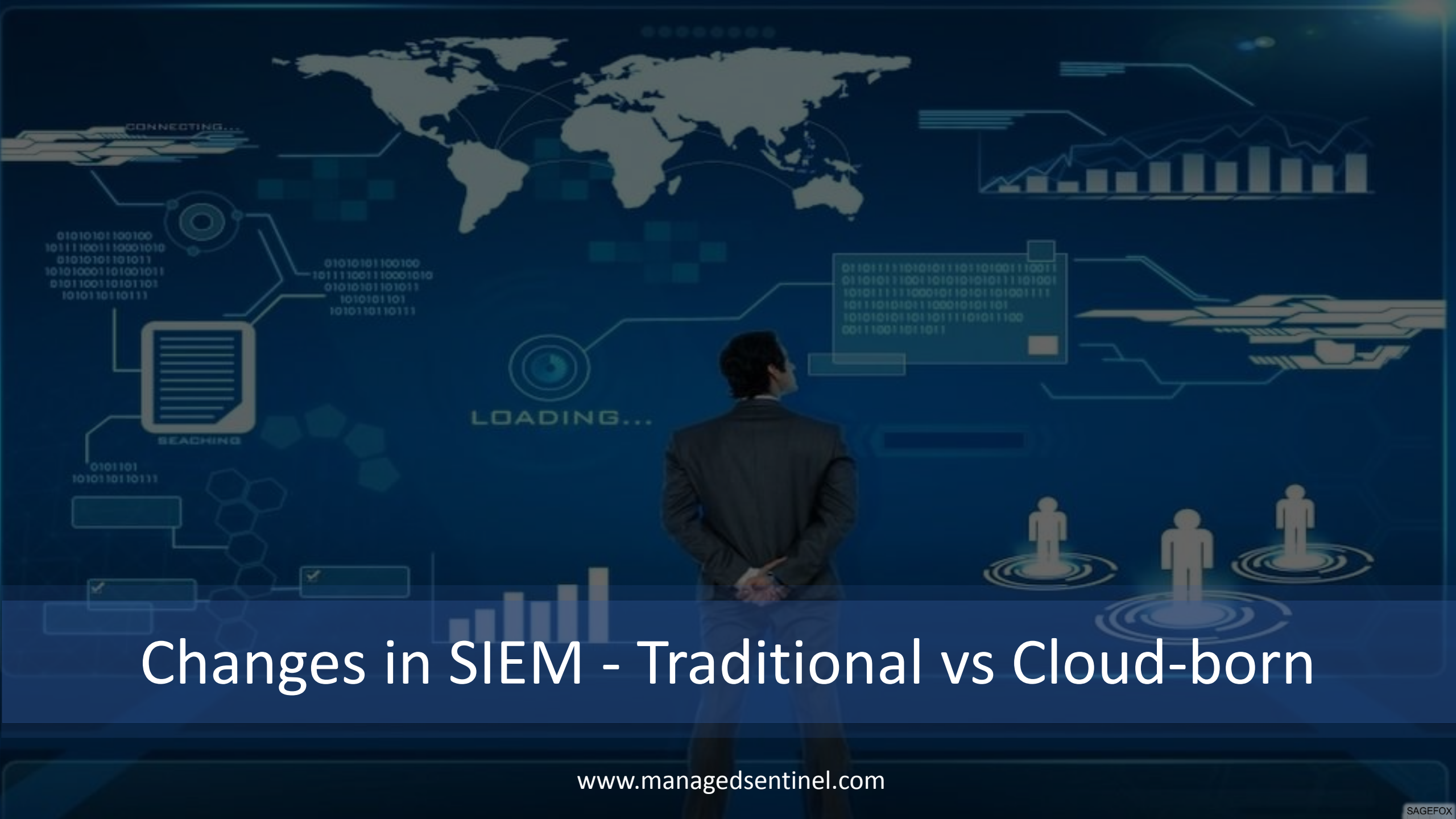




Changes in SIEM - Traditional vs Cloud-born

Security Information and Events Management

- Term coined by by Mark Nicolett and Amrit Williams of Gartner in 2005
- Different acronyms used SIM, SEM, SELM, often misspelled as SEIM

SIEM Evolution

Mid 1990s

Centralized log collection
Basic query abilities (grep)

Mid 2000s

Compliance driven (PCI, SOX, HIPPA)
Emphasis on correlation, normalization

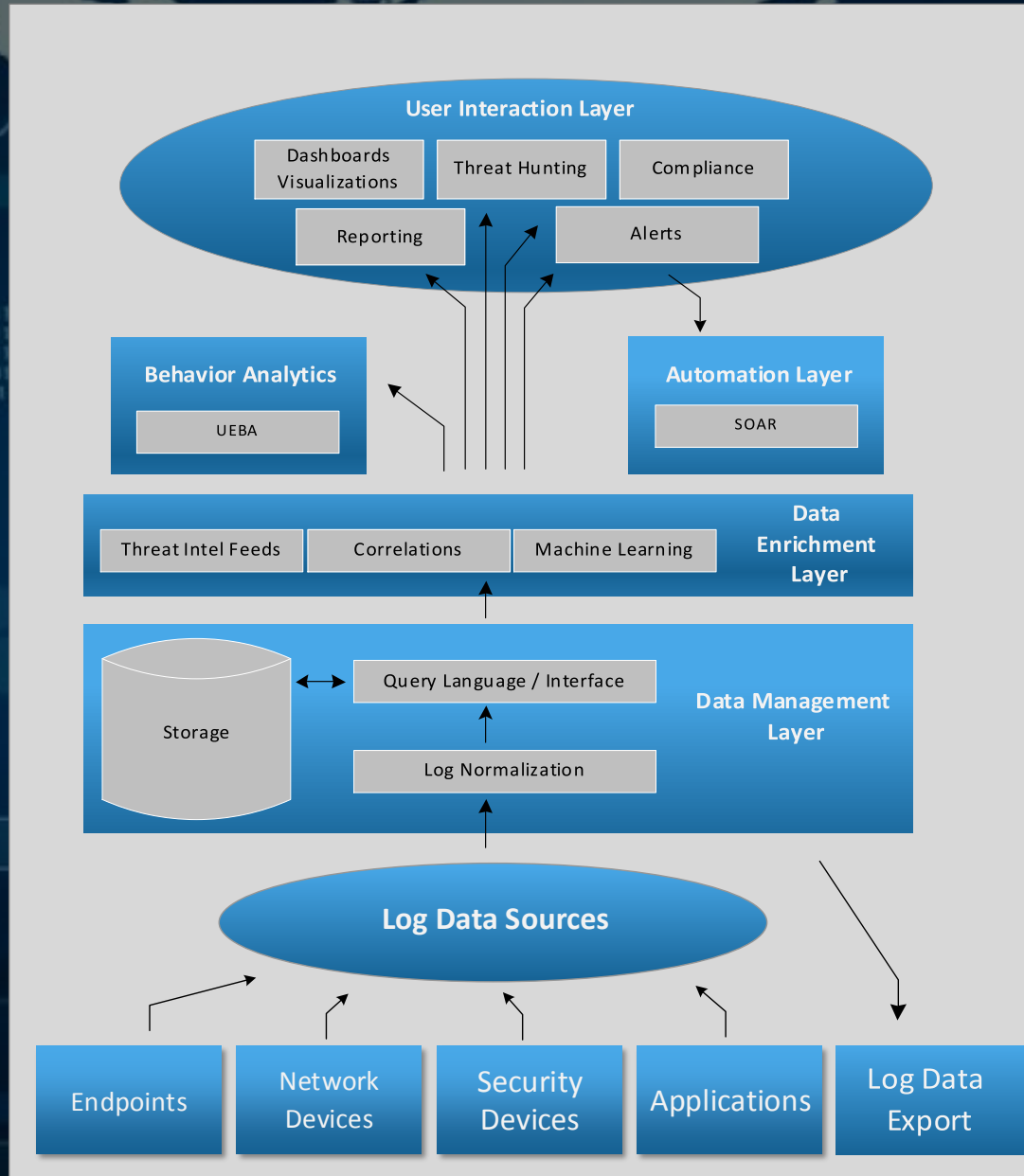
Mid 2010s

Big data
Machine Learning
Threat Hunting

Present

Cloud Migrations
Threat Intelligence / SOAR
Behavior Analysis

SIEM Architecture

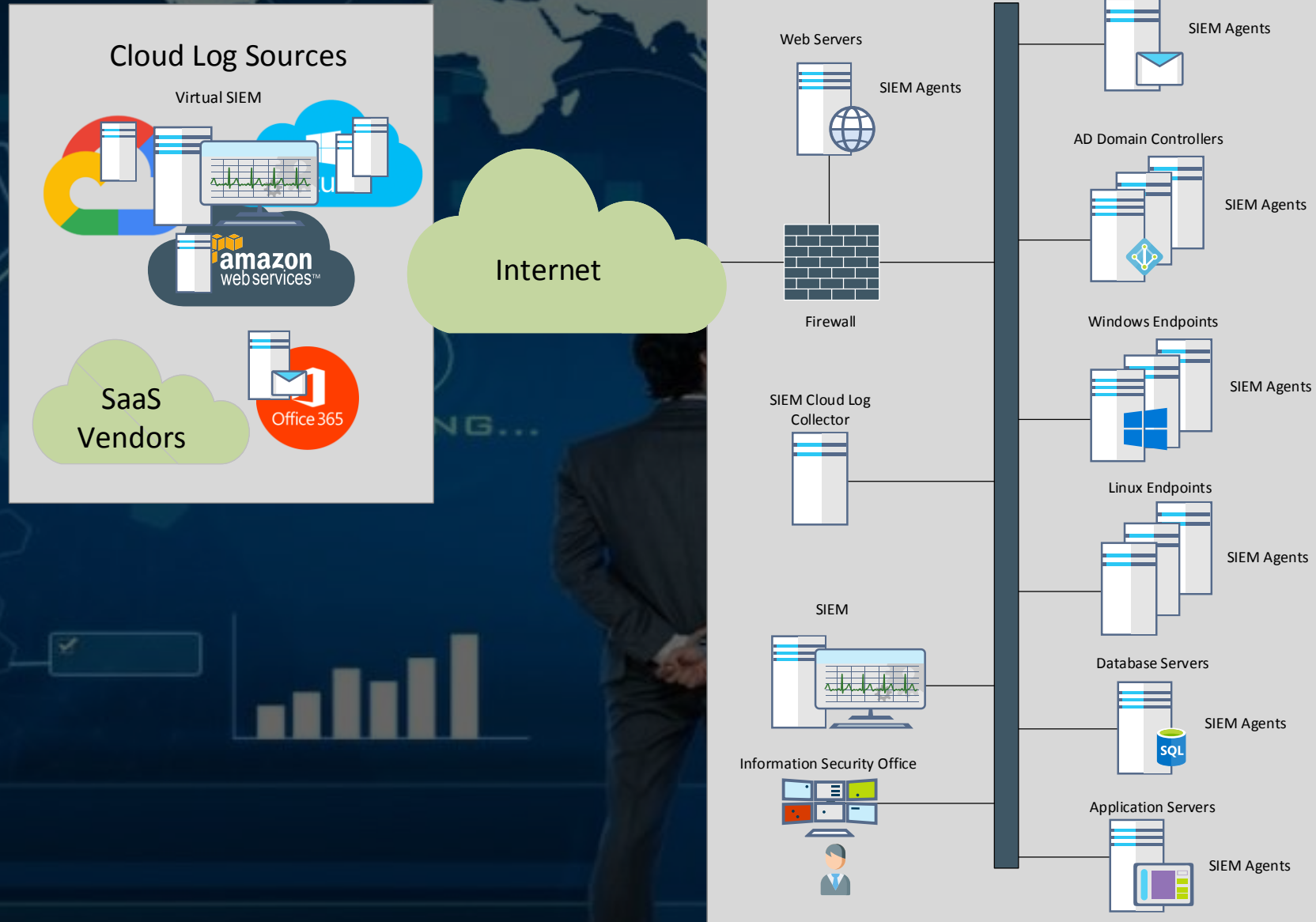


SIEM Vendors



Source: Gartner (December 2018)

Traditional SIEM Deployment



Traditional SIEM Challenges

Initial Costs

Prohibitive upfront capital required for hardware, maintenance, licenses and deployment.

Operating Costs

High operational costs for hosting, management and monitoring of traditional SIEM platforms

Data volume

Large volume of logs collected and stored in SIEM are artificially increasing the on-premises SIEM capacity and license requirements.



There is no cloud
It's just someone else's
computer

Cloud

Limited visibility into the organization's public and private cloud assets.

Use-cases

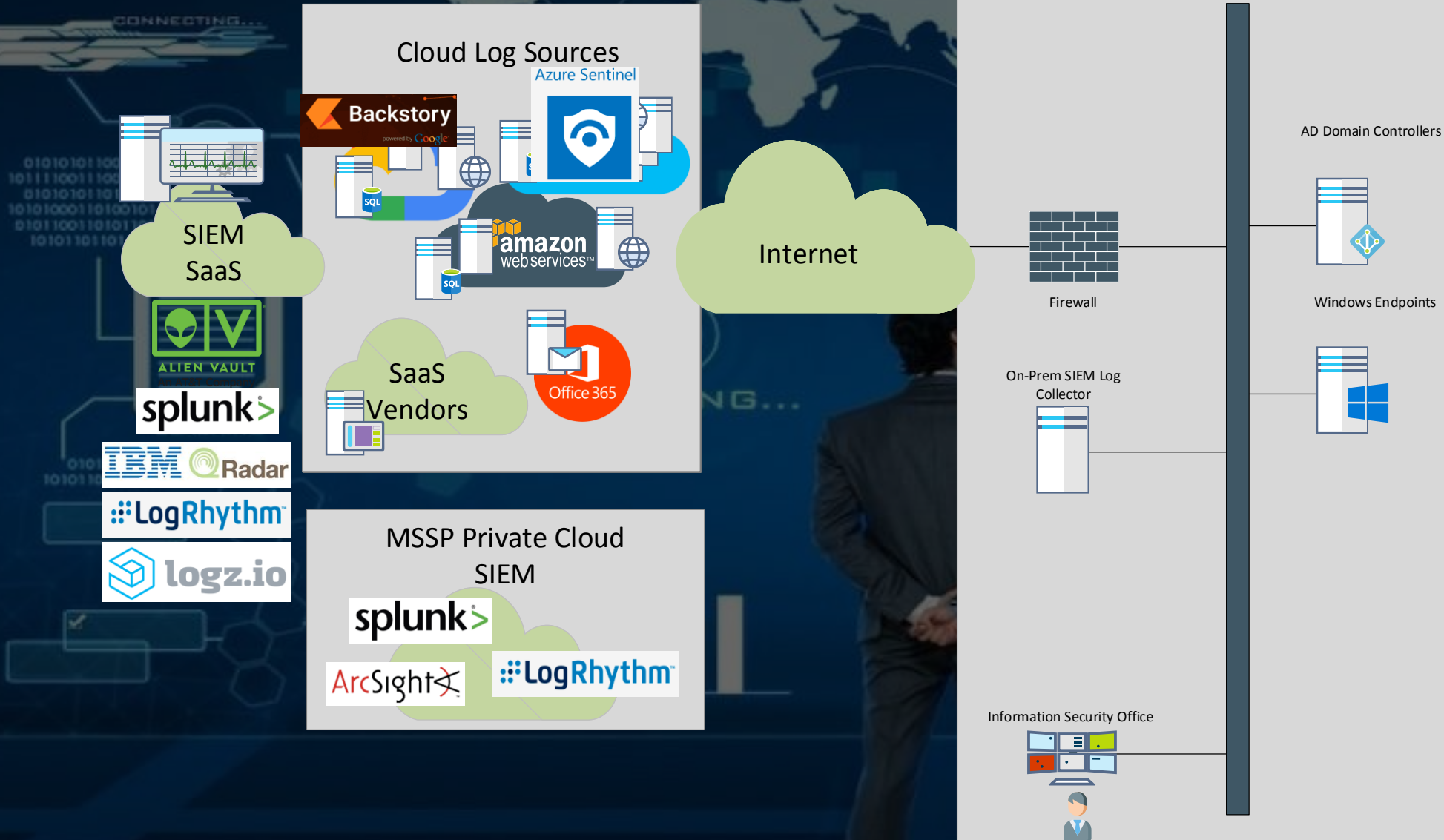
Lack of proper fine tuning of alerts and alarms in order to reduce the noise and generate actionable intelligence.

Skills

Lack of experienced staff available to manage the SIEM solution.

According to [Research and Markets](#), SIEMs and related technologies were a \$5.3 billion market in 2018, and the market is expected to growth at a compound annual growth rate of 19.7 percent – to \$12.9 billion by 2023. SIEMs are the fastest-growing segment of the market.

SIEM moves to the cloud



SIEMs from major cloud providers



Azure Sentinel



Microsoft Cloud SIEM



AWS Security Hub



www.managedsentinel.com

Demos

Splunk (On-prem): <http://192.168.5.25:8000>

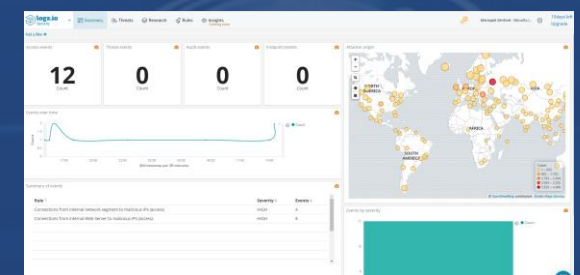
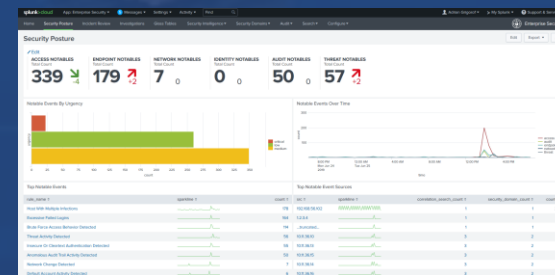
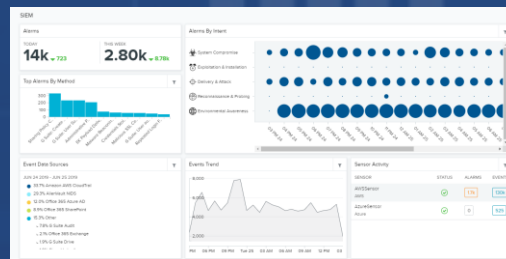
Splunk ES (Cloud): https://prd-p-ngvhg5fjf82c.cloud.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/ess_home

Alienvault (Cloud): <https://www.alienvault-demo-usm-anywhere.com/#/dashboard/>

Logz.io (Elastic Stack on Cloud): <https://app.logz.io>

IBM QRadar: <https://qradar-trial-11469.qradar.ibmcloud.com/console/core/jsp/Main.jsp>

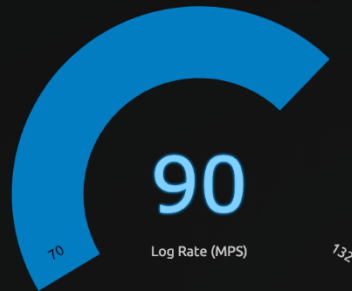
Azure Sentinel (Cloud): <https://portal.azure.com>



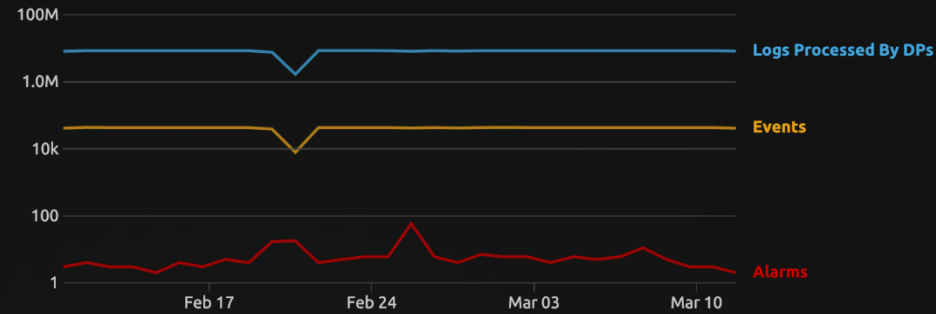
Presentation available at:

<https://www.managedsentinel.com/2019/06/26/siem-traditional-vs-cloud/>

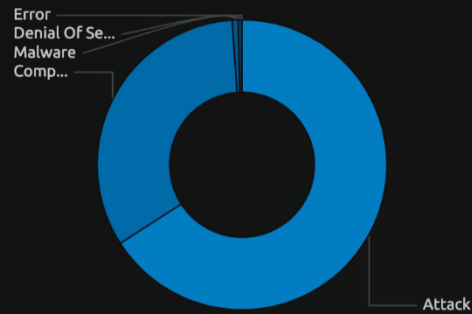
Log Processing Rate



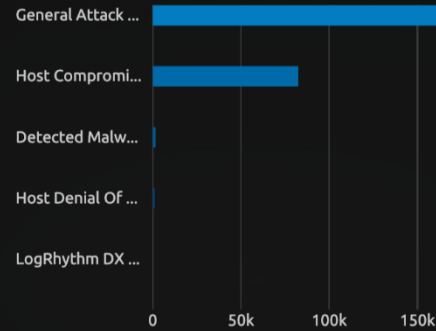
Log, Event, and Alarm Trend Last 30 Days



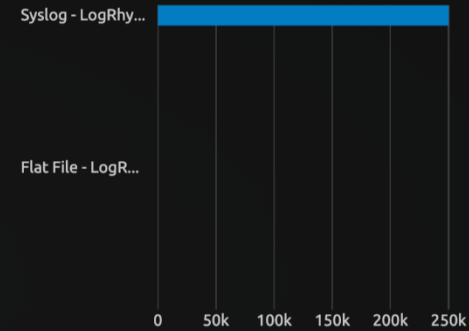
Top Classification Last 5d 18h



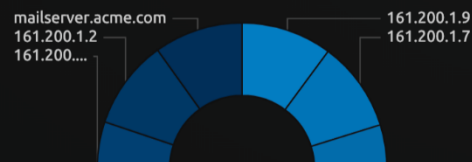
Top Common Event Last 5d 18h



Top Log Source Type Last 5d 18h



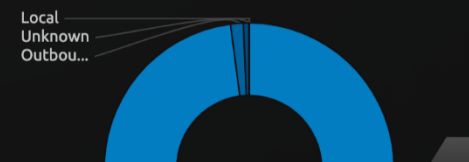
Top Host (Impacted) Last 5d 18h



Top Application Last 5d 18h



Top Direction Last 5d 18h



ArcSight ESM

ASWorkBench

ArcSight Console 6.9.1.2195.0 [vm-esm691c-demo:admin.ast] Trial license. Customer: ARST-SE, Expiration date: 2017/02/01

File Edit View Window Tools System Help

Navigator

Resources Packages Use Cases

Filters

Showing: All Filters

admin's Filters

- Hotlist
- New Filter

Shared

All Filters

- ArcNet Filters
 - ACL
 - Custom
 - DMA Analytics
 - Identity Corre
 - IdentityView v
 - Management
 - NetFlow
 - Scenario Spec
 - Security Intelli
 - Viewers and D
- ArcSight Administr
- ArcSight Core Sec
- ArcSight Foundati
- ArcSight Interacti
- ArcSight Solutions
- ArcSight System
- Deprecated
- Downloads
- JumpStart
- Personal
- Public

Viewer

Connector Overview ESM Overview Demo Live

Database Performance Statistics Event Throughput ESM System Information System Events Last Hour

Connector Status Connector Connection and Cache Status Database Performance Statistics ArcSight User Status

Active Channel: Demo Live Total Events: 465

Start Time: 6 Dec 2016 13:16:00 PST Very High: 27

End Time: 6 Dec 2016 14:17:00 PST High: 83

Filter: (MatchesFilter ("Non-ArcSight Internal Events") And Generator URI NOT Contains "Stan... Medium: 204

Inline Filter: No Filter Low: 103 Very Low: 48

Radar

End Time	Name	Attacker User Name	Target User Name	Attacker Address
6 Dec 2016 14:14:27 PST	FTP_User			10.0.111.22
6 Dec 2016 14:14:25 PST	FTP_Pass			10.0.111.22
6 Dec 2016 14:14:24 PST	accept			199.248.65.119
6 Dec 2016 14:14:23 PST	Encrypted Data Transfer			10.0.111.27
6 Dec 2016 14:14:22 PST	FTP_Pass			10.0.111.22
6 Dec 2016 14:14:20 PST	Encrypted Data Transfer			10.0.111.27
6 Dec 2016 14:14:19 PST	Encrypted Data Transfer			10.0.111.27
6 Dec 2016 14:14:18 PST	Encrypted Data Transfer			10.0.111.27
6 Dec 2016 14:14:17 PST	Encrypted Data Transfer			10.0.111.27
6 Dec 2016 14:14:16 PST	Encrypted Data Transfer			10.0.111.27
6 Dec 2016 14:14:14 PST	Encrypted Data Transfer			10.0.111.27
6 Dec 2016 14:14:13 PST	Too Many TCP SYNS			
6 Dec 2016 14:14:12 PST	Encrypted Data Transfer			10.0.111.27
6 Dec 2016 14:14:11 PST	accept			192.168.111.1
6 Dec 2016 14:14:10 PST	Too Many TCP SYNS			

Grid

Inspect/Edit

Filter: New Filter

Event Inspector Active Channel: Demo Live

Attributes Filter Sort Fields Local Variables Notes

Filters Assets Vulnerabil

Edit Summary

Event conditions

event1

AND

MatchesFilter("/All Filters/ArcSight System/

Generator URI NOT Contains Standard Ru

Event Annotation Flags NOT Contains Bits

on Conditions Editor +/- Global Variable...

Name	Op	Con
Event		
Aggregated Event Co...		
Application Protocol		
Bytes In		
Bytes Out		
Correlated Event Count		
Customer		
Domain		
Domain External ID		
Domain ID		
Domain Name		

Search for:

OK Cancel Apply Help

6) [2:16:24] Filter "New Filter" added successfully.

IBM QRadar Security Intelligence

admin ▾ Help ▾ Messages 11 ▾ IBM

DashboardOffensesLog ActivityNetwork ActivityAssetsReportsRisksVulnerabilitiesAdminDeploymentUser Analytics

Quick Insights

Search for User

Q

Next Refresh: 00:45 ↻

Monitored Users

3.6k

Current High Risk Users

3.5k

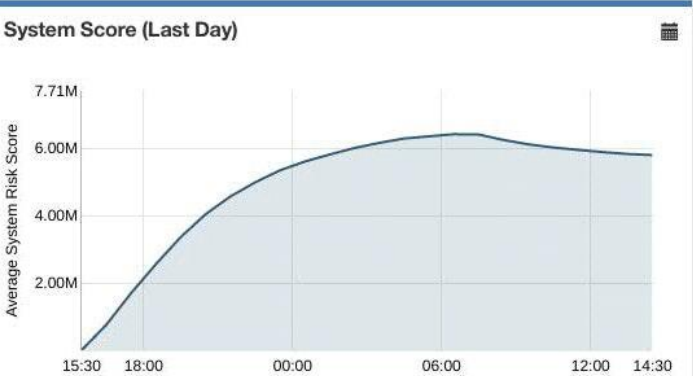
Sense Events (Last Hour)

778.9k

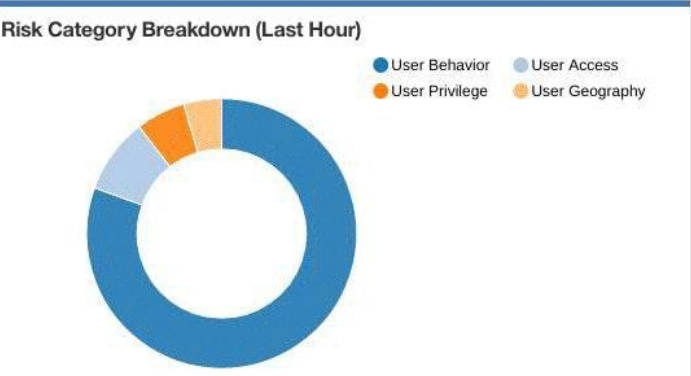
Offenses Generated (Last Hour)

606

System Score (Last Day)



Risk Category Breakdown (Last Hour)



Recent Offenses

Offense # 7638
User: **dacuss**
Event Count: 270 Flow Count: 0 Magnitude: 5/10

Offense # 7637
User: **liq1-2394**
Event Count: 201 Flow Count: 0 Magnitude: 6/10

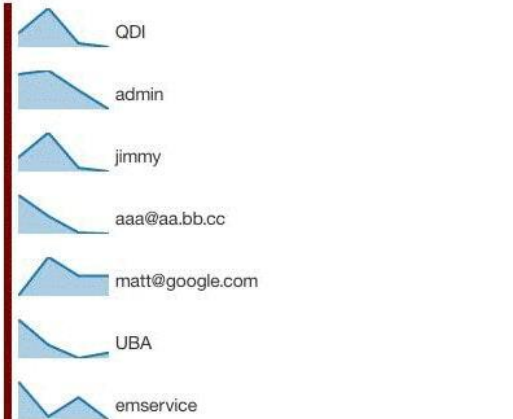
Offense # 7636
User: **seafood1-0151**
Event Count: 201 Flow Count: 0 Magnitude: 6/10

Offense # 7635
User: **benitsp**
Event Count: 185 Flow Count: 0 Magnitude: 5/10

Offense # 7634
User: **price1-5747**
Event Count: 254 Flow Count: 0 Magnitude: 6/10

Users with the highest risk score

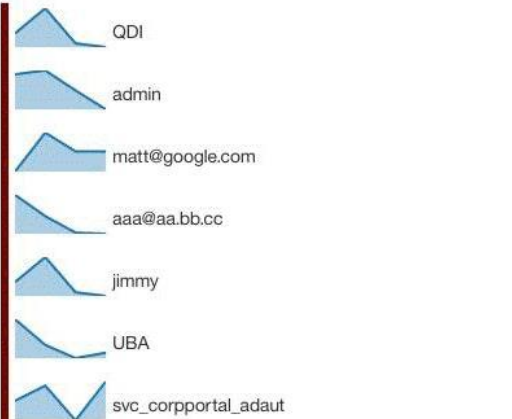
View all >



QDI	362344	👁
admin	64146	👁
jimmy	54980	👁
aaa@aa.bb.cc	54941	👁
matt@google.com	54888	👁
UBA	23807	👁
emservice	18380	👁

Users with the most recent risk activity

View all >



QDI	+19620	👁
admin	+3060	👁
matt@google.com	+2980	👁
aaa@aa.bb.cc	+2980	👁
jimmy	+2980	👁
UBA	+1330	👁
svc_corportal_adaut	+1070	👁

Watchlist

QDI	362.3k	↘	⊖
jimmy	55k	↘	⊖
matt@google.com	54.9k	↘	⊖

SAGEFOX

SIEM

Alarms

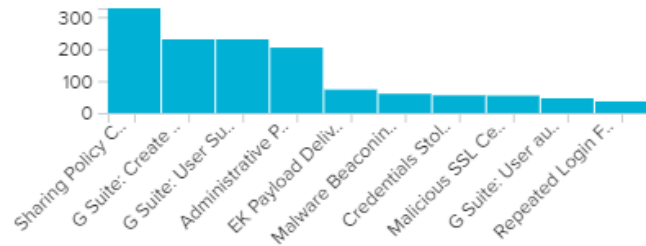
TODAY

14k ▼ 723

THIS WEEK

2.80k ▼ 8.78k

Top Alarms By Method



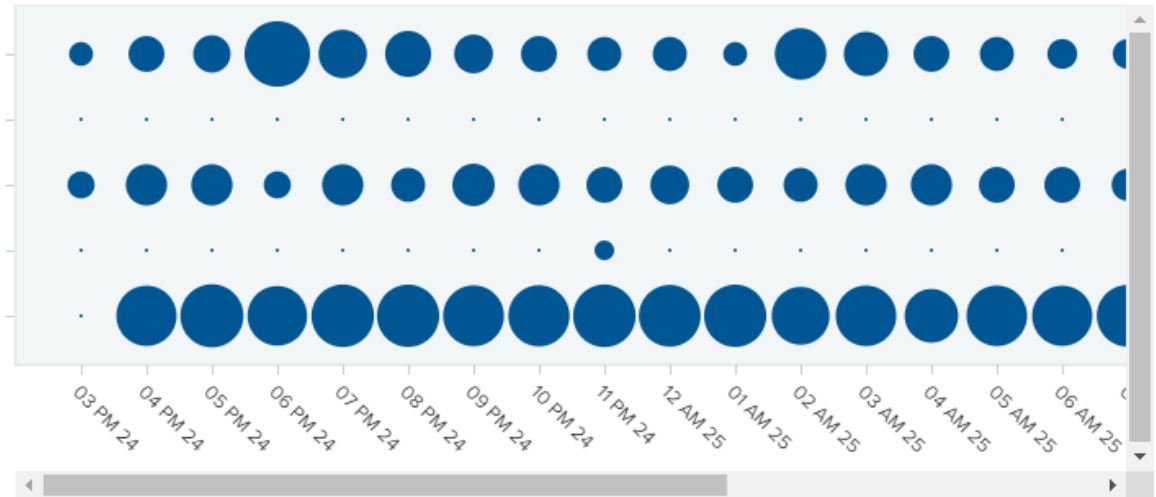
Event Data Sources

JUN 24 2019 - JUN 25 2019

- 33.7% Amazon AWS CloudTrail
- 29.3% AlienVault NIDS
- 12.0% Office 365 Azure AD
- 8.9% Office 365 SharePoint
- 15.3% Other
 - └ 7.8% G Suite Audit
 - └ 2.1% Office 365 Exchange
 - └ 1.9% G Suite Drive

Alarms By Intent

- System Compromise
- Exploitation & Installation
- Delivery & Attack
- Reconnaissance & Probing
- Environmental Awareness



Events Trend



Sensor Activity

SENSOR	STATUS	ALARMS	EVENTS
AWSSensor AWS	✓	1.7k	130k
AzureSensor Azure	✓	0	525

splunk>cloudApp: Enterprise Security▼5 Messages▼Settings▼Activity▼Find

Adrian Grigorof> My SplunkSupport & Services

HomeSecurity PostureIncident ReviewInvestigationsGlass TablesSecurity Intelligence▼Security Domains▼Audit▼Search▼Configure▼

Enterprise Security

Security Posture

EditExport...

Edit

ACCESS NOTABLESTotal Count339-4

ENDPOINT NOTABLESTotal Count179+2

NETWORK NOTABLESTotal Count70

IDENTITY NOTABLESTotal Count00

AUDIT NOTABLESTotal Count500

THREAT NOTABLESTotal Count57+2

Notable Events By Urgency

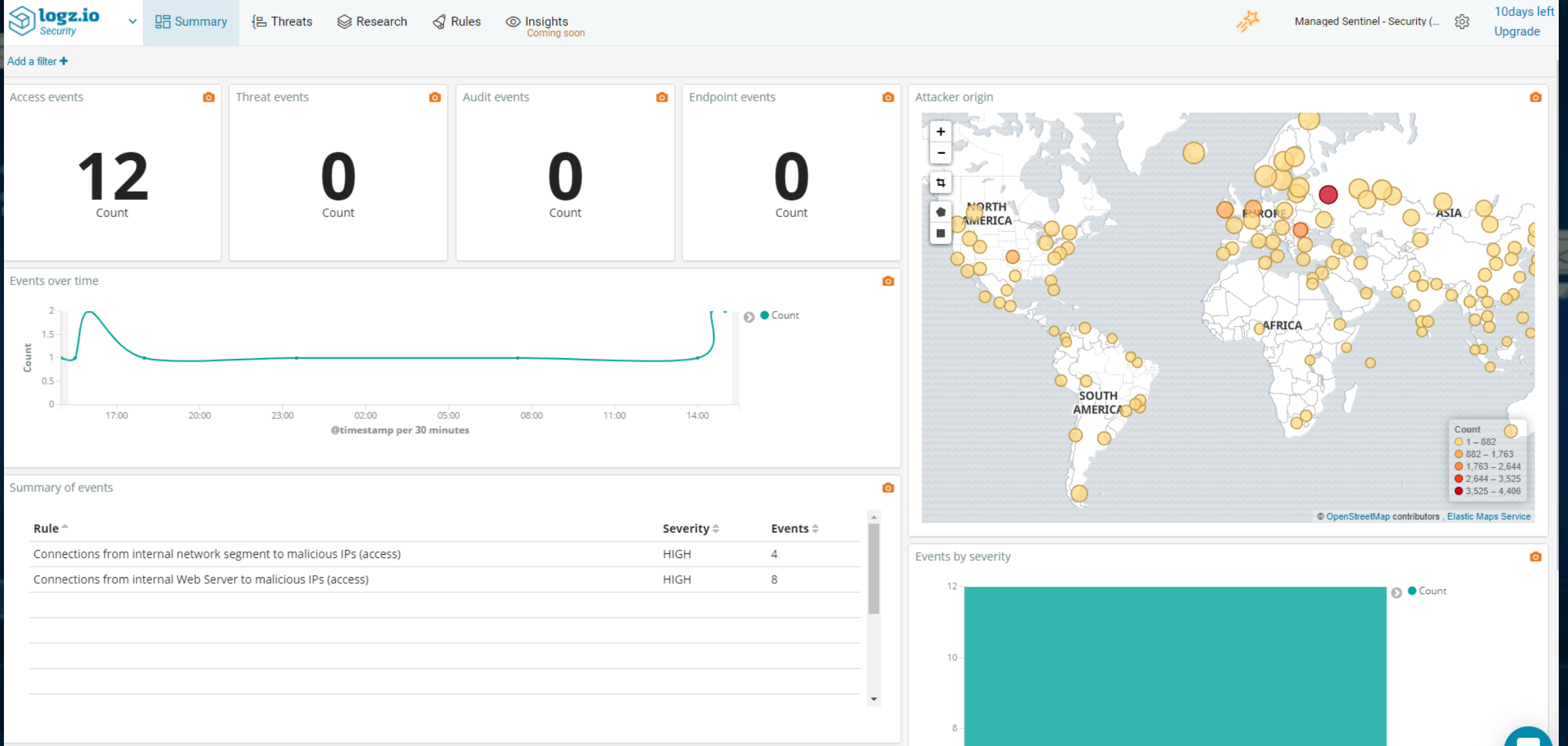
Notable Events Over Time

Top Notable Events

rule_name	sparkline	count
Host With Multiple Infections		178
Excessive Failed Logins		164
Brute Force Access Behavior Detected		114
Threat Activity Detected		56
Insecure Or Cleartext Authentication Detected		55
Anomalous Audit Trail Activity Detected		50
Network Change Detected		7
Default Account Activity Detected		6

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
192.168.56.102		1	1	23
1.2.3.4		1	1	8
...truncated...		1	1	7
10.11.36.10		3	2	6
10.11.36.13		3	2	6
10.11.36.15		3	2	6
10.11.36.14		3	2	5
10.11.36.16		3	2	5



Azure Sentinel

Azure Sentinel - Overview

Selected workspace: "Managed-Sentinel" - PREVIEW

Search (Ctrl+/)

Refresh Last 24 hours

General

Overview

Logs

Threat management

Cases

Dashboards

Hunting

Notebooks

Configuration

Getting started

Data connectors

Analytics

Playbooks

Community

Workspace settings

1.6M 41.2K
Events

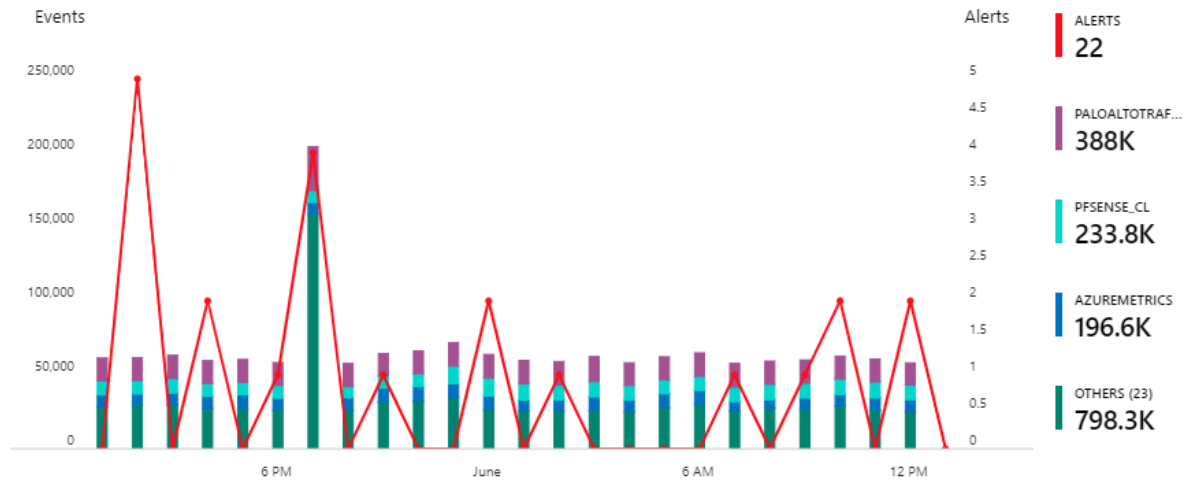
22 1
Alerts

22 1
Cases

CASES BY STATUS

NEW (22) IN PROGRESS (0) CLOSED (RESOLVED) (0) CLOSED (DISMISSED) (0)

Events and alerts over time



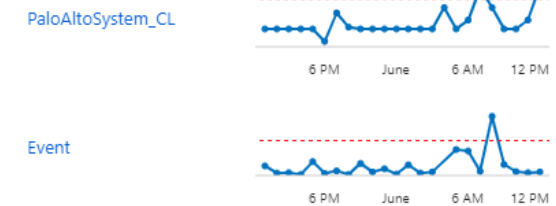
Potential malicious events



Recent cases

- MS-A005-1: Authentication failure detected - Pa... 1 Alerts
- MS-A085: Rare User Agent strings W3CIISLog 1 Alerts
- MS-A004: Anomalous sign-in location by user/a... 1 Alerts
- MS-A003: Anomalous sign-in location by user a... 1 Alerts
- MS-A119: Windows Audit Log Cleared 1 Alerts

Data source anomalies



Democratize ML for your SecOps