



QUALYS SECURITY CONFERENCE 2020

Threat Hunting with Qualys Going Beyond Your EDR Solutions

Chris Carlson

VP Product Management, Qualys, Inc.

Adversary Threat Tactics are Changing

Early 2010s

Zero-day Vulnerabilities

(Nation State, Industrial Espionage, Black Market)

Today

Rapidly weaponizing newly-disclosed vulnerabilities

(Good, Fast, Cheap – Pick 3)

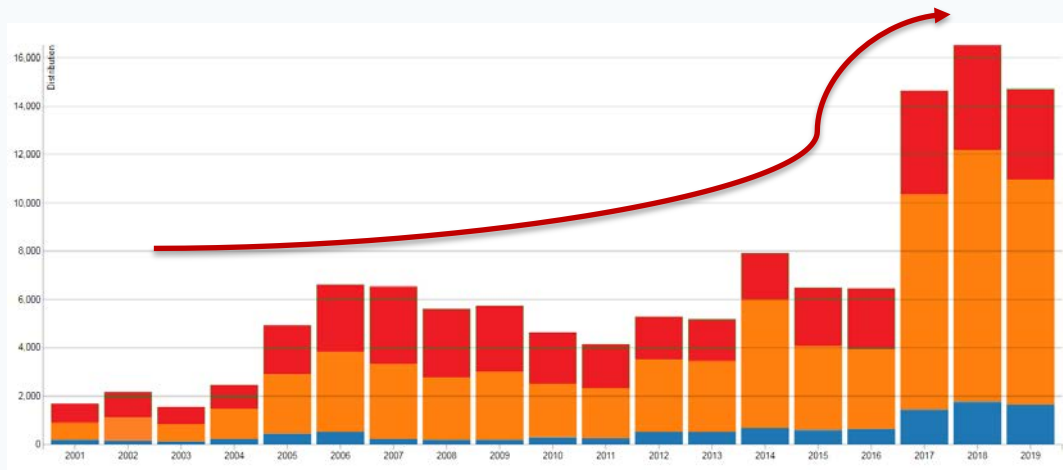
Known Critical Vulnerabilities are Increasing

14-16K vulnerabilities are disclosed 2017-2019

30-40% are ranked as “High” or “Critical” severity

Worm-able Vulnerabilities are increasing (WannaCry, BlueKeep)

“Mean Time to Weaponize” is rapidly decreasing year/year



Time to Weaponize

	<u>Vuln Disclosure</u>	<u>Exploit Date</u>	<u>Time</u>	<u>First Exploit Type</u>
WannaCry	March 2017	May 2017*	2 months	Ransomware
BlueKeep	May 2019	Nov 2019	6 months	Cryptominer
Citrix ADC	Dec 2019	Jan 2020	1 month	Cryptominer
Crypto DLL Vulnerability	Jan 2019	???	???	???

Get Proactive – Reduce the Attack Surface

AI

VM

Immediately discover assets and vulnerabilities

PM

Patch and verify remediation / stop the instance

PC

SCA

Change configuration to limit unauthorized access

CSA

Control network access / cloud security groups

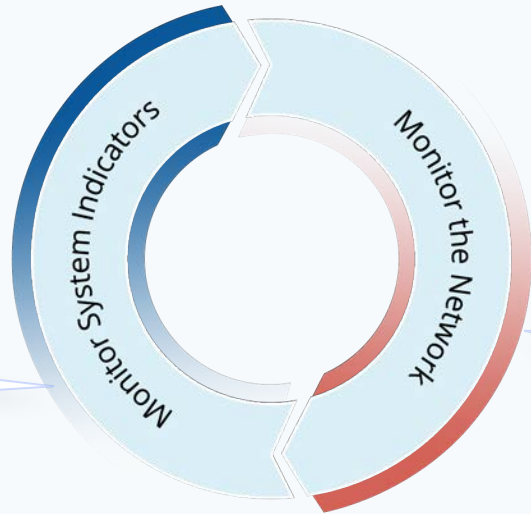
IOC

Add Endpoint Detection and Response

Proactively Hunt, Detect, and Respond

Indication of
Compromise

Detect malware, IOCs, IOAs,
and verify threat intel



Security Analytics
(Summer 2020)

Augment SIEMs by finding
attacks using behavioral
analytics and MITRE ATT&CK

Qualys IOC – Hunt Using Threat Intel

NotPetya Ransomware spreading using ETERNALBLUE Vulnerability and Credential Stealing

October 6, 2017

On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list.

Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods using the ETERNALBLUE vulnerability and credential stealing via a modified version of Mimikatz.

Technical Details

Anti-Virus Coverage

VirusTotal reports 0/66 anti-virus vendors have signatures for the credential stealer as of the date of this report

Files

Delivery – MD5: 71b6a493388e7d0b40c83ce903bc6b04

Installation – MD5: 7e37ab34ecdcc3e77e24522ddf4852d

Credential Stealer (new) – MD5: d926e76030f19f1f7ef0b3cd1a4e80f9

Secondary Actions

NotPetya leverages multiple propagation methods to spread within an infected network. According to malware analysis, NotPetya attempts the lateral movement techniques below:

2 Search for the file hash here...

The screenshot shows the Qualys Enterprise interface in the 'Hunting' section. A search bar at the top contains the MD5 hash 'd926e76030f19f1f7ef0b3cd1a4e80f9'. Below the search bar, a table lists related FIM events. The table has columns for TIME, OBJECT, ASSET, and SCORE. Two entries are visible, both for 'svvchost.exe' files on different assets.

TIME	OBJECT	ASSET	SCORE
a day ago 3:58:48 PM	svvchost.exe C:\14279270823	WIN2008R2-11566 10.11.114.113	
a day ago 12:22:57 PM	svvchost.exe C:\793972740527	WIN7-320860-T44 10.11.114.109	

1 Threat intelligence lists attack information ...

3 Find the object there.

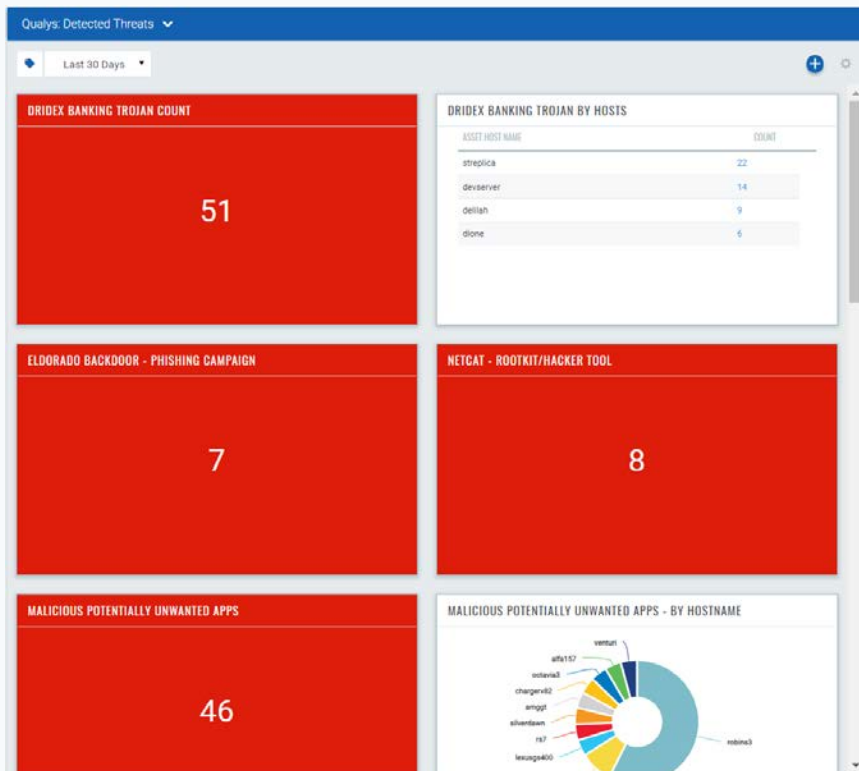
Detect Malware Missed by Anti-Virus

UK Government Contractor

- “Big 4” anti-virus installed
- Qualys Agent for Vulnerability Mgmt
- Added Qualys IOC on existing agents
- 256 hosts

Qualys IOC discovered...

- Dridex Banking Trojan (51)
- 4 domain controllers infected
- Backdoors (7) installed due to phishing campaigns
- Netcat (8) root kits installed
- 46 PUAs installed



Demo

a0c68e476f55d0b7cdd87b1b20a1e021672eec41f96e056d6289d8734491f9bb

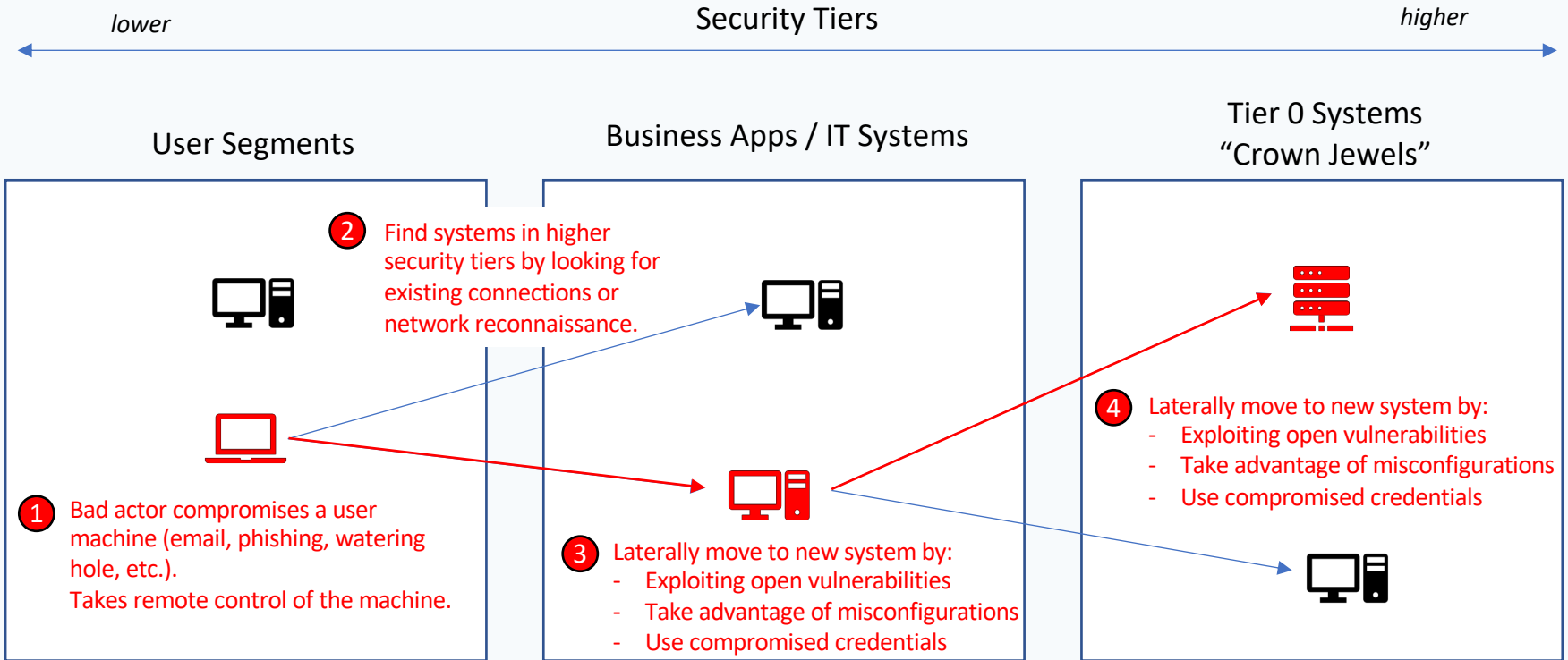
Beyond Endpoint Detection and Response: How can I better protect my crown jewels?

Threat Hunting Assumptions:

- Every user machine can be compromised – it only takes one click
- Every Remote Code Execution (RCE) vulnerability can be exploited
- Local Privilege Escalation and Credential Harvesting to move laterally
- System misconfigurations are often overlooked and easy to exploit
- Network segmentation is rarely used internally due to management

All attacks are not equal: can Adversaries reach my Critical Servers?

Adversary Lateral Movements (Attack Paths)



Attack Path Discovery *(Summer 2020)*

Network Reachability

Determine connections between hosts using Cloud Agent 

Passive + Active network collection

Store these connections in a Graph Database for fast query

+

Asset Security Posture

Remotely Exploitable Vulnerabilities  

System Misconfigurations  

Malware, IoCs, and Indicators of Activity 

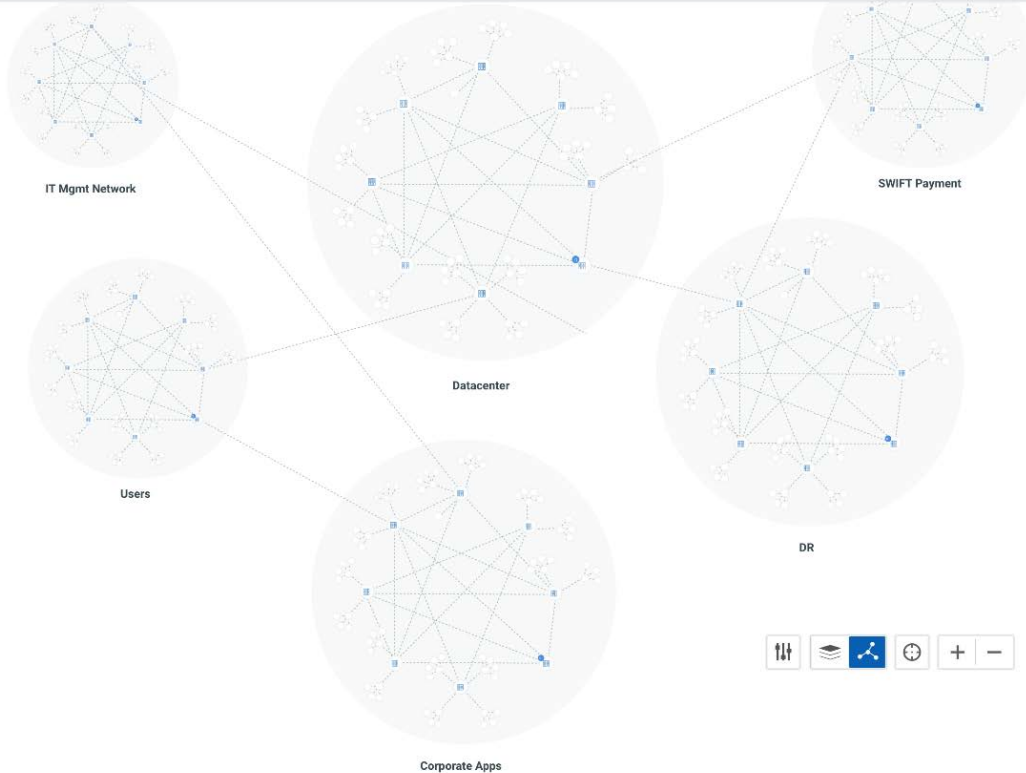
Network

Topology List View

🔍 Search

Last 7 days

🏠 🔍 Group Assets by...

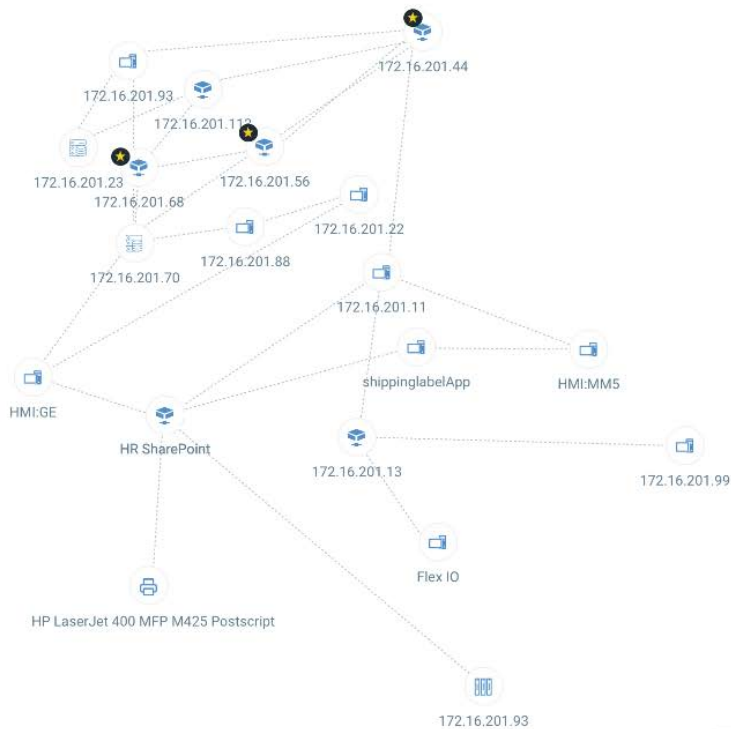


Search

Last 7 days



Group Assets by...



**Attack Path Discovery
for
Proactive Threat Hunting
and Response Priority**

Hunting

675K

Total Events

TYPE

file	258K
mutex	9.84K
network	19.4K
process	3.99K
registry	384K

EVENT ACTION

created	642K
established	4.65K
listening	14.7K
running	13.8K

SCORE

10	14
9	38
8	191
6	4
5	121

🔼 1 more

✕ 5ceec909f3dfc890fdd1e76d6f3cc093465c9d980d68b9987fc3f5eb289b6bd2

Active View ▾



1 - 50 of 675335



TIME ▾		OBJECT	ASSET	SCORE	DETAILS
3 minutes ago	⚙️	WindowsAzureTelemetryService.exe C:\WindowsAzure\GuestAgent_2.7.41491.949_2019-1...	WIN10PMIOC4 13.64.103.58,10.1.1.10	-	
3 minutes ago	⚙️	QualysAgent.exe C:\Program Files\Qualys\QualysAgent\QualysAgent.exe	WIN10PMIOC4 13.64.103.58,10.1.1.10	-	
3 minutes ago	⚙️	WmiPrvSE.exe C:\Windows\System32\wbem\WmiPrvSE.exe	WIN10PMIOC4 13.64.103.58,10.1.1.10	0	
3 minutes ago	🔄	125.227.22.242 (125-227-22-242.HINET-IP.hi... TCP CONNECTION - ESTABLISHED by svchost.exe	EC2AMAZ-Q1M5FIB 172.31.0.13,13.233.83.82	0	
3 minutes ago	🔄	13.82.189.202 : 63733 TCP CONNECTION - ESTABLISHED by svchost.exe	EC2AMAZ-Q1M5FIB 172.31.0.13,13.233.83.82	0	
3 minutes ago	🔄	fe80::281b:10bb:53e0:fff2%7 : 546 UDP CONNECTION - LISTENING by svchost.exe	EC2AMAZ-Q1M5FIB 172.31.0.13,13.233.83.82	0	
3 minutes ago	🔄	64.39.104.103 (qagpublic.qg2.apps.qualys.co... TCP CONNECTION - ESTABLISHED by QualysAgent.exe	WIN10PMIOC4 13.64.103.58,10.1.1.10	-	
3 minutes ago	🔄	211.247.115.130 : 57533 TCP CONNECTION - ESTABLISHED by svchost.exe	WIN10PMIOC4 13.64.103.58,10.1.1.10	0	
3 minutes ago	🔄	185.209.0.22 : 36585 TCP CONNECTION - ESTABLISHED by svchost.exe	WIN10PMIOC4 13.64.103.58,10.1.1.10	0	

Hunting

5

Total Events

TYPE

file	2
mutex	1
network	1
process	1

EVENT ACTION

created	2
established	1
running	2

SCORE

10	1
9	2
8	2

✕ 5ceec909f3dfc890fdd1e76d6f3cc093465c9d980d68b9987fc3f5eb289b6bd2 Active View ▾ ☰

1 - 5 of 5 🔍 📄 🔄 ⚙️

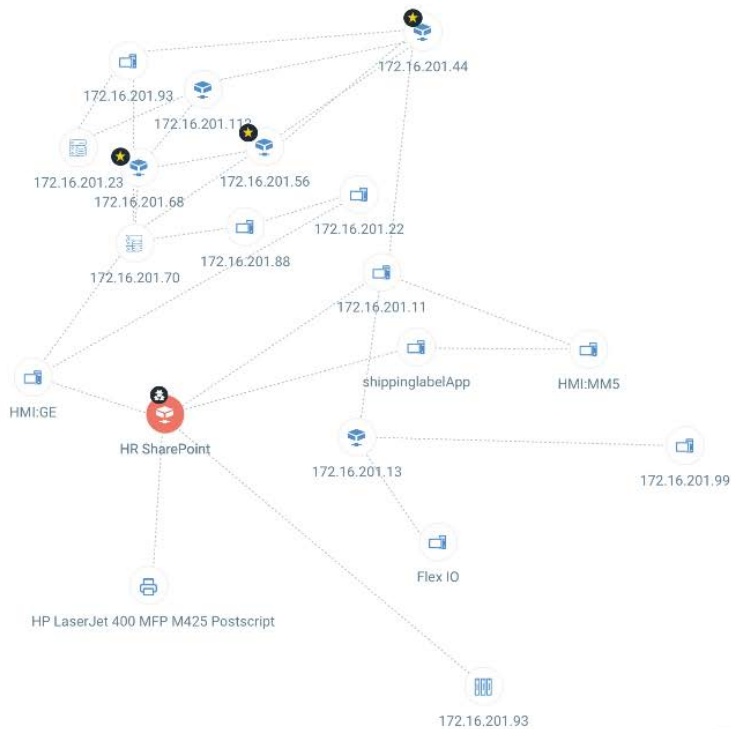
TIME ▾		OBJECT		ASSET	SCORE	DETAILS
21 hours ago 12:58:21 AM	🔗	66.85.173.57 (tar.theoutlan.com) : 443 TCP CONNECTION - ESTABLISHED by temp0291.exe	🇺🇸	SHAREPT003 172.31.0.111	10	Trickbot Trojan
a day ago 8:19:31 PM	📄	temp0291.exe c:\Users\qualys\AppData\Roaming	🇺🇸	SHAREPT003 172.31.0.111	8	Trickbot Trojan
a day ago 3:12:28 PM	⚙️	temp0291.exe C:\Users\qualys\AppData\Roaming\temp0291.exe	🇺🇸	SHAREPT003 172.31.0.111	9	Trickbot Trojan
a day ago 3:02:08 PM	🔒	\BaseNamedObjects\4C3D653494D1128 temp0291.exe	🇺🇸	SHAREPT003 172.31.0.111	9	Trickbot Trojan
2 days ago 11:18:23 AM	📄	temp0291.exe c:\Users\qualys\AppData\Roaming	🇺🇸	SHAREPT003 172.31.0.111	8	Trickbot Trojan

Search

Last 7 days



Group Assets by...

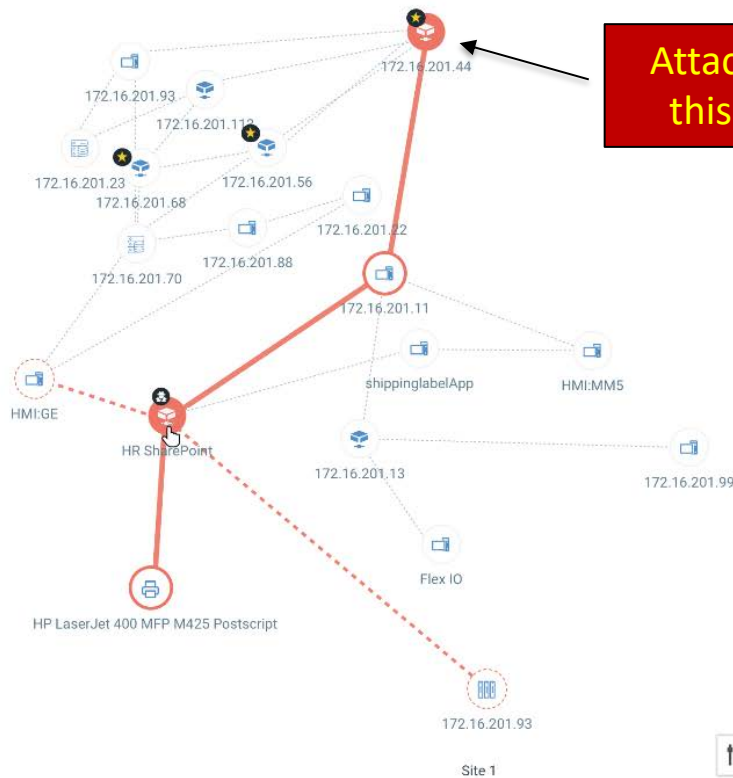


Search

Last 7 days



Group Assets by...



Attack path leads to this critical server

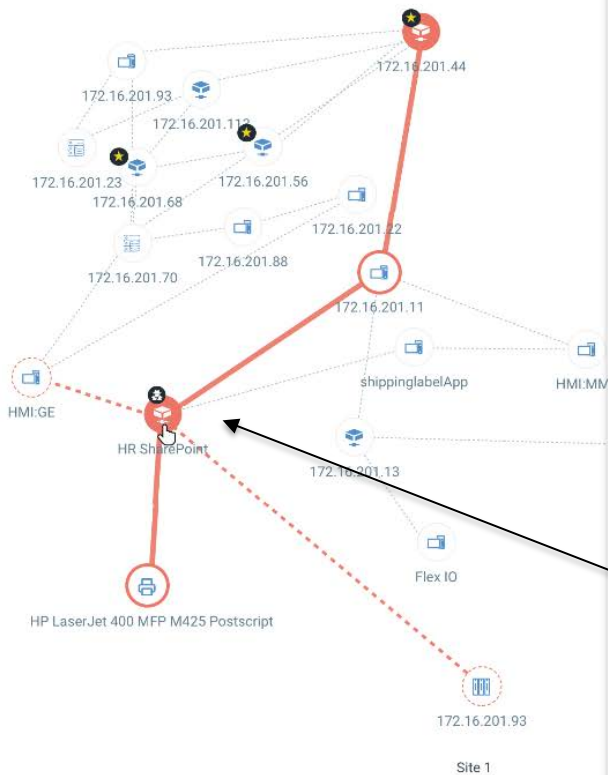


Search



Group Assets by...

Actions



HR SHAREPOINT

172.31.0.111

New York, NY

Tags

New York Corporate Apps HR Apps
Share Point 60_day_lastscan

INFECTIONS (4 Events)

Process: temp0294.exe

Malware: Trickbot | Risk Score: 9

File: WormDll64

Malware: Trickbot | Risk Score: 8

File: NetworkDll64

Malware: Trickbot | Risk Score: 8

File: ShareDll64

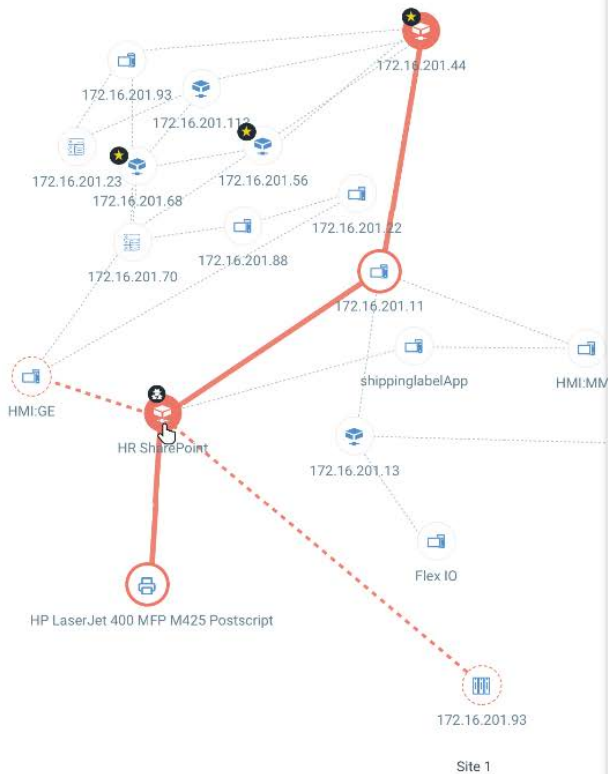
Malware: Trickbot | Risk Score: 8

Quickly investigate the host to see the active attack

Search



Group Assets by...



Actions



HR SHAREPOINT

172.31.0.111

New York, NY

Tags

New York Corporate Apps HR Apps
Share Point 60_day_lastscan

INFECTIONS (4 Events)

Process: temp0294.exe

Malware: Trickbot | Risk Score: 8

File: WormDll64

Malware: Trickbot | Risk Score: 8

File: NetworkDll64

Malware: Trickbot | Risk Score: 8

File: ShareDll64

Malware: Trickbot | Risk Score: 8

Quick Menu

- View Asset Details
- Execute a Response
- Quarantine Host

Take action on this host to stop the attacker in their tracks

Network

Search

Group As

Execute a Response

The following response will be executed for the selected processes and files on the defined hosts.

Process (1)

RISK SCORE	PROCESS NAME	MALWARE	PID	HOST
9	temp0291.exe	TrickBot	4417	SHAREPT003

 Kill Process Quarantine File

File Type (3)

RISK SCORE	FILE NAME	MALWARE	HOST
8	WormDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003
8	NetworkDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003
8	ShareDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003

 Quarantine File

Cancel

Confirm

172.16.201.93

Site 1



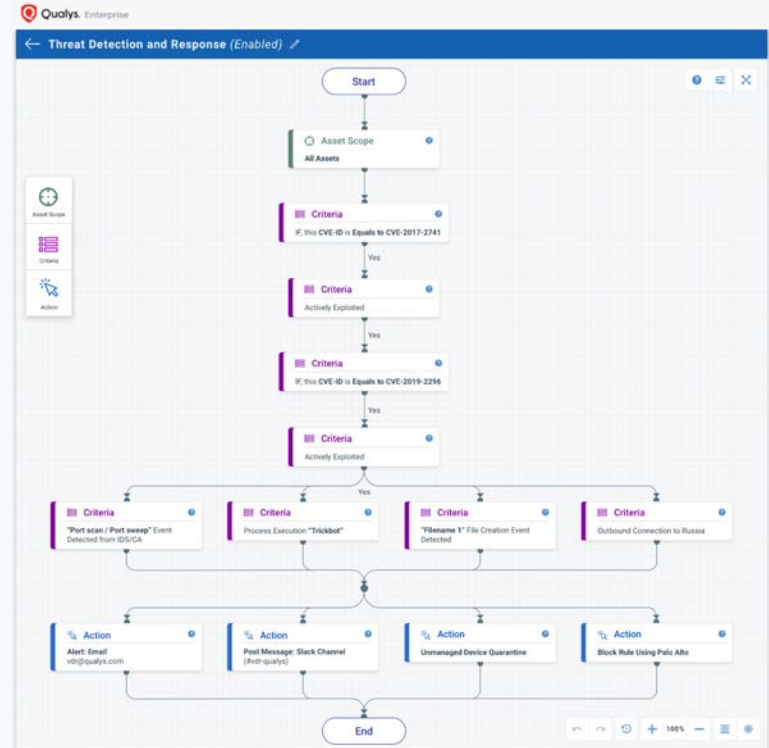
Scale Human Response with Automation

Qualys finds active attacks on endpoint using Indication of Compromise

Go beyond endpoint detection with Security Analytics – correlate user, network, application, cloud, container

Use attack path discovery as metadata to detect attacks that can reach critical assets

Automate response to protect critical assets using Security Orchestration response playbooks



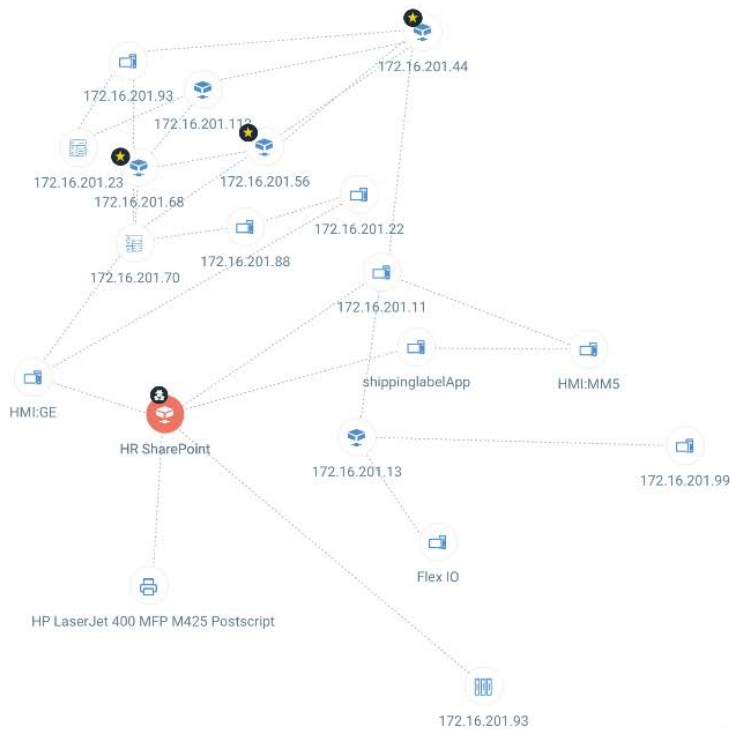
**Attack Path Discovery
to
Prioritize Patching
and
Improve Security Defenses**

Search

Last 7 days



Group Assets by...

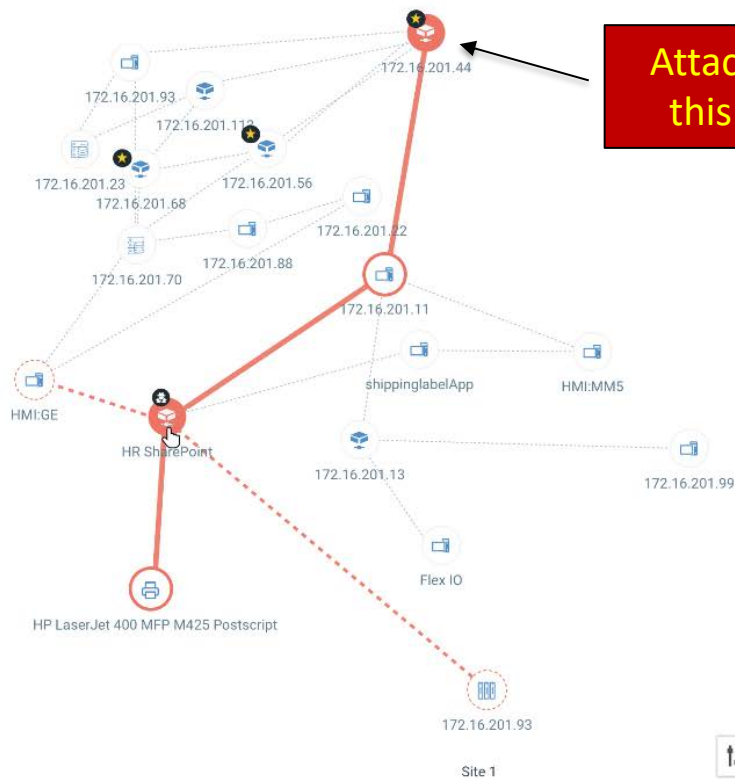


Search

Last 7 days



Group Assets by...



Attack path leads to this critical server

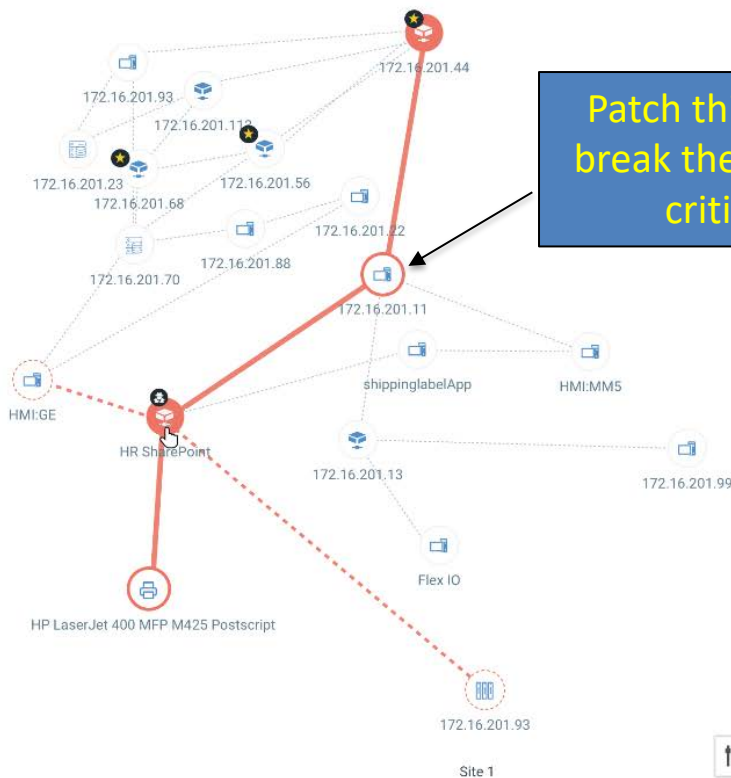


Search

Last 7 days



Group Assets by...



Patch this one asset to break the attack path to critical server



Vulnerability Remediation Prioritization

CVSSv2 / CVSSv3 base scores

Qualys QID Severity score

Qualys Tagging for Asset Business Criticality

Qualys Threat Protection Real-Time Indicators
(based on threat intel and live attacks)

Qualys VMDR Threat Prioritization
(Machine Learning model + Contextual Awareness)

Qualys Attack Path Discovery



Thank You

Chris Carlson

ccarlson@qualys.com