Sumo Logic Security and Compliance Certification

sumo logic

Agenda:

55 min: Presentation & Labs

10 min: Break

40 min: Labs

1 hr: Exam

Welcome!
Note you are currently muted.
We will get started shortly.

● This session is being recorded

Course Agenda

- 10 min. — Introduction to Security and Compliance
- 5 min. — Security Demo
- 105 min. — **Hands On Labs:**
  - 50 min. — Labs 1-5: Starter SOC dashboard with lookup filters
  - 10 min. — Break
  - 45 min. — Labs 6-8: Export Starter SOC dashboard, Compliance, Threat Intel with Crowdstrike
- 60 min. — Sumologic Certification for Security & Compliance

Sumo Logic Machine Data Analytics Platform

Continuous Intelligence for Applications & Infrastructure

sumo logic

Sumo Logic Confidential

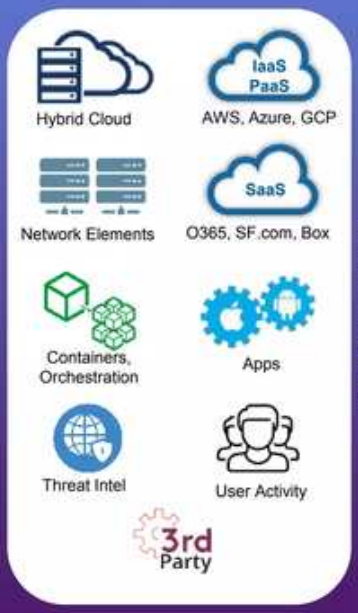

DEMO

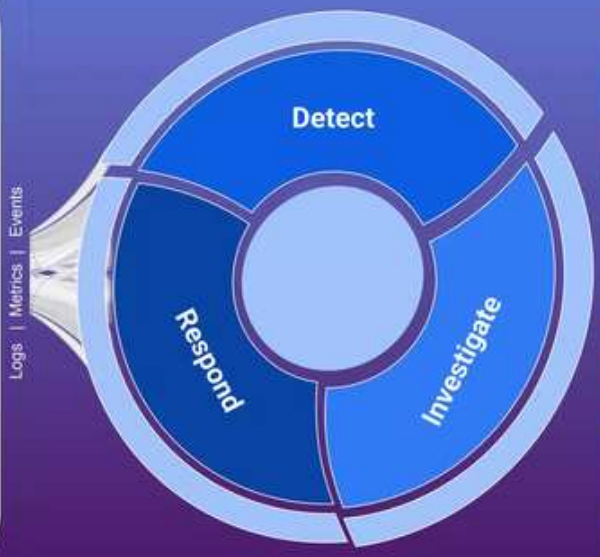
Centralized log management is key to your security

Gaps	Shifts	Human Scale
		
Transformation to cloud producing gaps in visibility	Shifts happening in threat landscape	Security operation is no long a human scale problem

Your data in one centralized log management source gets you to that single pane of glass SOC.

Detect, investigate, and respond in real-time





- Meet compliance deadlines
- Reduce security risks

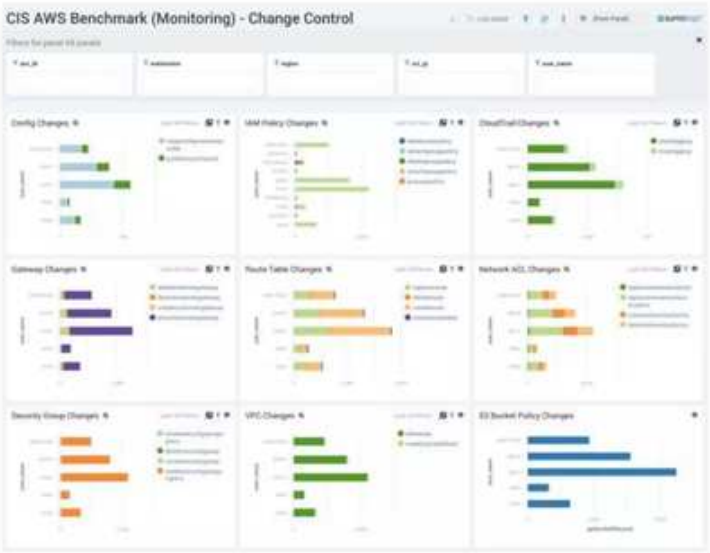
- Identify potential security breaches
- Neutralize new threat patterns

- Transform reactive/ manual processes into integrated /proactive/ automated

sumo logic

Sumo Logic Confidential

Compliance



- ✓ Pre-built PCI compliance content for Firewall, AWS, Linux, and Windows
- ✓ Deploy and monitor controls for PCI, CIS, and HIPAA regulations
- ✓ Detect & respond to configuration drifts, changes, and misconfigurations
- ✓ Monitor & enforce your enterprise security & compliance on cloud
- ✓ Built on a FedRAMP Ready platform

Delivering Security & Compliance from the Cloud

Global view of all security threats

Out-of-the-box Apps for AWS, Office365, GCP, Salesforce, Okta, Palo Alto

Machine learning to detect anomalies

Compliance insights and full stack security visibility

Integration with 3rd party security technology solutions such as Cisco, Cylance, Kubernetes,

Integrated threat intelligence (Crowdstrike, GuardDuty, etc.)

Security visibility into hybrid and multicloud tools

SPS COMMERCE

With Sumo Logic, I can now see threats that are happening, and quickly react to those threats"

Milinda Rambel Stone
Sr. Director of Security

sumo logic

Sumo Logic Confidential

Login to training environment and go to labs

Training Environment:

url: service.sumologic.com

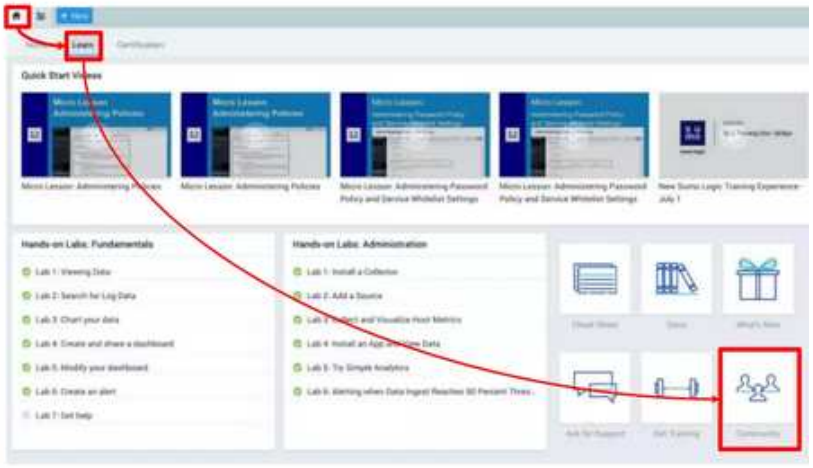
email: training+labs@sumologic.com

password: Sumo2020!

Hands-on Labs:

In chat click this link I shared

https://help.sumologic.com/01Start-Here/Quick-Start-Tutorials/Hands-on_Labs%3A_Security_and_Compliance

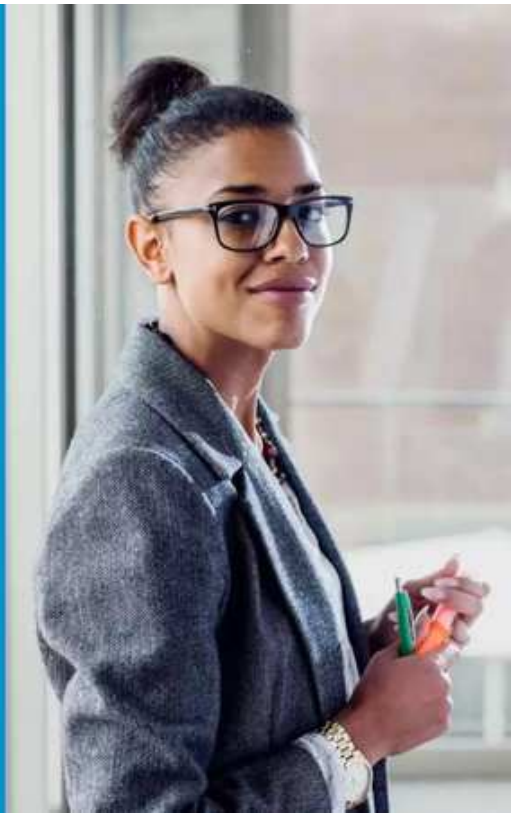


Reference Slides follow

Search and Parse

Filter and Provide Structure

sumo logic



Data Analytics ⇨ Query Syntax

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

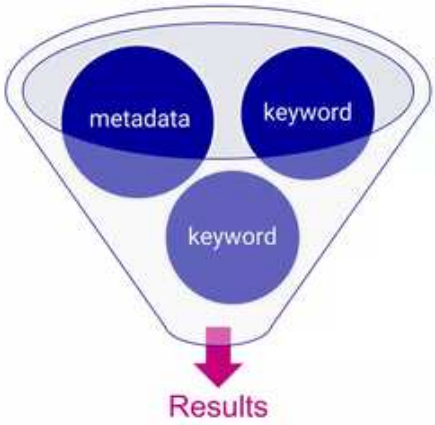
Sumo Logic Confidential

Data Analytics ⇨ Query Syntax

Use metadata and keywords to narrow your search scope

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```



Data Analytics ⇨ Query Syntax

Extract meaningful fields to provide structure to your data

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```

Parse Anchor:

```
| parse " *@* " as user,domain
```

Parse Regex:

```
| parse regex "(?<src_ip>\d{1,3}
\.\d{1,3}\.\d{1,3}\.\d{1,3})"
```

Other Parse Operators:

```
csv, json, keyvalue, split, xml
```

Learn more: Parse Operators

Data Analytics ⇨ Query Syntax

Further filter results using your extracted fields

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```

where operator:

```
| where !(status_code=304)
```

in operator:

```
| if(status_code in("501","502"),
"Error","OK") as code_type
```

Other Filter Operators:

```
join, lookup, matches, filter,
isEmpty, isNull, isBlank
```

Learn more: Filter operator example

Data Analytics ⇨ Query Syntax

Evaluate messages and place them into groups

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```

count operator:

```
| count by status_code
```

avg operator:

```
| avg(size) by src_ip
```

pct operator:

```
| pct(filesize,75) by _sourceHost
```

Other Aggregation Operators:

```
sum, count_distinct, stddev, min, max
```

Learn more: Aggregation operators

Data Analytics ⇨ Query Syntax

Format to display desired results succinctly

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```

top operator:

```
| top 5 src_ip by avg_size
```

fields operator:

```
| fields src_ip, avg_size
```

transpose operator:

```
| transpose row src_ip column url
```

Other formatting Operators:

```
format, formatdate, limit, sort
```

Learn more: Trends over time using transpose

Sumo Logic Confidential

Search and Parse

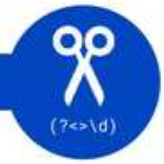
Search and **Filter** your data

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

Simple Analytics

Conditional Logic, Filtering, Formatting Results

sumo logic

Simple Analytics

Aggregation

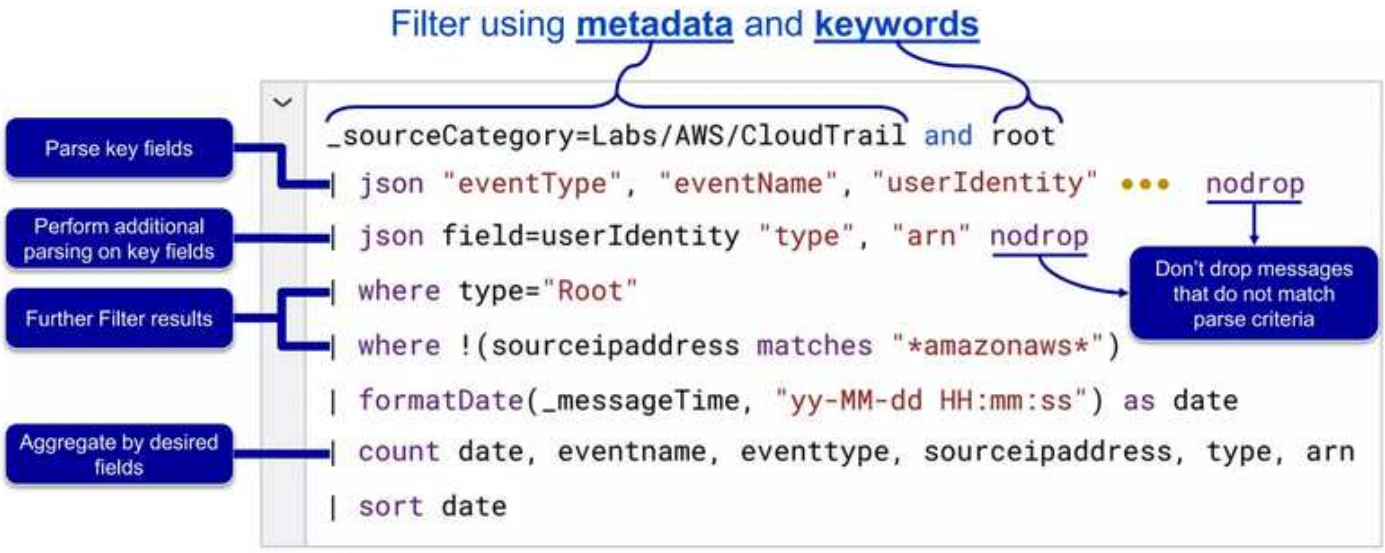
```
| count[]
| sum
| avg
| min()
| max()
```

Conditional

```
| if()
| []matches[]
| <>in()
| filter
| where
```

Formatting

```
| transpose
| fields
| limit
| sort by
| top
```


Filter using metadata and keywords
Parse key fields
Perform additional parsing on key fields
Further Filter results
Aggregate by desired fields
Don't drop messages that do not match parse criteria
_sourceCategory=Labs/AWS/CloudTrail and root
| json "eventType", "eventName", "userIdentity" ••• 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

Advanced Analytics

Outliers, Trends, Needle in the Haystack

sumo logic

Advanced Analytics

LogReduce → New security attacks/breaches.

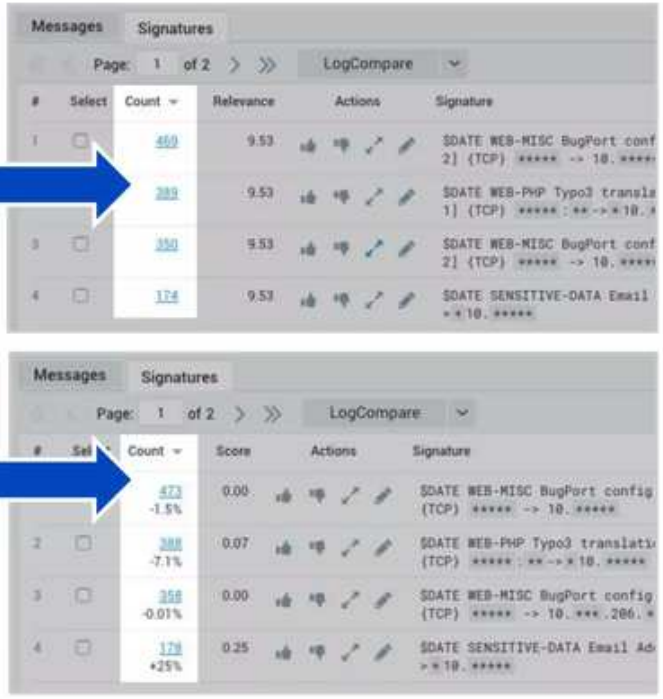
Find the "needle in the haystack" by identifying patterns.

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

LogCompare → Compare attacks/breaches to other time periods.

Compare today's patterns with patterns in the past.

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



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
```

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/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/snort", %"Labs/Apache/Access" in _sourceCategory
| where %"Labs/snort">0 and %"Labs/Apache/Access">0
```

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

sumo logic

Apps: Palo Alto Networks

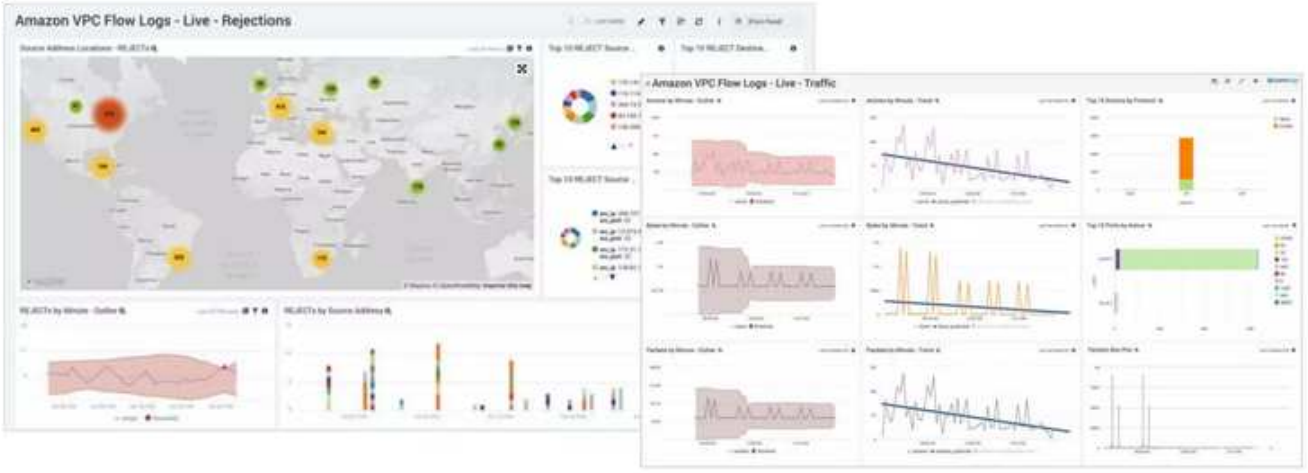
Discover threats, consumption, traffic patterns, and other security-driven issues, providing additional insight for investigations.

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.

Out-of-the-box Security Content

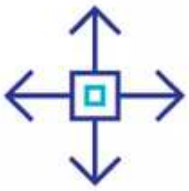
*Add-on Cloud SIEM Enterprise option

Global Intelligence

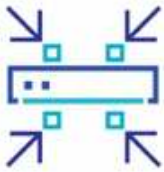
for Amazon GuardDuty 3.0

sumo logic

Amazon GuardDuty: 12 threat purposes



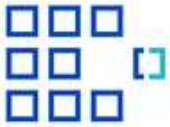
unusual outbound:
network ports / suspicious
IP / data transfer



inbound connections
from suspicious IP

Recon: suspicious
port scan

PenTest



launching EC2
instances

bitcoin mining
on EC2

unusual API calls to change
permissions

root credential usage

privilege escalation

Disabling CloudTrail
or modifying
password policy

sumo logic

Sumo Logic Confidential

Example: Which is more risky?

bitcoin mining on your EC2 instances

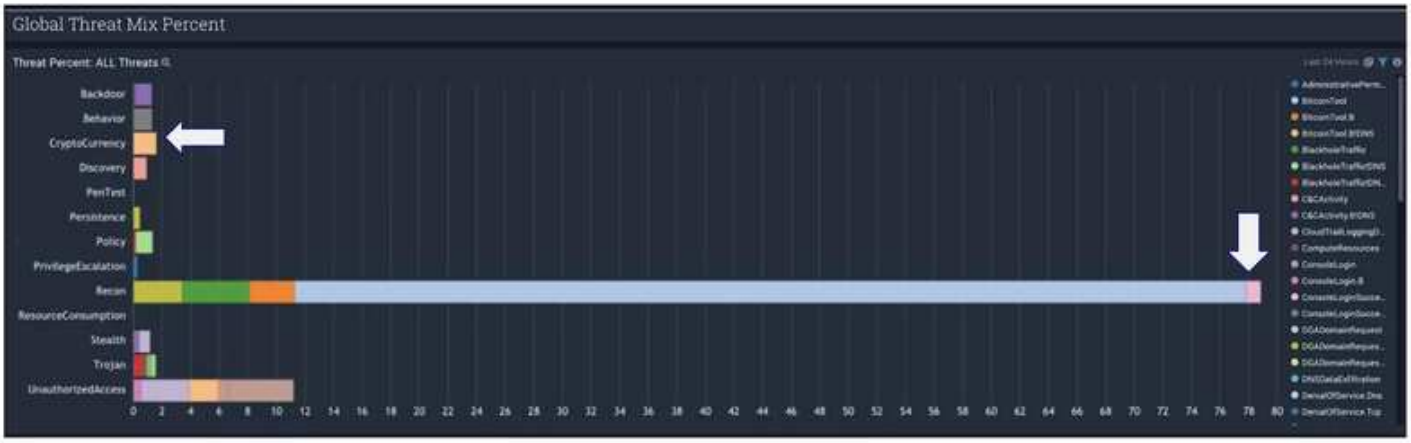
Recon: suspicious port scan

Choices:
(A)bitcoin mining
(B)Recon
(C)No idea

Sumo Logic Confidential

Example: Which is more risky?

Does global context help?



Too many false positives

Posted by u/CyberOwl_01 4 months ago

53

Is GuardDuty a false positive hero?

monitoring

So I understand that Guard duty is all about historical anomalies (never seen this before type) but that's literally causing too many false positives. We have no way of teaching Guard duty model. Does anyone use Guard duty for monitoring. What is your experience? What has worked for you?

34 Comments Share Save Hide Report

91% Upvoted

https://www.reddit.com/r/aws/comments/dgfos0/is_guardduty_a_false_positive_hero/

Global Intelligence for Amazon GuardDuty 3.0

As a SecOps users, use insights from Sumo Logic customers to prioritize and act on Amazon GuardDuty threats

1

What threats are customers experiencing?

2

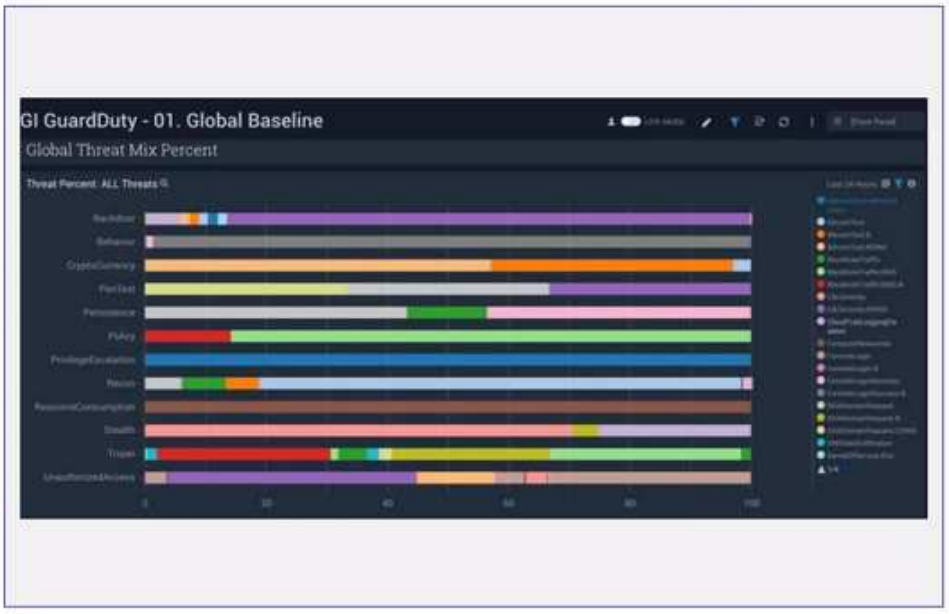
How does my company compare?

3

What should we do?

What threats are customers experiencing?

1



Global Threat Mix

Global Threat Share

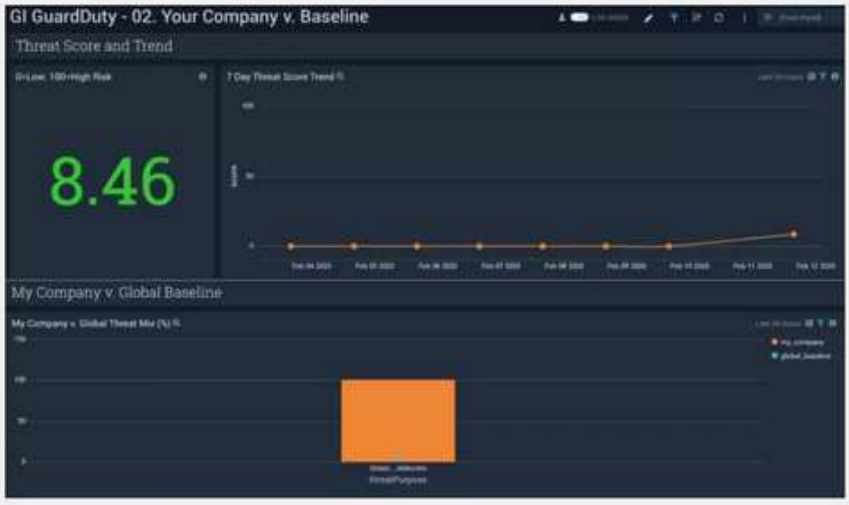
Global Threat Map

Rare threats

Sumo Logic Confidential

How does my company compare?

2



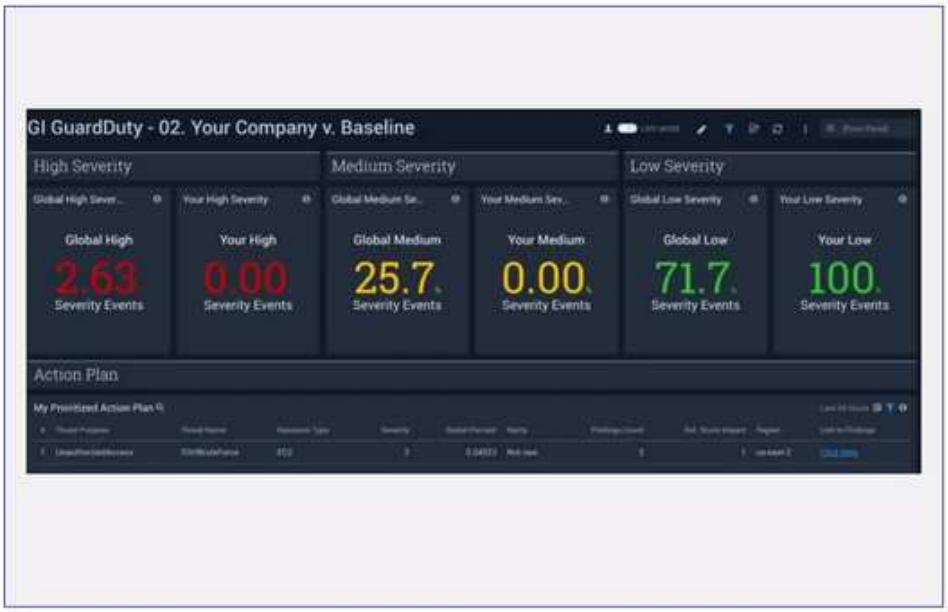
Threat score (100 = high risk)

Threat score trend

My Company v. Global Baseline of threats

What should we do?

3



Action plan by affected resource

Priority

- findings count
- severity
- unusualness compared to baseline

Sumo Logic Confidential

Global Intelligence

for AWS CloudTrail 1.0

sumo logic

Example of a breach

0. Get AWS credentials from public repositories -> run AWS SDK
1. `EC2_ListSecurityGroups*` -> find EC2 instances with open ports to open a remote session on machine (MITRE: Discovery)
2. `EC2_List instances*` -> find IAM profiles associated with EC2 instances (MITRE: Discovery)
3. `IAM_CreateUpdatePolicy*` to add S3 read privileges to EC2's IAM role (MITRE: Privilege Escalation)
4. Connect to S3 bucket using role and read all data (MITRE: Exfiltration)

*Notable events in AWS CloudTrail- detect & prioritize to reduce breach risk

See https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

Sumo Logic Confidential

Global Intelligence for AWS CloudTrail

As a SecOps user, use insights from Sumo Logic customers to detect and prioritize notable security events in AWS CloudTrail

1. How does my *attack surface* compare to peers?
2. How do my *notable events* compare to peers?
3. What should we do?

How does my attack surface compare to peers?

1

AWS services covered

- EC2
- S3
- IAM
- RDS
- Redshift
- Lambda
- CloudTrail

Cohorts based on:

- Variety - Unique AWS services in use (e.g. EC2, S3)
- Volume- Count of resources
- Velocity - Create, Update, Delete events

Correlated with breach risk

How do my notable events compare to peers?

2

Notable event counts v. peers by MITRE Att&ck Framework

- Credential Access
- Defense Evasion
- Discovery
- Execution
- Exfiltration
- Initial Access
- Lateral Movement
- Persistence
- Privilege Escalation

How do my notable events compare to peers?

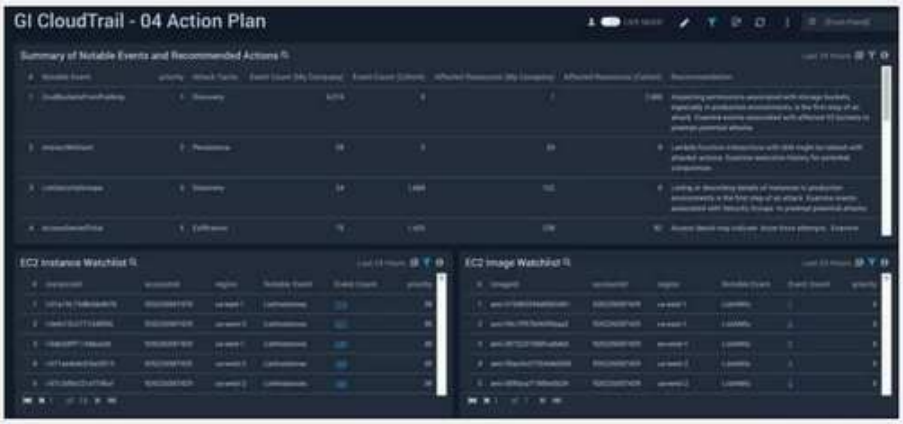
2

Count resources affected by notable events v. peers

- EC2 (instances, AMIs)
- S3 (buckets)
- IAM (user, roles, policies)
- RDS (cluster, instances)
- Redshift (cluster)
- Lambda (functions)
- CloudTrail (trails)

What should we do?

3



Action plan by affected resource

- EC2 (instances, AMIs)
- S3 (buckets)
- IAM (user, roles, policies)
- RDS (cluster, instances)
- Redshift (cluster)
- Lambda (functions)
- CloudTrail (trails)

Priority - Unusualness of Event Count x Number of Resources

End of Reference Slides

Questions?

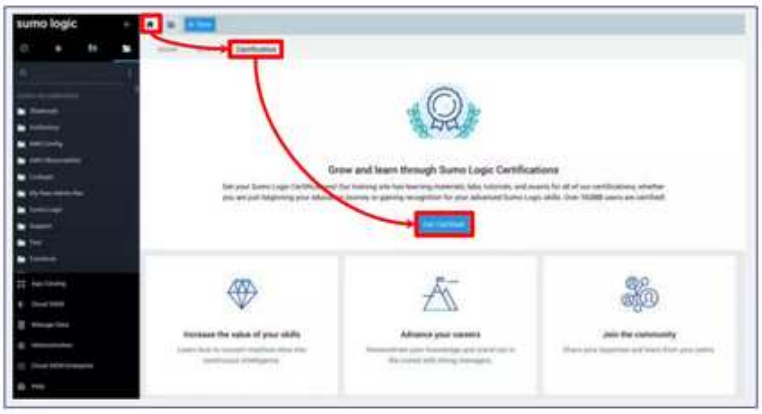
Assessment

Assessment Description

- 30 questions coming from a pool of questions
- 60 minutes to take it
- Need a 75% to pass
- Open Resource (slides, labs, and documentation)

Certification

In order to get credit for the exam, go to **your own Sumo account and login**
(your company account, not the training account)



Assessment:

1. Click  > **Certification**
2. Click **Get Certified**
3. Click **<course category>**
4. **Click <course name>**
5. Click Register | FREE
6. Under **Read Me First,** click **Before you start**
7. Click Next
8. Click **START ASSESSMENT**

If you find your login is cycling back to the exam screen, do the following:

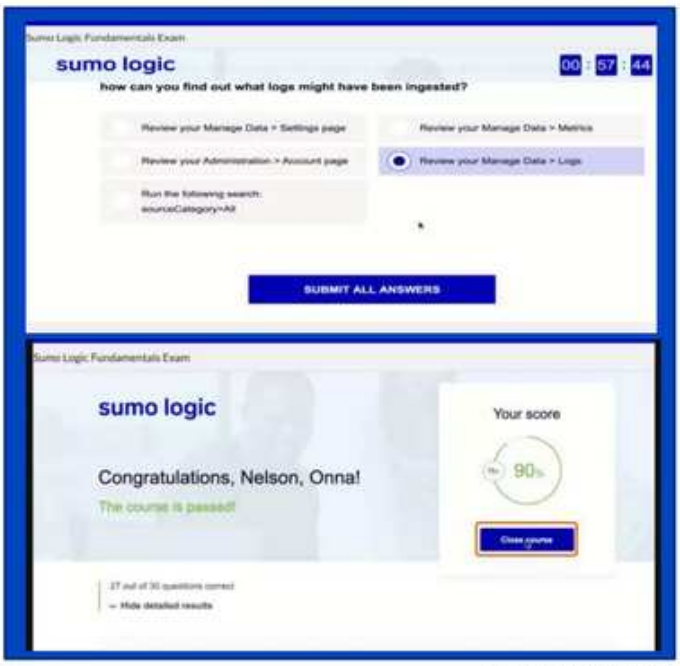
- Click on Help in the black left bar
- Click Community in the black left bar
- An email verification should be sent
- Once you verify, you should able to take the exam without any issues

sumo logic

In order to get credit for the assessment

Follow these steps:

1. After each section, click **Next** or **Submit**
2. When you get to the last section, click **Go to results**
3. When you passed the class, you'll get a congratulations message. Then click **Submit results**.
4. After your feedback, you can click **Close course**



Sumo Logic Confidential

For passing the exam, you will earn:

- A Certificate
- An invitation to our LinkedIn Group
- The respect of your peers
- Fame, Fortune and more...

How did we do?

Please take our survey:
https://forms.gle/2KMtxPuD9cSYV8SJ6

sumo logic


s
u
Empowering the
people who power
modern business
m
o
sumo logic