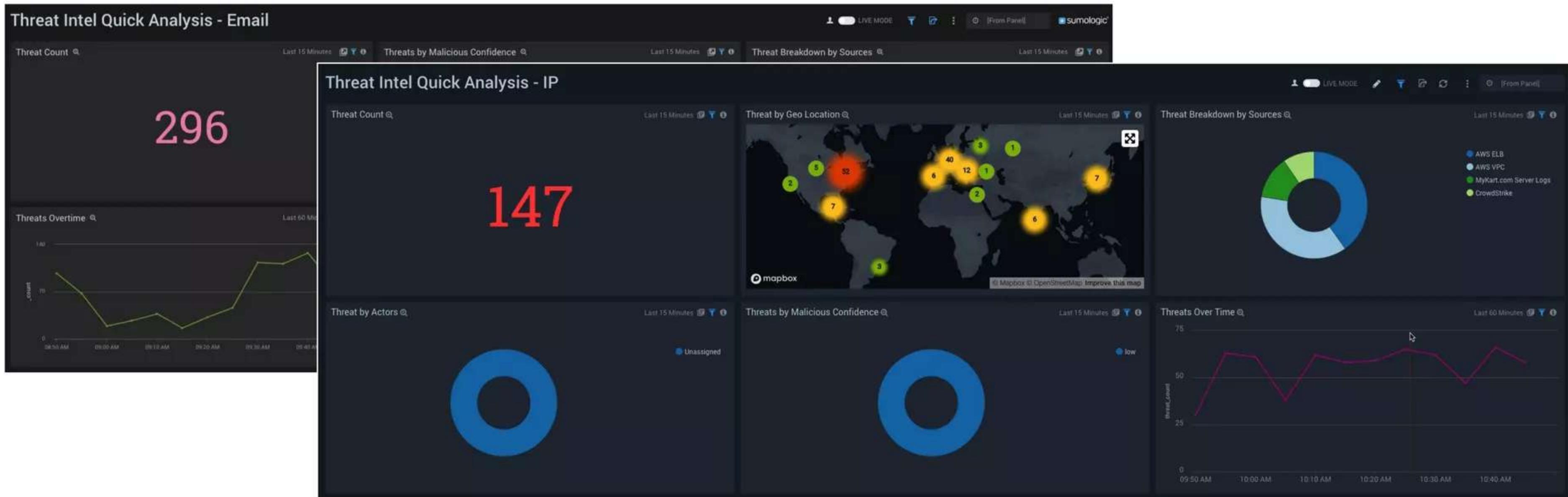
# Apps: Threat Intelligence for AWS

Correlate CrowdStrike threat intelligence data with your AWS log data, for real-time security analytics to detect threats and protect against cyber-attacks. The Threat Intel for AWS App scans AWS CloudTrail, AWS ELB and AWS VPC Flow logs for threats based on IP address.



# Apps: Threat Intelligence Quick Analysis

Correlate CrowdStrike threat intelligence data with your own log data, for real-time security analytics to detect threats and protect against cyber-attacks. This app scans your selected logs for threats based on IP, filename, URL, domain, Hash 256, and email.



# Apps: CrowdStrike

Analyze CrowdStrike security events by type, status and detection method. The CrowdStrike Falcon platform provides Endpoint Detection and Response, Antivirus and Threat Intelligence services via the cloud.



# Apps: O365

Monitor and analyze your complete Office 365 system for administrator and user activity. This app monitors Audit logs for Azure Active Directory, Exchange and SharePoint.



# Security Certification: Hands-On Labs

Using Sumo Logic

---

## Labs 19-20: Sumo Logic Apps

- Installing AWS CloudTrail App
- Installing the Threat Intel App for OSSEC data

# Use Cases

"How To" templates to implement in  
your Environment



# General Use Cases

## How to Create and Alert on Ratios or Percentages

- Outlier

## How to Compare and Alert on Historical Data

- Compare and Outlier

## Detect Patterns and Changes Across Environments and Time

- LogCompare

## Visualize Trends in Your Signatures

- LogReduce and Timeslice

# Security Use Cases

- [Security Queries for PAN \(Firewalls\)](#)
- [Security Queries for AWS](#)
- [Security Queries for Linux](#)
- [Security Queries for Windows](#)

# Where do I go from here?

Training, Docs, Community, Support

sumo logic®



# Need knowledge? → try the **Learn** tab

The screenshot shows the Sumo Logic Learn tab interface. At the top, there's a navigation bar with 'sumologic' logo, a home icon, a menu icon, and a '+ New' button. Below the navigation bar, there are three tabs: 'Home', 'Learn' (which is underlined in blue), and 'Certification'. A callout bubble points to the 'Learn' tab with the text 'Explore the tutorials'.

**Quick Start Videos**

- Sumo Logic Quickstart
- Introduction to Search
- Building Dashboards
- Simplifying Search with Search Templates
- Introduction to Metrics in Sumo

Sumo Logic QuickStart Webinar - August 2018      Introduction to Search      Building Dashboards      Simplifying Search with Search Templates      Introduction to Metrics in Sumo

**Using Sumo Logic Tutorial**

- Part 1: Viewing Data
- Part 2: Search for Log Data
- Part 3: Chart your data
- Part 4: Create and share a dashboard
- Part 5: Modify your dashboard
- Part 6: Create an alert
- Part 7: Get help

**Set Up Sumo Logic Tutorial**

- Part 1: Install a Collector
- Part 2: Add a Source
- Part 3: Install an App and View Data
- Part 4: Try Simple Analytics
- Part 5: Collect and Visualize Host Metrics

Cheat Sheet      Docs      What's New

Ask for Support      Get Training      Community

# Need knowledge? → try the Learn tab

The screenshot shows the Sumo Logic interface with the 'Learn' tab selected. The top navigation bar includes 'sumologic' with a dropdown menu, a home icon, a folder icon, and a '+ New' button. Below the navigation is a horizontal menu with 'Home', 'Learn' (which is underlined), and 'Certification'. The main content area is divided into several sections:

- Quick Start Videos:** A grid of video thumbnails. One thumbnail for 'Simplifying Search with Search Templates' is highlighted with a white border. A white arrow points from this highlighted thumbnail to the text 'Explore the tutorials'.
- Using Sumo Logic Tutorial:** A list of 7 completed steps with green checkmarks:
  - Part 1: Viewing Data
  - Part 2: Search for Log Data
  - Part 3: Chart your data
  - Part 4: Create and share a dashboard
  - Part 5: Modify your dashboard
  - Part 6: Create an alert
  - Part 7: Get help
- Set Up Sumo Logic Tutorial:** A list of 5 steps:
  - Part 1: Install a Collector
  - Part 2: Add a Source
  - Part 3: Install an App and View Data
  - Part 4: Try Simple Analytics
  - Part 5: Collect and Visualize Host Metrics
- Support and Resources:** A row of icons with labels:
  - Cheat Sheet (magnifying glass over a waveform)
  - Docs (document icon)
  - What's New (megaphone icon)
  - Ask for Support (speech bubble with question mark)
  - Get Training (speech bubble with gear and play button)
  - Community (person icon)

Explore the tutorials

Access comprehensive lists of operators and more

# Need knowledge? → try the Learn tab

The screenshot shows the Sumo Logic Learn tab interface. At the top, there are navigation links: Home, Learn (which is underlined in blue), and Certification. Below this is a section titled "Quick Start Videos" featuring five video thumbnails:

- Sumo Logic Quickstart
- Introduction to Search
- Building Dashboards
- Simplifying Search with Search Templates
- Introduction to Metrics in Sumo

Below the videos, there are two columns of tutorials:

- Using Sumo Logic Tutorial**:
  - Part 1: Viewing Data
  - Part 2: Search for Log Data
  - Part 3: Chart your data
  - Part 4: Create and share a dashboard
  - Part 5: Modify your dashboard
  - Part 6: Create an alert
  - Part 7: Get help
- Set Up Sumo Logic Tutorial**:
  - Part 1: Install a Collector
  - Part 2: Add a Source
  - Part 3: Install an App and View Data
  - Part 4: Try Simple Analytics
  - Part 5: Collect and Visualize Host Metrics

At the bottom right of the interface, there are several links with icons:

- Cheat Sheet (magnifying glass over a chart)
- Docs (document icon)
- What's New (megaphone icon)
- Ask for Support (speech bubble with question mark)
- Get Training (speech bubble with green checkmark)
- Community (person icon)

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

# Need knowledge? → try the Learn tab

The screenshot shows the Sumo Logic interface with the 'Learn' tab selected. At the top, there are 'Quick Start Videos' including 'Sumo Logic Quickstart', 'Introduction to Search', 'Building Dashboards', 'Simplifying Search with Search Templates', and 'Introduction to Metrics in Sumo'. Below this, there are two columns of tutorials:

- Using Sumo Logic Tutorial:**
  - Part 1: Viewing Data
  - Part 2: Search for Log Data
  - Part 3: Chart your data
  - Part 4: Create and share a dashboard
  - Part 5: Modify your dashboard
  - Part 6: Create an alert
  - Part 7: Get help
- Set Up Sumo Logic Tutorial:**
  - Part 1: Install a Collector
  - Part 2: Add a Source
  - Part 3: Install an App and View Data
  - Part 4: Try Simple Analytics
  - Part 5: Collect and Visualize Host Metrics

At the bottom right, there are links for 'Cheat Sheet', 'Docs', 'What's New', 'Ask for Support', 'Get Training', and 'Community'. A callout bubble points to the 'What's New' link.

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

# Need knowledge? → try the Learn tab

The screenshot shows the Sumo Logic Learn tab interface. At the top, there are navigation links: Home, Learn (which is underlined in blue), and Certification. Below this, the "Quick Start Videos" section displays five video thumbnails with titles: "Sumo Logic Quickstart", "Introduction to Search", "Building Dashboards", "Simplifying Search with Search Templates", and "Introduction to Metrics in Sumo". Each thumbnail includes a play button icon. Below the videos, there are two sections: "Using Sumo Logic Tutorial" and "Set Up Sumo Logic Tutorial". The "Using Sumo Logic Tutorial" section lists seven completed steps with green checkmarks: Part 1: Viewing Data, Part 2: Search for Log Data, Part 3: Chart your data, Part 4: Create and share a dashboard, Part 5: Modify your dashboard, Part 6: Create an alert, and Part 7: Get help. The "Set Up Sumo Logic Tutorial" section lists five steps: Part 1: Install a Collector, Part 2: Add a Source, Part 3: Install an App and View Data, Part 4: Try Simple Analytics (this step is grayed out), and Part 5: Collect and Visualize Host Metrics. To the right of these sections is a sidebar with several icons: "Cheat Sheet" (magnifying glass over a chart), "Docs" (document icon), "What's New" (megaphone icon), "Ask for Support" (speech bubble with question mark), "Get Training" (speech bubble with gear icon), and "Community" (person icon). A white line connects the "Community" icon to a callout bubble on the right.

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

# Need knowledge? → try the Learn tab

The screenshot shows the Sumo Logic Learn tab interface. At the top, there are navigation links: Home, Learn (which is underlined in blue), and Certification. Below this, the "Quick Start Videos" section displays five video thumbnails with titles: "Sumo Logic Quickstart", "Introduction to Search", "Building Dashboards", "Simplifying Search with Search Templates", and "Introduction to Metrics in Sumo". Each thumbnail includes a play button icon. Below the videos, there are two sections: "Using Sumo Logic Tutorial" and "Set Up Sumo Logic Tutorial". The "Using Sumo Logic Tutorial" section lists seven completed steps with green checkmarks: Part 1: Viewing Data, Part 2: Search for Log Data, Part 3: Chart your data, Part 4: Create and share a dashboard, Part 5: Modify your dashboard, Part 6: Create an alert, and Part 7: Get help. The "Set Up Sumo Logic Tutorial" section lists five steps: Part 1: Install a Collector, Part 2: Add a Source, Part 3: Install an App and View Data, Part 4: Try Simple Analytics (this step is grayed out), and Part 5: Collect and Visualize Host Metrics. To the right of these sections are several icons: "Cheat Sheet" (magnifying glass over a chart), "Docs" (document icon), "What's New" (megaphone icon), "Ask for Support" (speech bubble with question mark), "Get Training" (speech bubble with green checkmark), and "Community" (person icon). A white callout box with a black border and a white arrow points from the "Get Training" icon towards the text "Attend/review training and get certified".

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

# Need knowledge? → try the Learn tab

The screenshot shows the Sumo Logic interface with the 'Learn' tab selected. At the top, there's a navigation bar with 'sumologic' logo, a home icon, a 'New' button, and tabs for 'Home', 'Learn' (which is underlined), and 'Certification'. Below the navigation is a section titled 'Quick Start Videos' featuring five video thumbnails:

- Sumo Logic Quickstart
- Introduction to Search
- Building Dashboards
- Simplifying Search with Search Templates
- Introduction to Metrics in Sumo

Below the videos, there are two columns of tutorials:

- Using Sumo Logic Tutorial**:
  - Part 1: Viewing Data
  - Part 2: Search for Log Data
  - Part 3: Chart your data
  - Part 4: Create and share a dashboard
  - Part 5: Modify your dashboard
  - Part 6: Create an alert
  - Part 7: Get help
- Set Up Sumo Logic Tutorial**:
  - Part 1: Install a Collector
  - Part 2: Add a Source
  - Part 3: Install an App and View Data
  - Part 4: Try Simple Analytics
  - Part 5: Collect and Visualize Host Metrics

On the right side of the interface, there are several icons:

- Cheat Sheet (magnifying glass over a chart)
- Docs (document icon)
- What's New (megaphone icon)
- Ask for Support (speech bubble with question mark)
- Get Training (speech bubble with gear)
- Community (person icon)

A white callout box with a blue arrow points from the 'Ask for Support' icon to the text 'Open a Support case'.

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

# Need knowledge? → try the Learn tab

The screenshot shows the Sumo Logic Learn tab interface. At the top, there are navigation icons for Home, Learn (which is underlined), and Certification, along with a '+ New' button. Below this, the 'Quick Start Videos' section displays five video thumbnails with titles: 'Sumo Logic Quickstart', 'Introduction to Search', 'Building Dashboards', 'Simplifying Search with Search Templates', and 'Introduction to Metrics in Sumo'. Each thumbnail includes a play button icon. Below the videos, there are two sections: 'Using Sumo Logic Tutorial' and 'Set Up Sumo Logic Tutorial', each listing numbered steps with green checkmarks. To the right of these sections are several utility icons: 'Cheat Sheet' (magnifying glass over a waveform), 'Docs' (document icon), 'What's New' (megaphone icon), 'Ask for Support' (speech bubble with question mark), 'Get Training' (speech bubble with gear), and 'Community' (person icon). The bottom of the page features the Sumo Logic logo.

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

# Questions?

# Security Labs

<https://bit.ly/2MyZ7vi>



In order to get credit for the exam,  
In YOUR OWN INSTANCE, go to  
Certification Tab.

- Online Exam
- 30 Multiple choice questions
- 60-minute time limit
- 3 attempts

The image shows a snippet of a website for a Sumo Logic certification. At the top is a circular badge with a blue plus sign in the center, surrounded by the text "CERTIFIED PROFESSIONAL" at the top and "SUMO SECURITY USER" on a banner below it, with "SUMO LOGIC" at the bottom. Below the badge, the text "Sumo Security Power User" is displayed. Further down, it says "ONLINE EXAM: 30 QUESTIONS | 60 MINUTES" and "PREP: SECURITY ANALYTICS WEBINAR & HANDS ON LABS". A pink arrow points to a blue button labeled "Take the Exam". Below the button is a link "Learn More". The background features abstract blue and red lines.

CERTIFIED PROFESSIONAL

SUMO SECURITY USER

SUMO LOGIC

Sumo Security Power User

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: SECURITY ANALYTICS WEBINAR &

HANDS ON LABS

This certification is valid for one year

Take the Exam

Learn More

s

u

Empowering the  
people who power  
modern business

m

o

sumo logic