QUALYS SECURITY CONFERENCE 2020

Security Data Lake and Analytics Cloud Platform

Dilip Bachwani
Senior Vice President, Engineering and Cloud Operations,
Qualys, Inc.

Cloud Platform Evolution

Growing portfolio with 19+ apps

Cloud Agent driving product adoption

Organically built multi-petabyte data lake

Better cross-product and third-party data correlation…

Qualys.

Data Lake and Security Analytics Goals

Provide a coherent and actionable view of your security posture by breaking down security data silos

Coalesce all data into a centralized highly scalable security data lake

Combine and enrich Qualys generated findings with third party signals

Leverage the strength of Qualys Cloud Platform, Cloud Agent and Apps to build a comprehensive security analytics platform

Qualys.

Security Analytics Use Cases

Real-time streaming correlation and analytics with out-of-box rules

Out-of-band batch analytics over historical data

Ad-hoc querying and threat hunting on enriched and security aware data sets

Advanced analytics use cases using machine learning

Orchestration with playbooks

Response and endpoint protection

Qualys.

Advanced Correlation and Analytics

ML/AI Service
Patterns | Outlier | Predictive SoC

Orchestration & Automation
Integration | Playbooks | Response

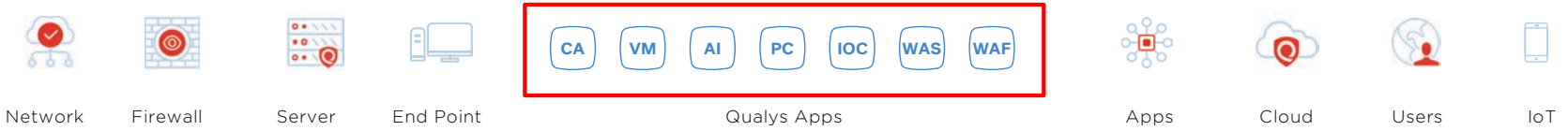
UEBA
User & Entity Behavior Analytics

Threat Hunting
Search | Exploration | Behavior Graph

Security Analytics
Anomaly | Visualization | Dashboard

Advanced Correlation
Actionable Insights | Out-of-box Rules

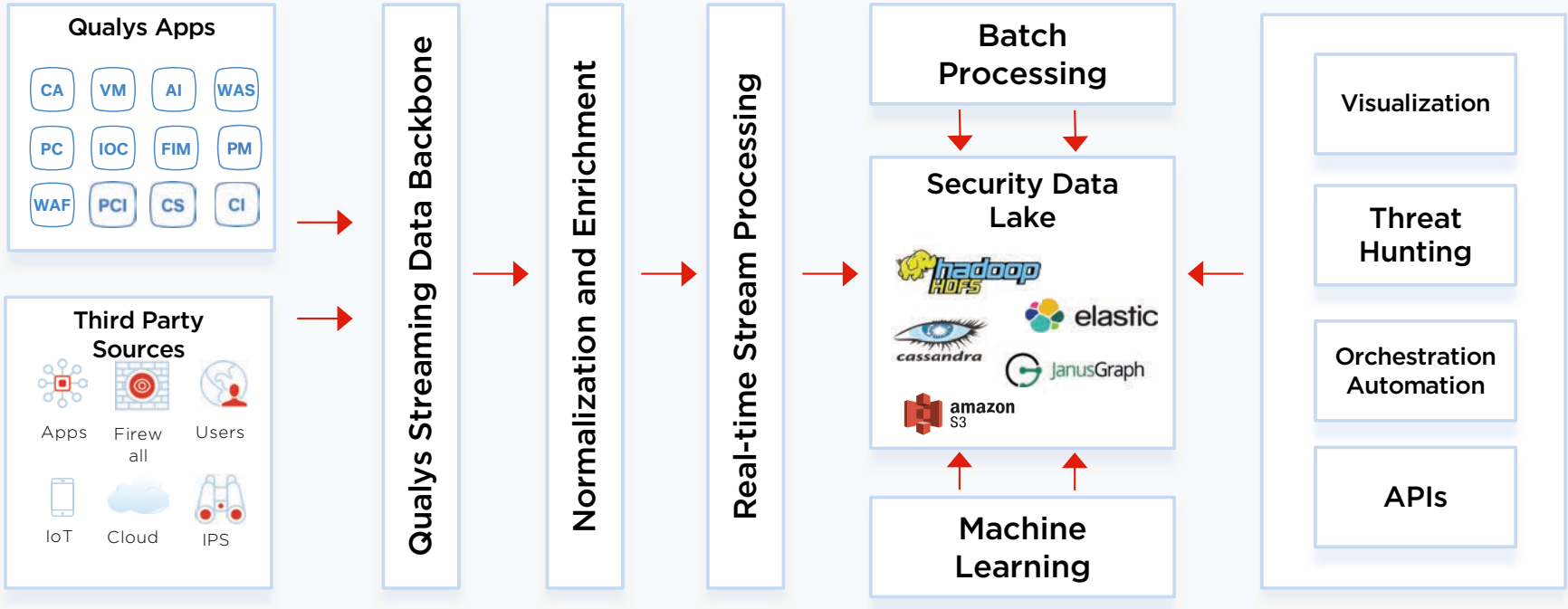
Qualys Security Data Lake Platform
Data Ingestion | Normalization | Enrichment | Governance



Network | Firewall | Server | End Point | Qualys Apps | Apps | Cloud | Users | IoT

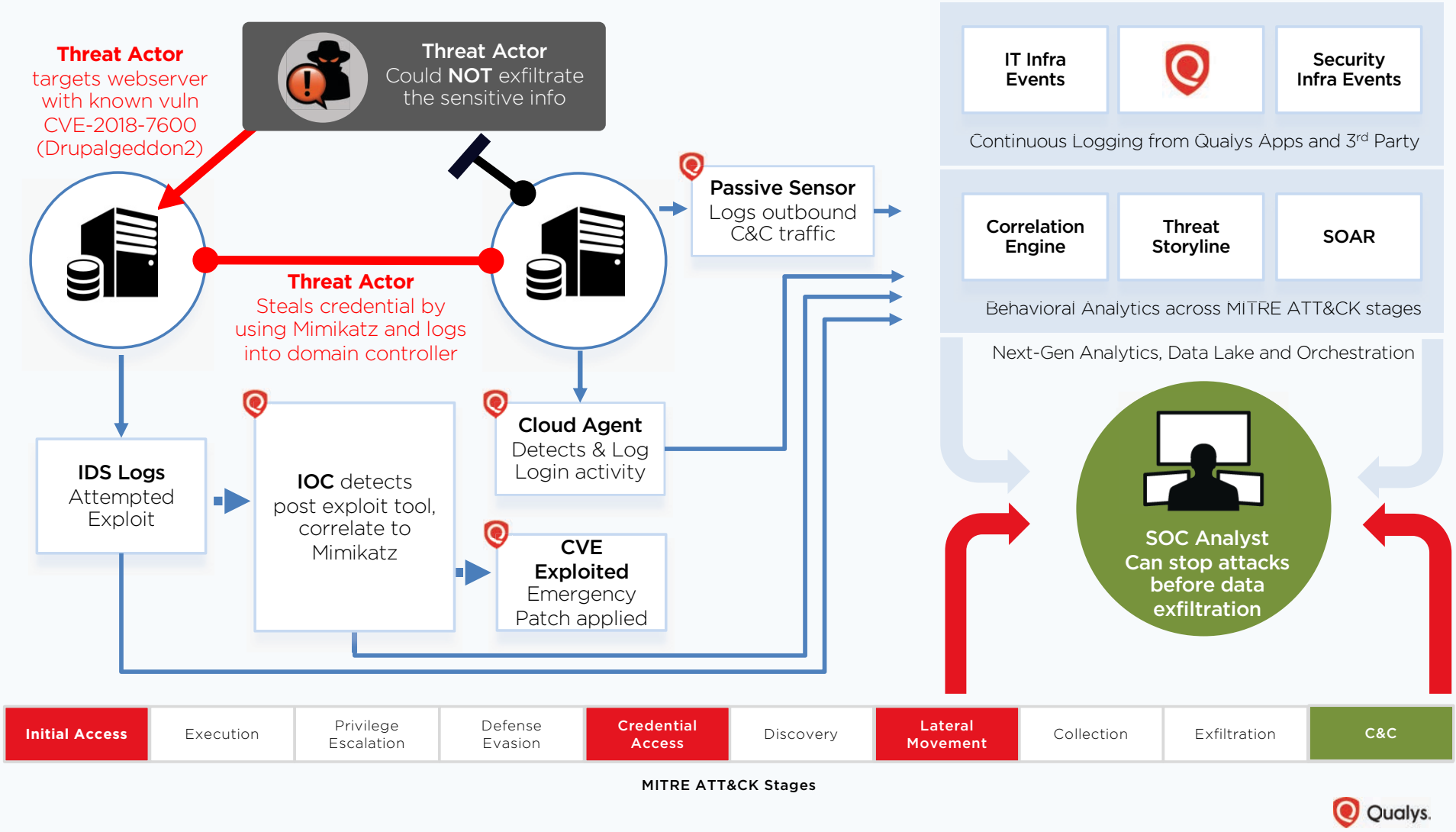
Qualys Quick Connectors

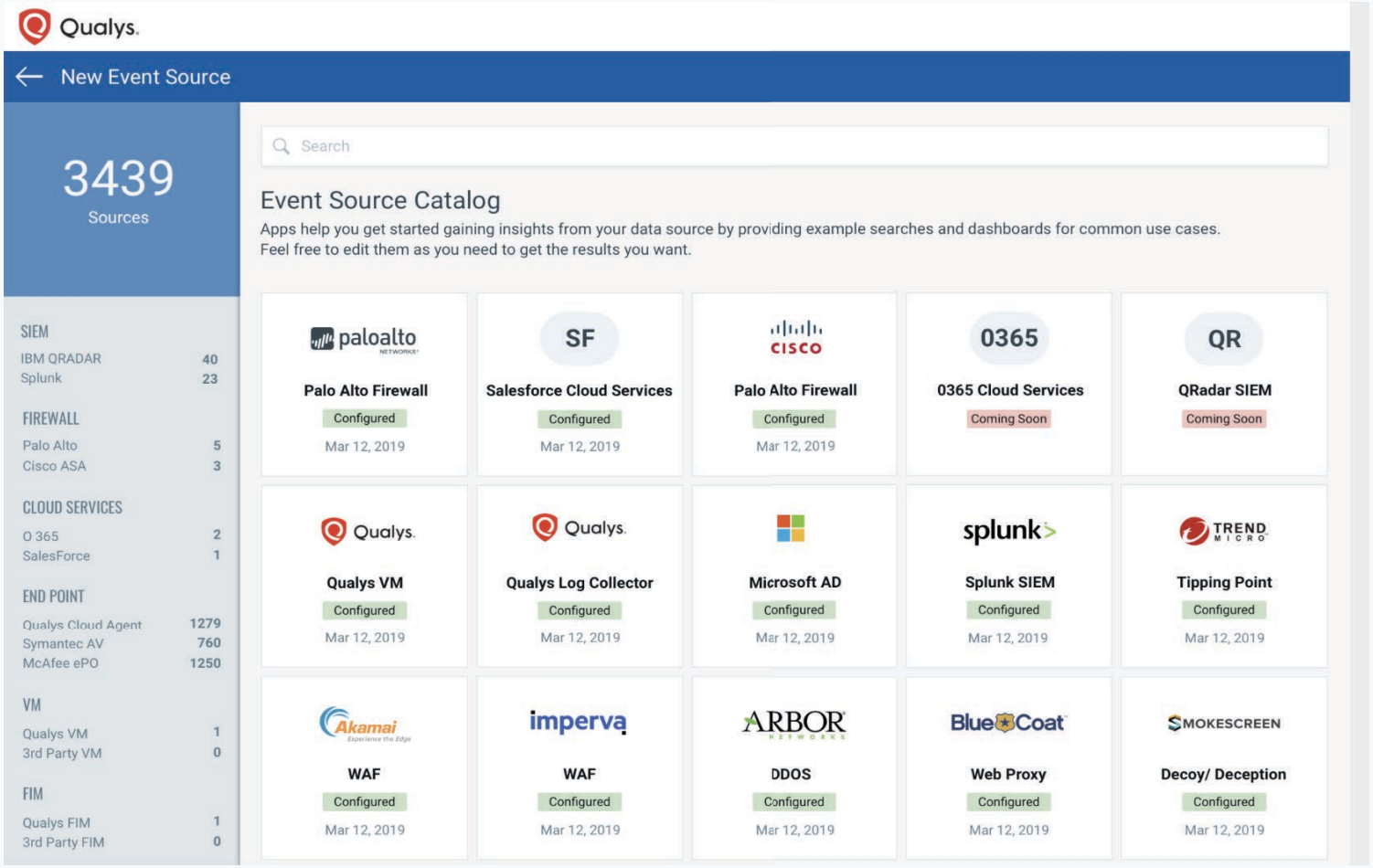
Correlation and Data Platform Architecture

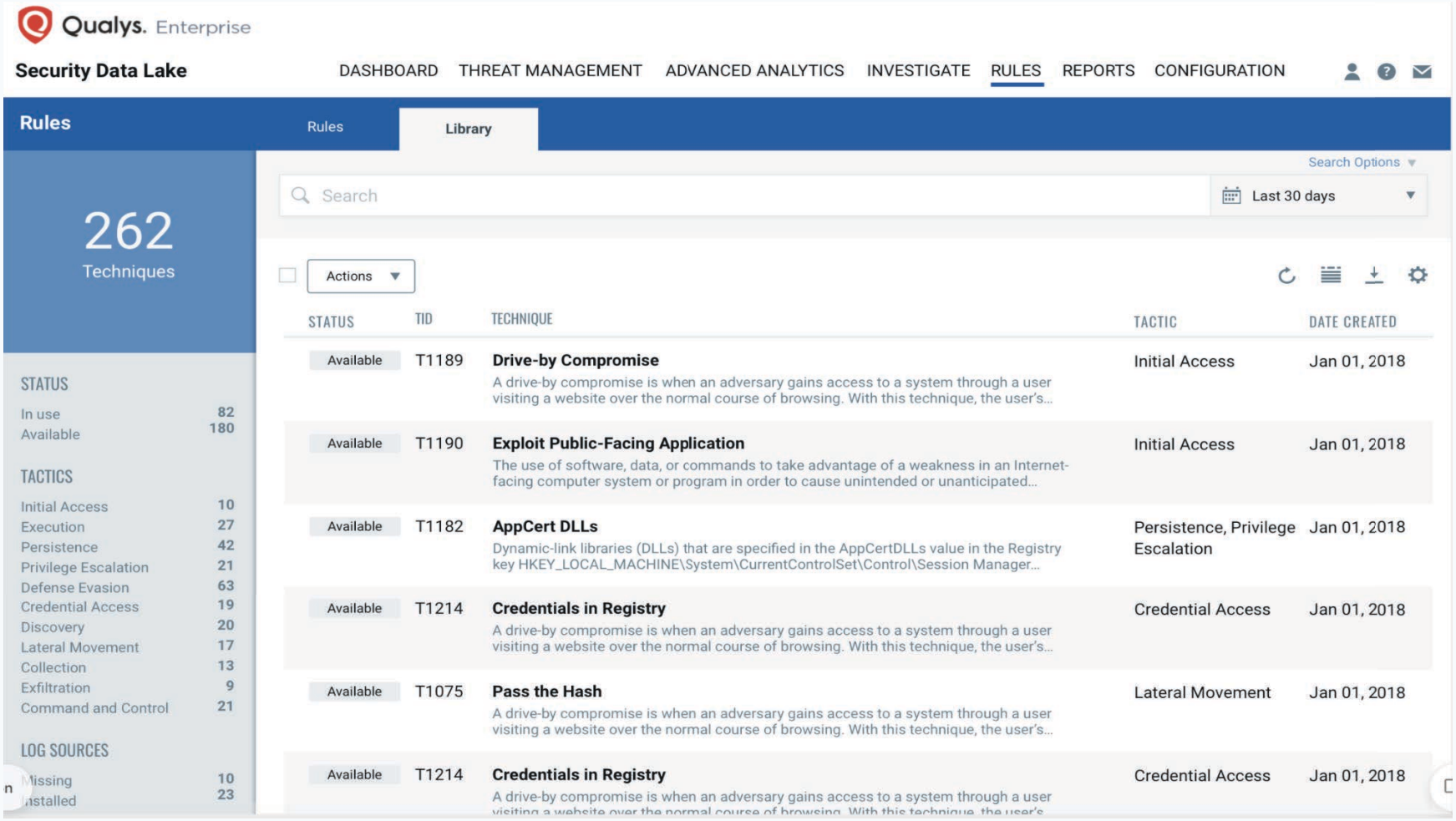


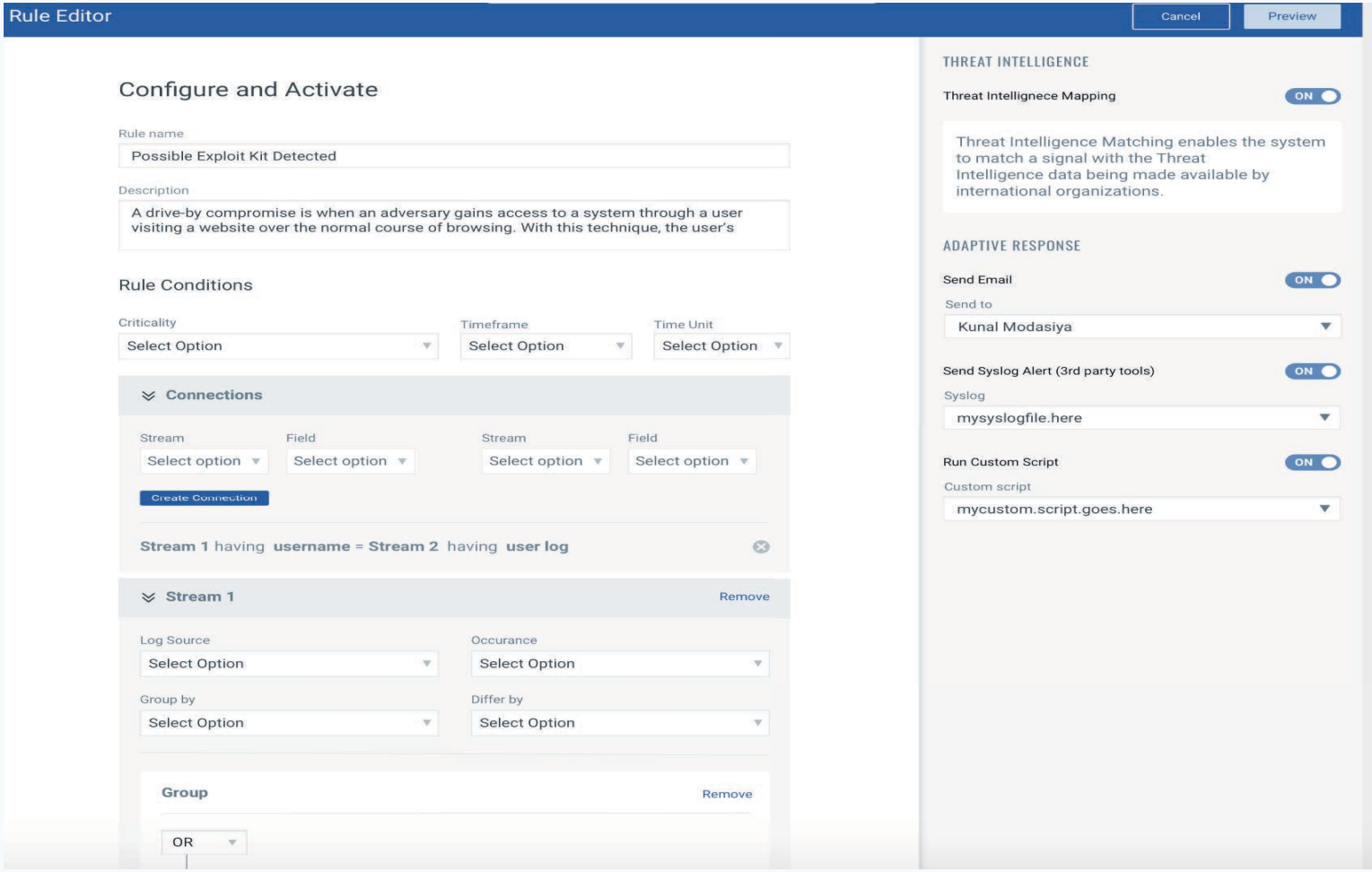
Qualys.

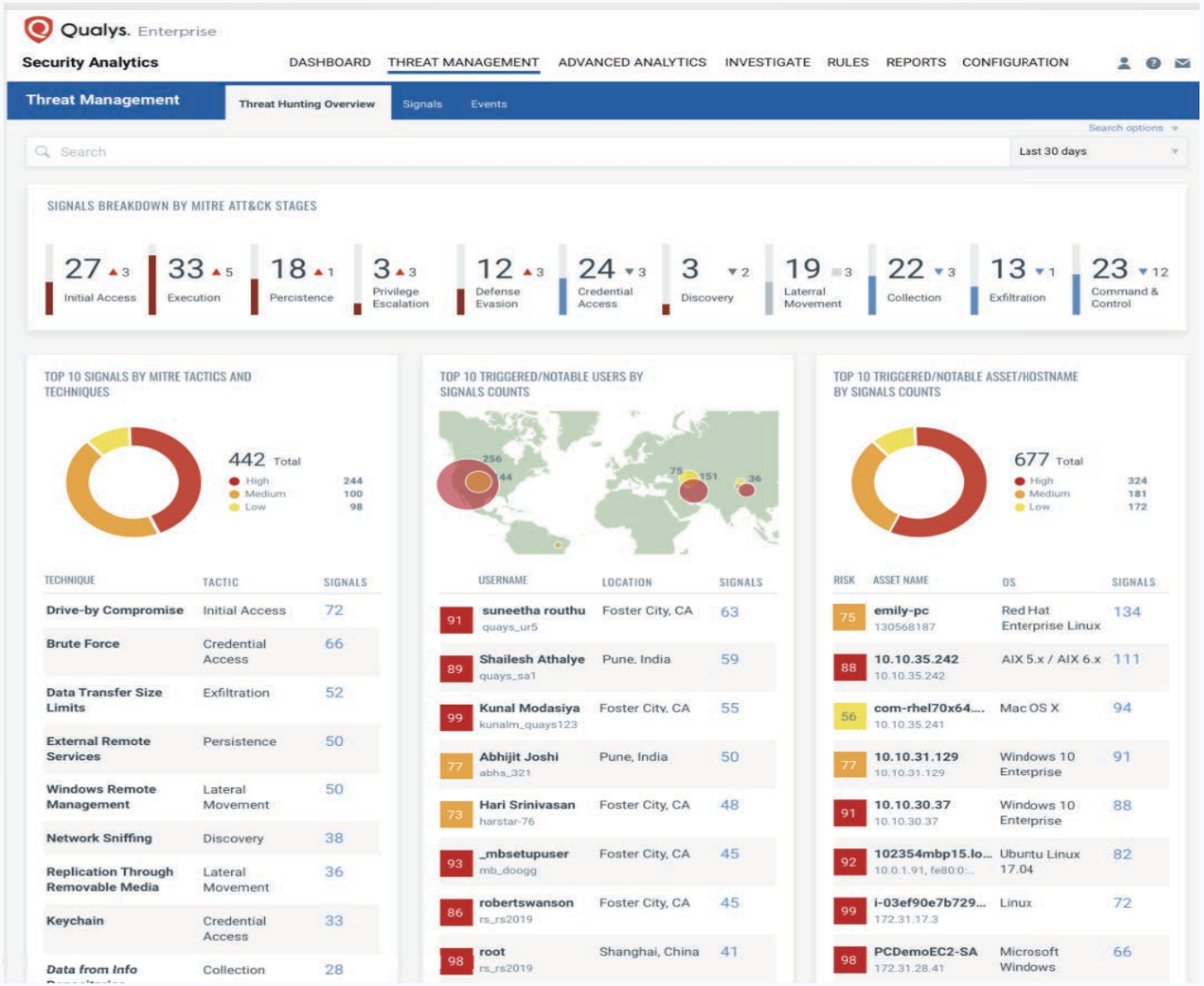
7


Threat Actor
targets webserver with known vuln CVE-2018-7600 (Drupalgeddon2)
Threat Actor
Could NOT exfiltrate the sensitive info
Passive Sensor
Logs outbound C&C traffic
Threat Actor
Steals credential by using Mimikatz and logs into domain controller
IDS Logs
Attempted Exploit
IOC detects post exploit tool, correlate to Mimikatz
Cloud Agent
Detects & Log Login activity
CVE Exploited
Emergency Patch applied
IT Infra Events
Security Infra Events
Continuous Logging from Qualys Apps and 3rd Party
Correlation Engine
Threat Storyline
SOAR
Behavioral Analytics across MITRE ATT&CK stages
Next-Gen Analytics, Data Lake and Orchestration
SOC Analyst Can stop attacks before data exfiltration
Initial Access
Execution
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
C&C
MITRE ATT&CK Stages
Qualys.


Qualys.
New Event Source
3439
Sources
SIEM
IBM QRADAR 40
Splunk 23
FIREWALL
Palo Alto 5
Cisco ASA 3
CLOUD SERVICES
O 365 2
SalesForce 1
END POINT
Qualys Cloud Agent 1279
Symantec AV 760
McAfee ePO 1250
VM
Qualys VM 1
3rd Party VM 0
FIM
Qualys FIM 1
3rd Party FIM 0
Search
Event Source Catalog
Apps help you get started gaining insights from your data source by providing example searches and dashboards for common use cases.
Feel free to edit them as you need to get the results you want.
Palo Alto Firewall
Configured
Mar 12, 2019
Salesforce Cloud Services
Configured
Mar 12, 2019
Palo Alto Firewall
Configured
Mar 12, 2019
0365 Cloud Services
Coming Soon
QRadar SIEM
Coming Soon
Qualys VM
Configured
Mar 12, 2019
Qualys Log Collector
Configured
Mar 12, 2019
Microsoft AD
Configured
Mar 12, 2019
Splunk SIEM
Configured
Mar 12, 2019
Tipping Point
Configured
Mar 12, 2019
WAF
Configured
Mar 12, 2019
WAF
Configured
Mar 12, 2019
DDOS
Configured
Mar 12, 2019
Web Proxy
Configured
Mar 12, 2019
Decoy/ Deception
Configured
Mar 12, 2019

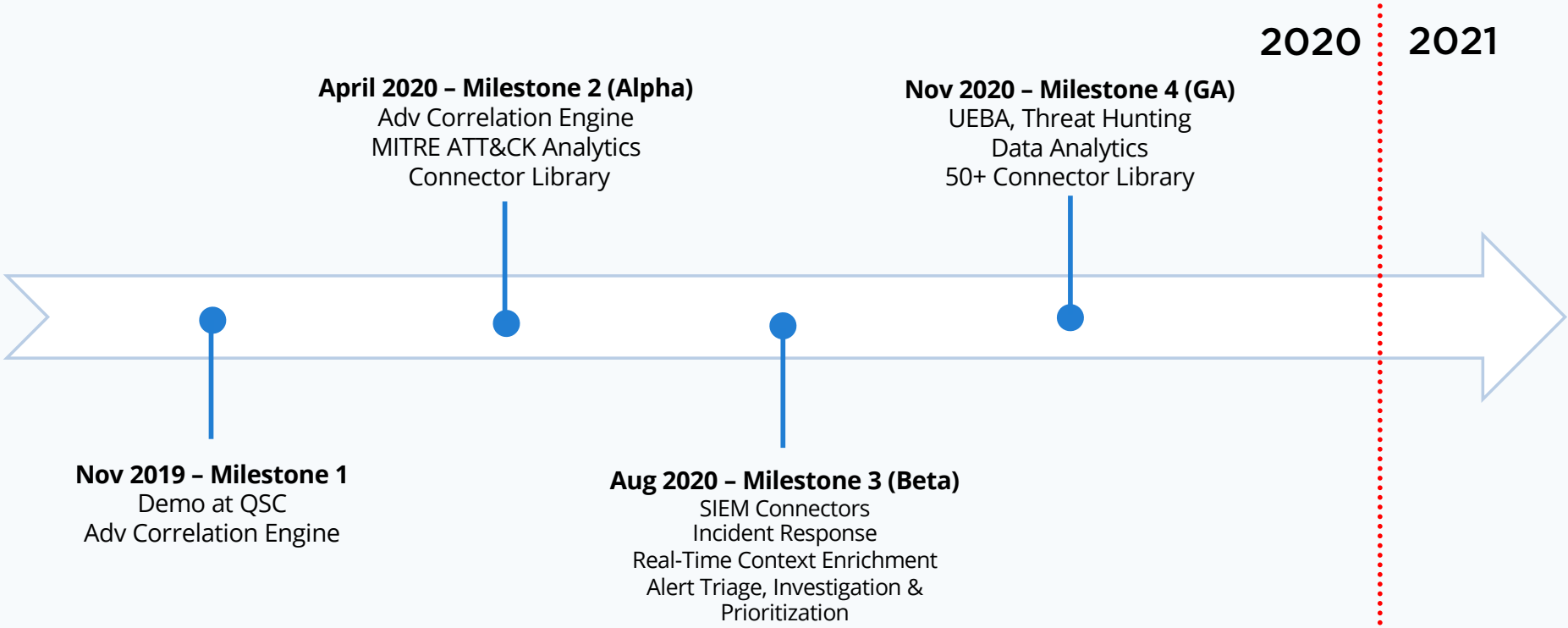

Qualys. Enterprise
Security Data Lake
DASHBOARD
THREAT MANAGEMENT
ADVANCED ANALYTICS
INVESTIGATE
RULES
REPORTS
CONFIGURATION
Rules
Rules
Library
Search Options
Search
Last 30 days
262
Techniques
Actions
STATUS
TID
TECHNIQUE
TACTIC
DATE CREATED
STATUS
In use 82
Available 180
TACTICS
Initial Access 10
Execution 27
Persistence 42
Privilege Escalation 21
Defense Evasion 63
Credential Access 19
Discovery 20
Lateral Movement 17
Collection 13
Exfiltration 9
Command and Control 21
LOG SOURCES
Missing 10
Installed 23
Available T1189 Drive-by Compromise A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's... Initial Access Jan 01, 2018
Available T1190 Exploit Public-Facing Application The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated... Initial Access Jan 01, 2018
Available T1182 AppCert DLLs Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager... Persistence, Privilege Escalation Jan 01, 2018
Available T1214 Credentials in Registry A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's... Credential Access Jan 01, 2018
Available T1075 Pass the Hash A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's... Lateral Movement Jan 01, 2018
Available T1214 Credentials in Registry A drive-by compromise is when an adversary gains access to a system through a user Credential Access Jan 01, 2018


Rule Editor
Cancel
Preview
Configure and Activate
Rule name
Possible Exploit Kit Detected
Description
A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's
Rule Conditions
Criticality
Select Option
Timeframe
Select Option
Time Unit
Select Option
Connections
Stream
Select option
Field
Select option
Stream
Select option
Field
Select option
Create Connection
Stream 1 having username = Stream 2 having user log
Stream 1
Remove
Log Source
Select Option
Occurance
Select Option
Group by
Select Option
Differ by
Select Option
Group
Remove
OR
THREAT INTELLIGENCE
Threat Intellignece Mapping
ON
Threat Intelligence Matching enables the system to match a signal with the Threat Intelligence data being made available by international organizations.
ADAPTIVE RESPONSE
Send Email
ON
Send to
Kunal Modasiya
Send Syslog Alert (3rd party tools)
ON
Syslog
mysyslogfile.here
Run Custom Script
ON
Custom script
mycustom.script.goes.here


Qualys. Enterprise
Security Analytics
DASHBOARD
THREAT MANAGEMENT
ADVANCED ANALYTICS
INVESTIGATE
RULES
REPORTS
CONFIGURATION
Threat Management
Threat Hunting Overview
Signals
Events
Search options
Search
Last 30 days
SIGNALS BREAKDOWN BY MITRE ATT&CK STAGES
27 ▲3 Initial Access
33 ▲5 Execution
18 ▲1 Percistence
3 ▲3 Privilege Escalation
12 ▲3 Defense Evasion
24 ▼3 Credential Access
3 ▼2 Discovery
19 ■3 Laterral Movement
22 ▼3 Collection
13 ▼1 Exfiltration
23 ▼12 Command & Control
TOP 10 SIGNALS BY MITRE TACTICS AND TECHNIQUES
442 Total
High 244
Medium 100
Low 98
TECHNIQUE
TACTIC
SIGNALS
Drive-by Compromise
Initial Access
72
Brute Force
Credential Access
66
Data Transfer Size Limits
Exfiltration
52
External Remote Services
Persistence
50
Windows Remote Management
Lateral Movement
50
Network Sniffing
Discovery
38
Replication Through Removable Media
Lateral Movement
36
Keychain
Credential Access
33
Data from Info
Collection
28
TOP 10 TRIGGERED/NOTABLE USERS BY SIGNALS COUNTS
256
44
75
151
36
USERNAME
LOCATION
SIGNALS
91 suneetha routhu quays_ur5 Foster City, CA 63
89 Shailesh Athalye quays_sa1 Pune, India 59
99 Kunal Modasiya kunalm_quays123 Foster City, CA 55
77 Abhijit Joshi abhs_321 Pune, India 50
73 Hari Srinivasan harstar-76 Foster City, CA 48
93 _mbsetupuser mb_doogg Foster City, CA 45
86 robertswanson rs_rs2019 Foster City, CA 45
98 root rs_rs2019 Shanghai, China 41
TOP 10 TRIGGERED/NOTABLE ASSET/HOSTNAME BY SIGNALS COUNTS
677 Total
High 324
Medium 181
Low 172
RISK
ASSET NAME
OS
SIGNALS
75 emily-pc 130568187 Red Hat Enterprise Linux 134
88 10.10.35.242 10.10.35.242 AIX 5.x / AIX 6.x 111
56 com-rhel70x64.... 10.10.35.241 Mac OS X 94
77 10.10.31.129 10.10.31.129 Windows 10 Enterprise 91
91 10.10.30.37 10.10.30.37 Windows 10 Enterprise 88
92 102354mbp15.lo... 10.0.1.91, fe80:0:... Ubuntu Linux 17.04 82
99 i-03ef90e7b729... 172.31.17.3 Linux 72
98 PCDemoEC2-SA 172.31.28.41 Microsoft Windows 66

Qualys.

Security Analytics – Milestone Timelines



Thank You

Dilip Bachwani
dbachwani@qualys.com