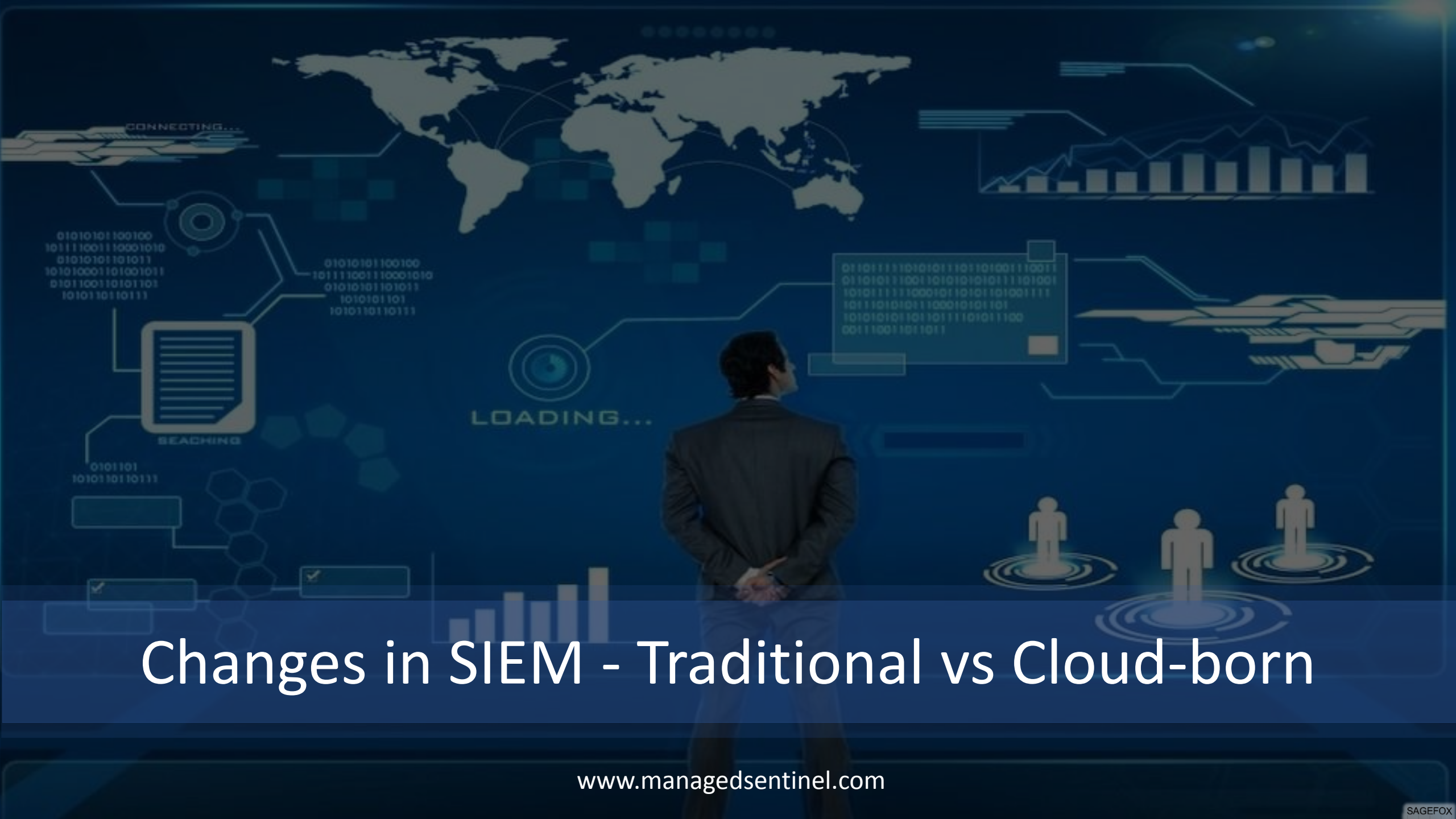


Changes in SIEM - Traditional vs Cloud-born

www.managedsentinel.com

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

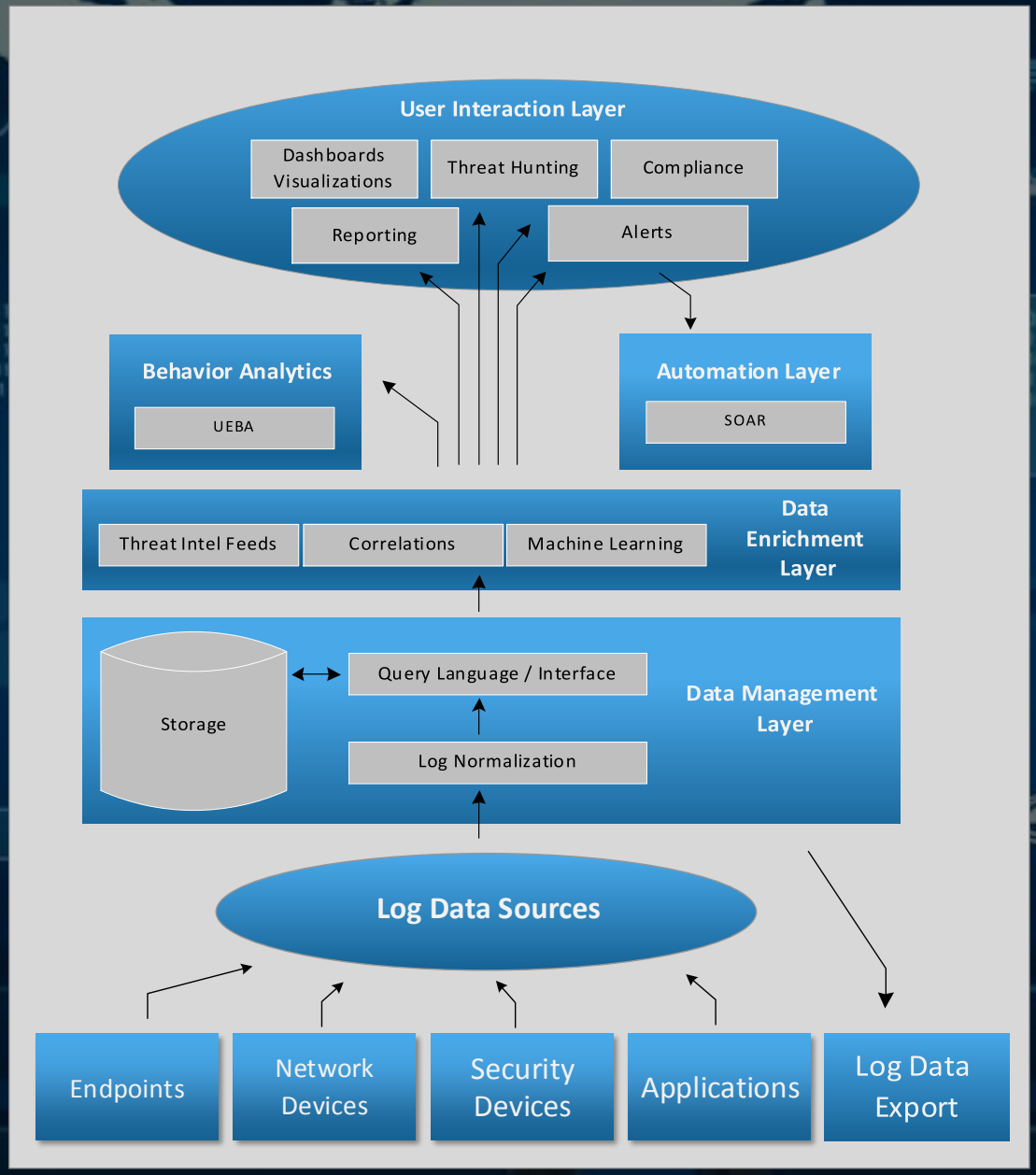
Mid 2010s

- Big data
- Machine Learning
- Threat Hunting

Present

- Cloud Migrations
- Threat Intelligence / SOAR
- Behavior Analysis

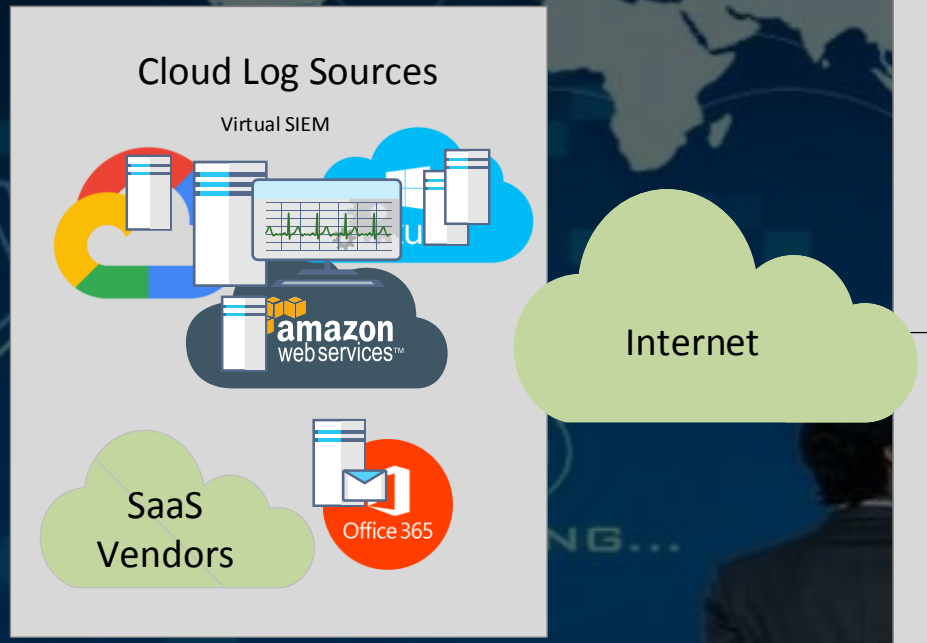
SIEM Architecture



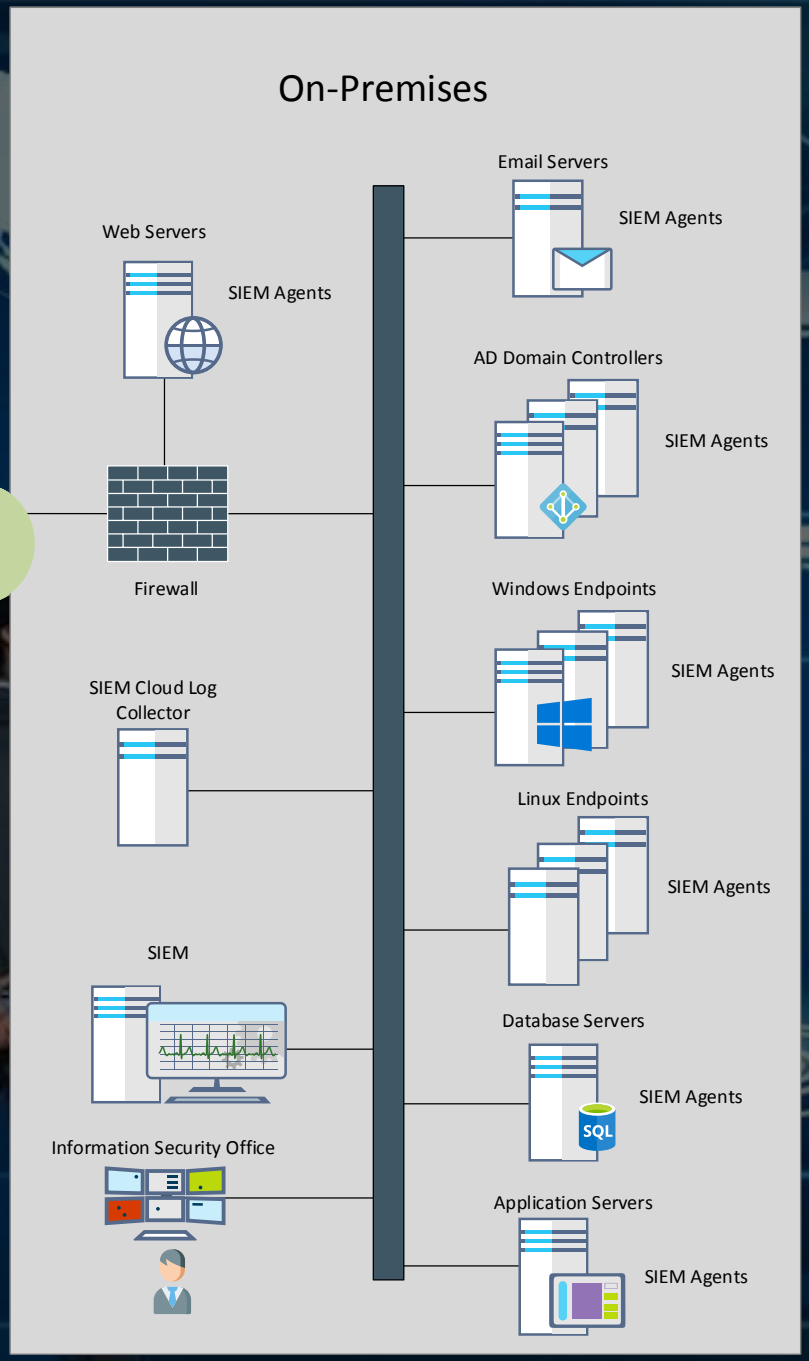
SIEM Vendors

Source: Gartner (December 2018)

Traditional SIEM Deployment



Internet



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

Use-cases

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

Data volume

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

Skills

Lack of experienced staff available to manage the SIEM solution.

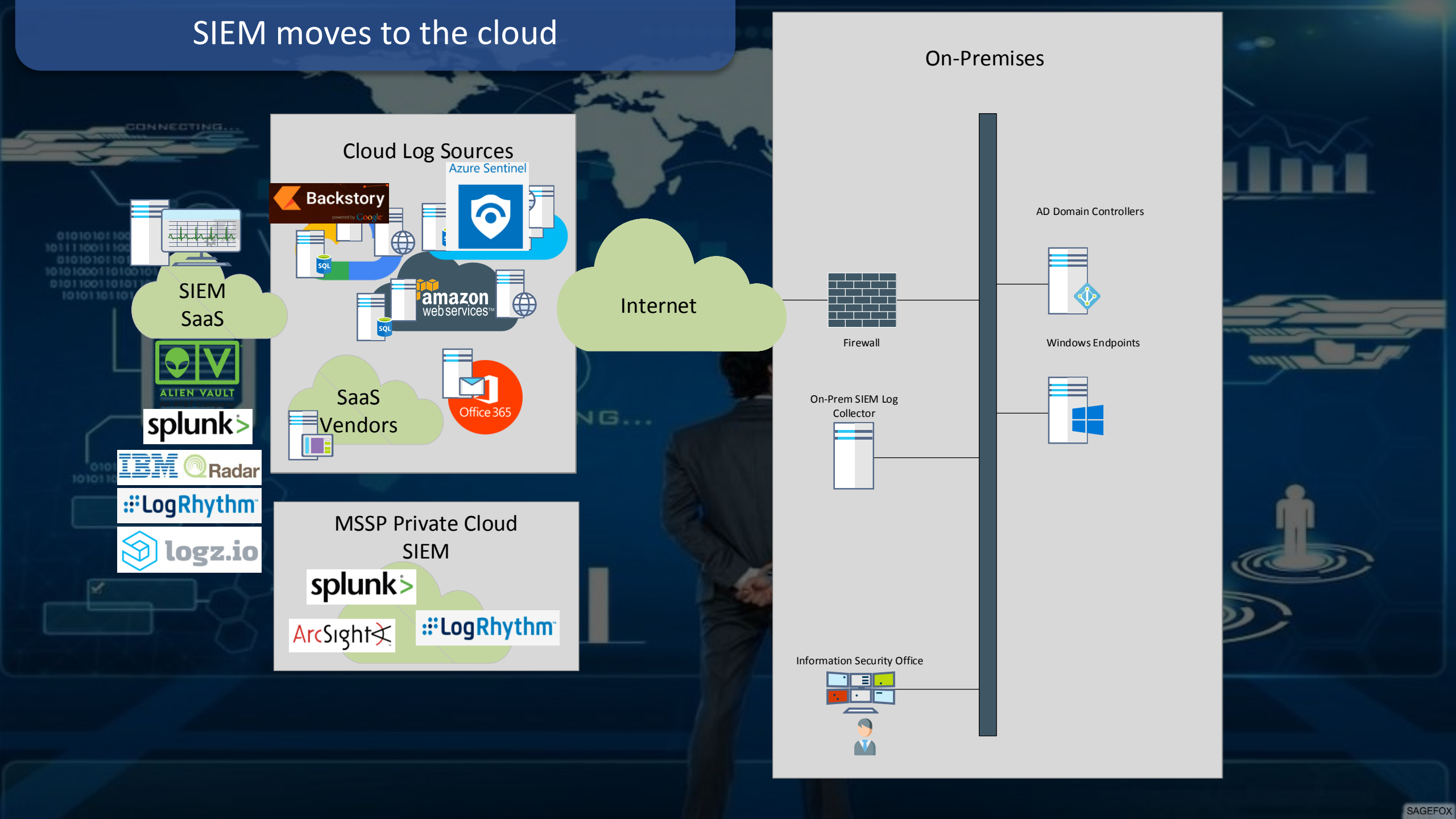
There is no cloud
It's just someone else's computer

Cloud

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

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

Backstory
powered by Google

Azure Sentinel

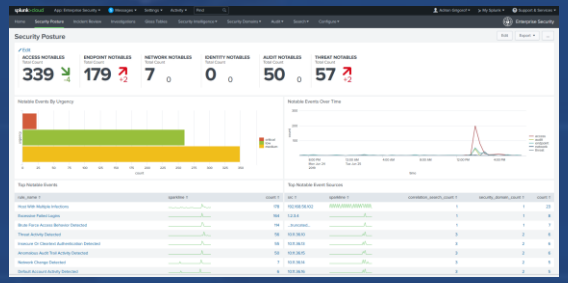
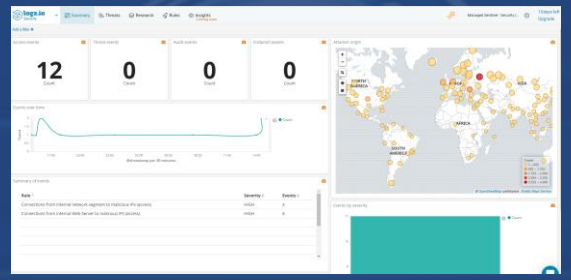
Microsoft Cloud SIEM

AWS Security Hub

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



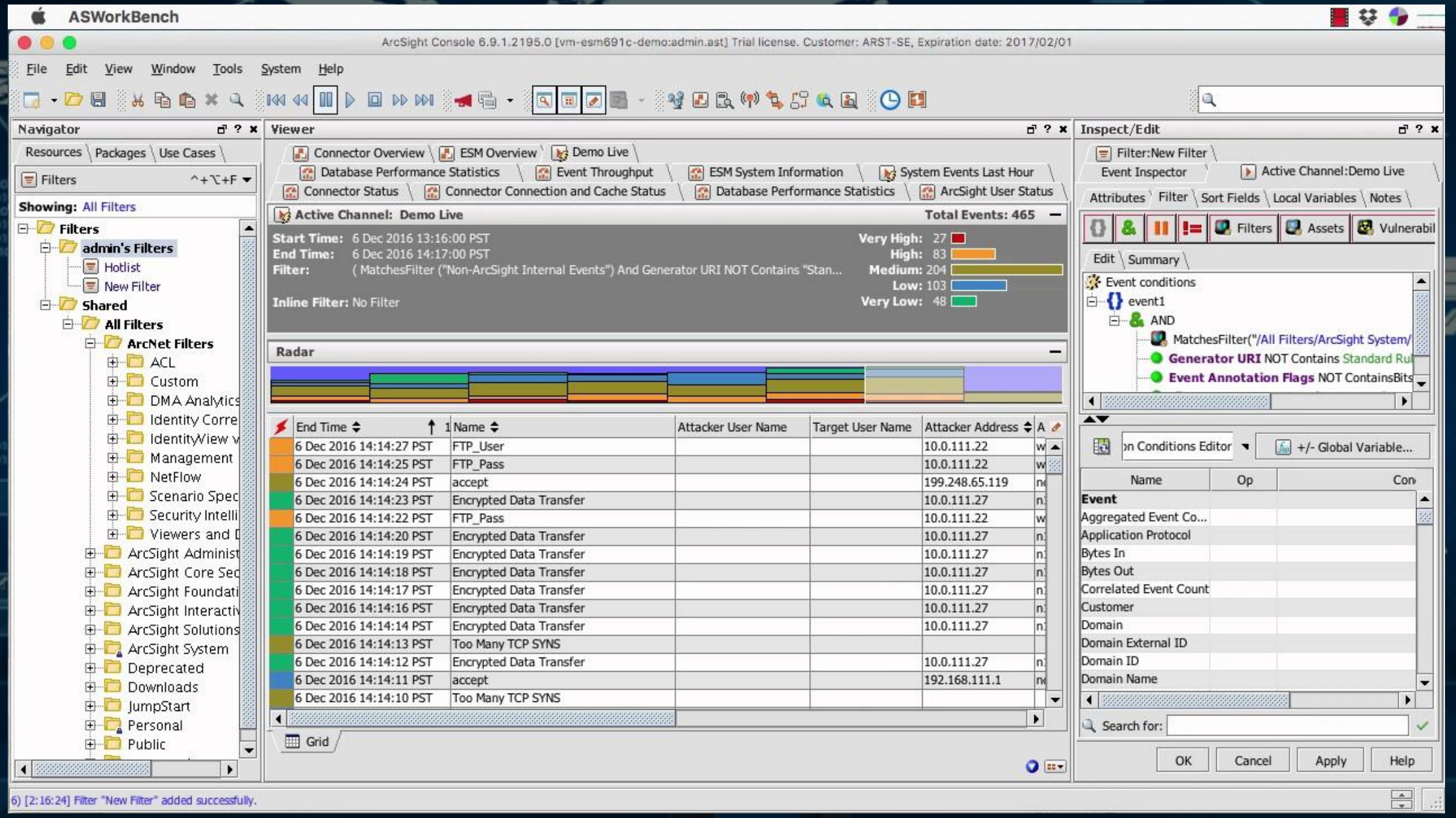
Q & A

Presentation available at:

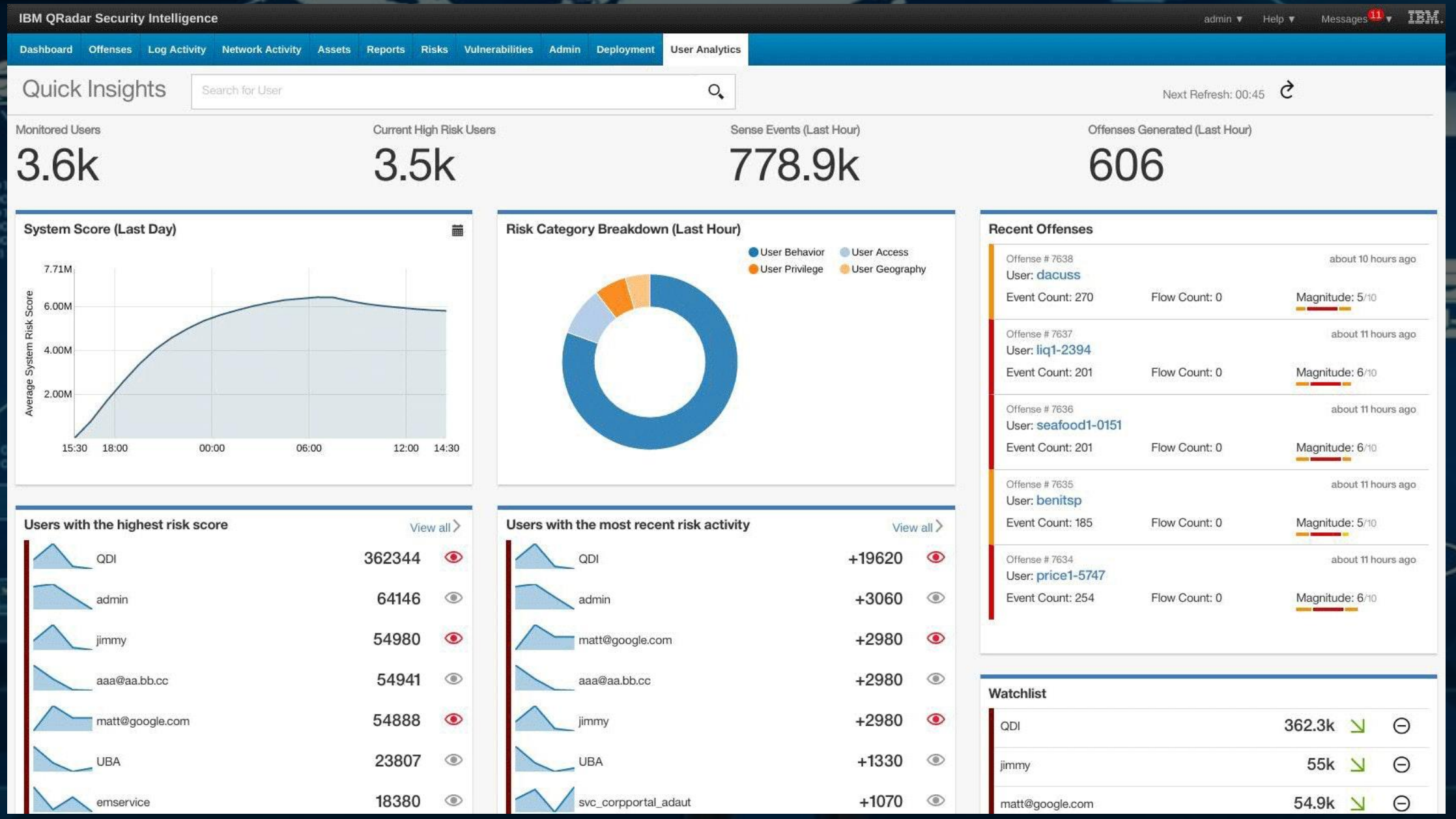
https://www.managedsentinel.com/2019/06/26/**siem-traditional-vs-cloud/**

LogRhythm

ArcSight ESM



IBM QRadar



Alienvault USM

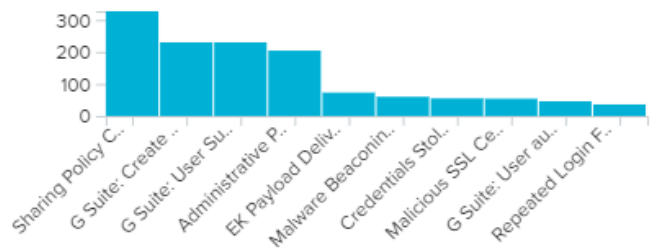
SIEM

Alarms

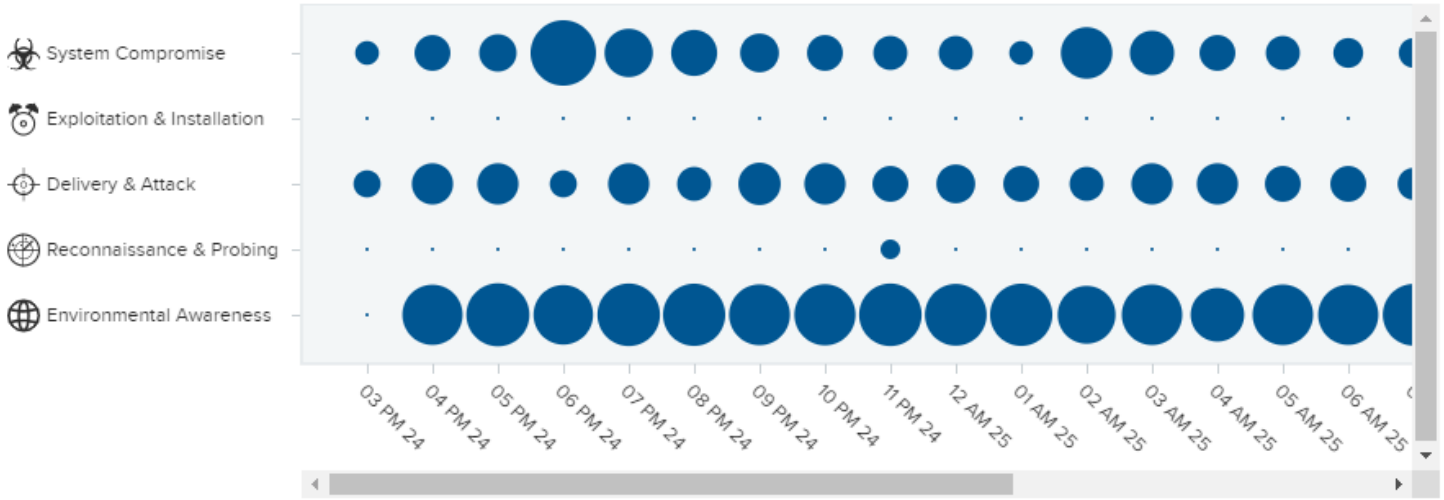
TODAY
14k 723

THIS WEEK
2.80k 8.78k

Top Alarms By Method



Alarms By Intent



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

Events Trend

Sensor Activity

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

Splunk ES

splunk>cloud App: Enterprise Security ▾ 5 Messages ▾ Settings ▾ Activity ▾ Find Adrian Grigorof ▾ > My Splunk ▾ Support & Services ▾

Home | Security Posture | Incident Review | Investigations | Glass Tables | Security Intelligence ▾ | Security Domains ▾ | Audit ▾ | Search ▾ | Configure ▾ | Enterprise Security

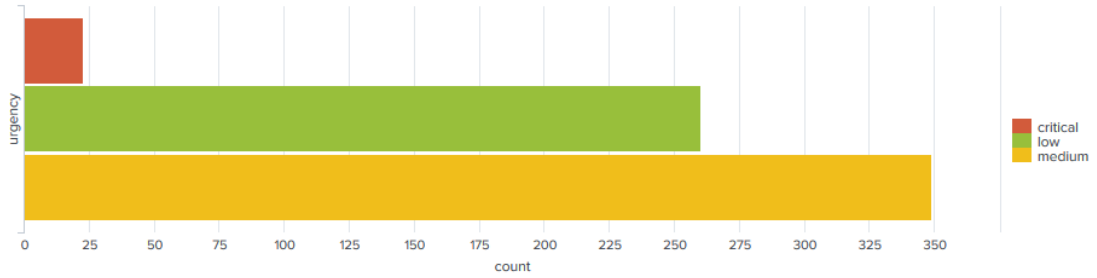
Security Posture

Edit | Export ▾ | ...

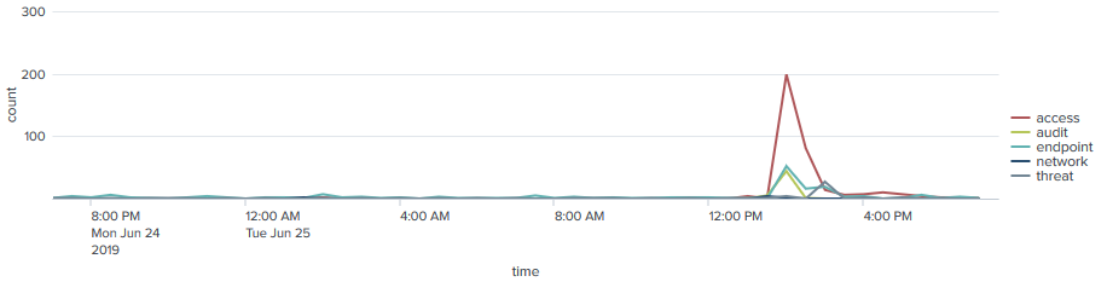
Edit

ACCESS NOTABLES	ENDPOINT NOTABLES	NETWORK NOTABLES	IDENTITY NOTABLES	AUDIT NOTABLES	THREAT NOTABLES
Total Count	Total Count	Total Count	Total Count	Total Count	Total Count
339 ↘ -4	179 ↗ +2	7 0	0 0	50 0	57 ↗ +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

Logz.io

logz.io Security | Summary | Threats | Research | Rules | Insights (Coming soon) | Managed Sentinel - Security (... | 10days left | Upgrade

Add a filter +

Access events

12

Count

Threat events

0

Count

Audit events

0

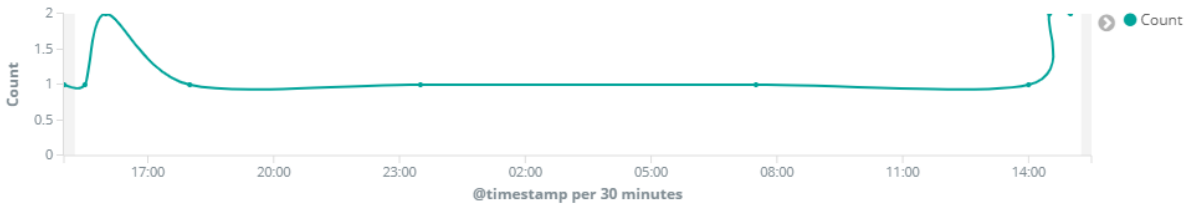
Count

Endpoint events

0

Count

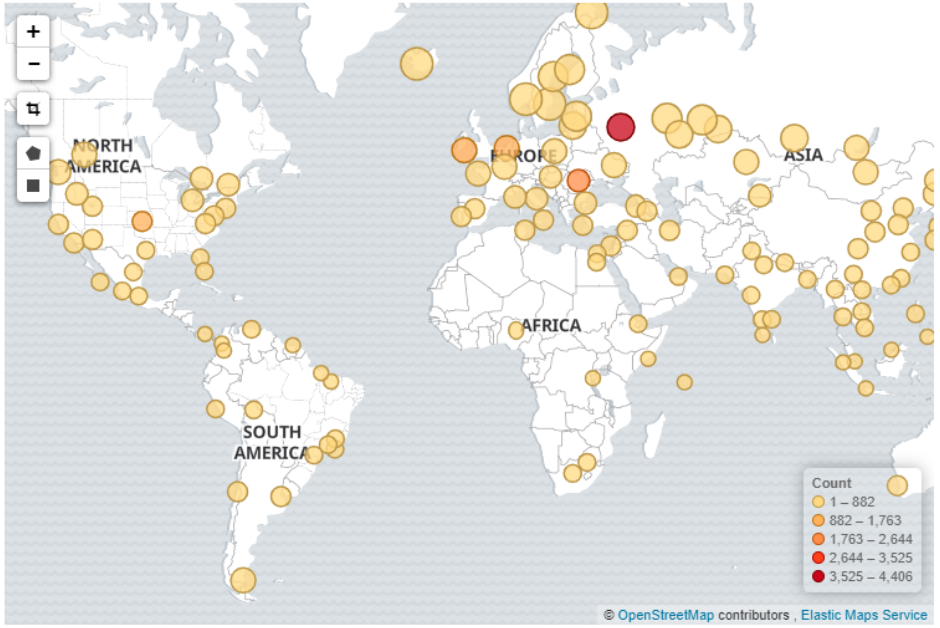
Events over time



Summary of events

Rule	Severity	Events
Connections from internal network segment to malicious IPs (access)	HIGH	4
Connections from internal Web Server to malicious IPs (access)	HIGH	8

Attacker origin



Events by severity

SAGEFOX

Azure Sentinel