How to Get Better Monitoring of MITRE ATT&CK Attack Techniques

Chase Snyder, Product Marketing Mgr., ExtraHop

Greg Copeland, Director Technical Alliances, Keysight

ExtraHop

KEYSIGHT TECHNOLOGIES

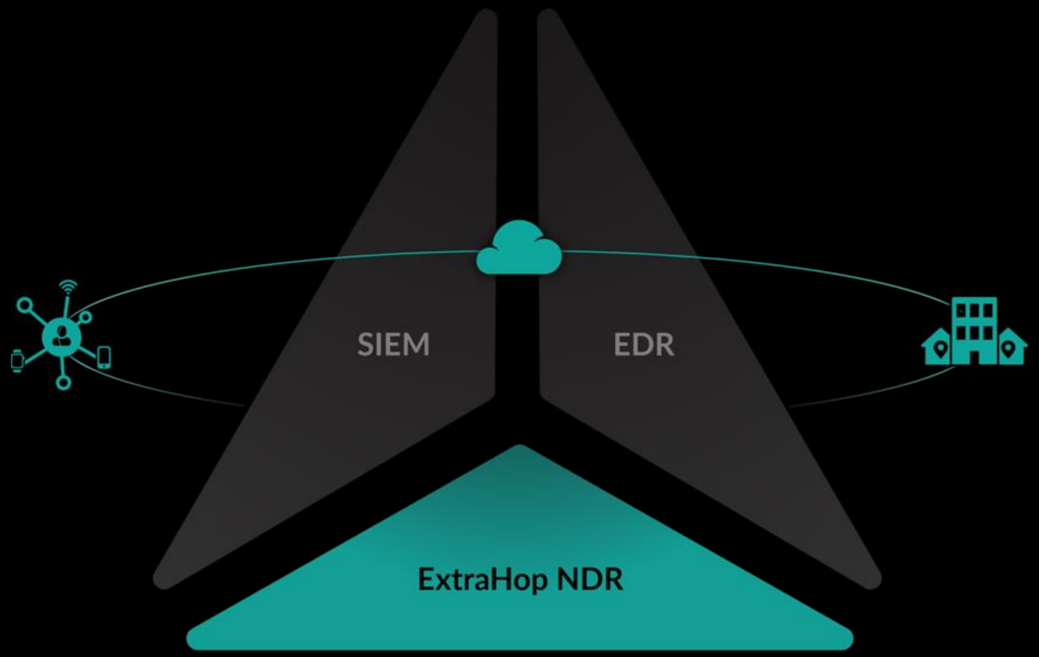
Agenda

- How network data complements logs
- Applying network data and analysis to MITRE attacks
- Example MITRE attack network detection and response
- Ensuring complete network visibility
- Examples of MITRE attack detection and analysis
- Validating security configuration against MITRE attacks.
- Q & A

Chase Snyder
Sr. Product Marketing Mgr.
ExtraHop

Greg Copeland
Dir. Technical Alliances,
Keysight

Network Intelligence Creates a Strong Foundation for Countering Advanced Threats



Difficult To Evade

So threats can't hide

Covert & Agentless

Stay stealth

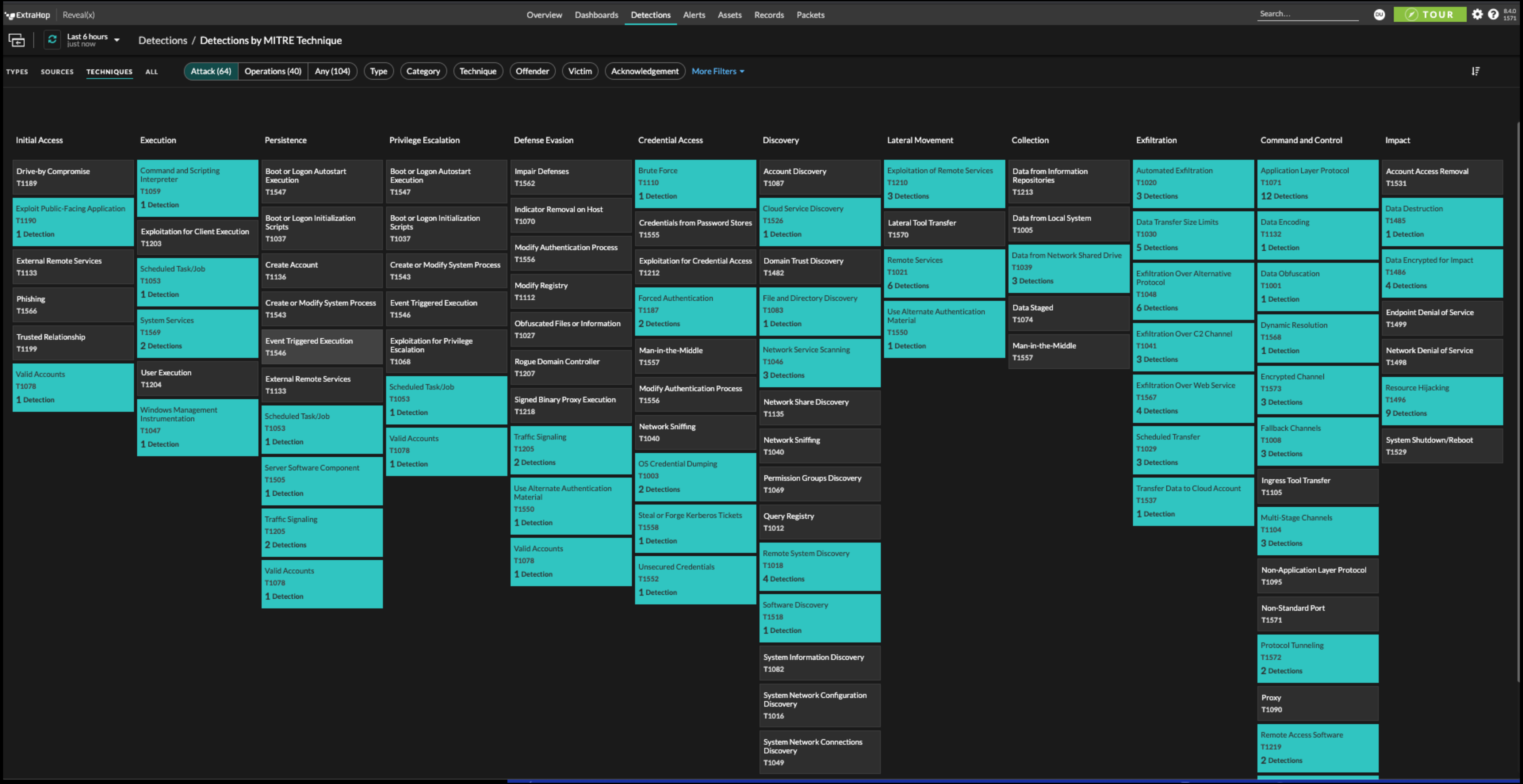
Ground Truth

From core to edge to cloud

> “ [A hacker's] worst nightmare is that out-of-band [tool] that’s capturing all the data, understanding anomalous behavior that's going on.

ROB JOYCE
NATIONAL SECURITY AGENCY

Network Data is Vital for Detecting MITRE ATT&CK Tactics



Initial Access

- Drive-by Compromise T1189
- Exploit Public-Facing Application T1190 1 Detection
- External Remote Services T1133
- Phishing T1566
- Trusted Relationship T1199
- Valid Accounts T1078 1 Detection

Execution

- Command and Scripting Interpreter T1059 1 Detection
- Exploitation for Client Execution T1203
- Scheduled Task/Job T1053 1 Detection
- System Services T1569 2 Detections
- User Execution T1204
- Windows Management Instrumentation T1047 1 Detection

Persistence

- Boot or Logon Autostart Execution T1547
- Boot or Logon Initialization Scripts T1037
- Create Account T1136
- Create or Modify System Process T1543
- Event Triggered Execution T1546
- External Remote Services T1133
- Scheduled Task/Job T1053 1 Detection
- Server Software Component T1505 1 Detection
- Traffic Signaling T1205 2 Detections
- Valid Accounts T1078 1 Detection

Privilege Escalation

- Boot or Logon Autostart Execution T1547
- Boot or Logon Initialization Scripts T1037
- Create or Modify System Process T1543
- Event Triggered Execution T1546
- Exploitation for Privilege Escalation T1068
- Scheduled Task/Job T1053 1 Detection
- Valid Accounts T1078 1 Detection

Defense Evasion

- Impair Defenses T1562
- Indicator Removal on Host T1070
- Modify Authentication Process T1556
- Modify Registry T1112
- Obfuscated Files or Information T1027
- Rogue Domain Controller T1207
- Signed Binary Proxy Execution T1218
- Traffic Signaling T1205 2 Detections
- Use Alternate Authentication Material T1550 1 Detection
- Valid Accounts T1078 1 Detection

Credential Access

- Brute Force T1110 1 Detection
- Credentials from Password Stores T1555
- Exploitation for Credential Access T1212
- Forced Authentication T1187 2 Detections
- Man-in-the-Middle T1557
- Modify Authentication Process T1556
- Network Sniffing T1040
- OS Credential Dumping T1003 2 Detections
- Steal or Forge Kerberos Tickets T1558 1 Detection
- Unsecured Credentials T1552 1 Detection

Discovery

- Account Discovery T1087
- Cloud Service Discovery T1526 1 Detection
- Domain Trust Discovery T1482
- File and Directory Discovery T1083 1 Detection
- Network Service Scanning T1046 3 Detections
- Network Share Discovery T1135
- Network Sniffing T1040
- Permission Groups Discovery T1069
- Query Registry T1012
- Remote System Discovery T1018 4 Detections
- Software Discovery T1518 1 Detection
- System Information Discovery T1082
- System Network Configuration Discovery T1016
- System Network Connections Discovery T1049

Lateral Movement

- Exploitation of Remote Services T1210 3 Detections
- Lateral Tool Transfer T1570
- Remote Services T1021 6 Detections
- Use Alternate Authentication Material T1550 1 Detection

Collection

- Data from Information Repositories T1213
- Data from Local System T1005
- Data from Network Shared Drive T1039 3 Detections
- Data Staged T1074
- Man-in-the-Middle T1557

Exfiltration

- Automated Exfiltration T1020 3 Detections
- Data Transfer Size Limits T1030 5 Detections
- Exfiltration Over Alternative Protocol T1048 6 Detections
- Exfiltration Over C2 Channel T1041 3 Detections
- Exfiltration Over Web Service T1567 4 Detections
- Scheduled Transfer T1029 3 Detections
- Transfer Data to Cloud Account T1537 1 Detection

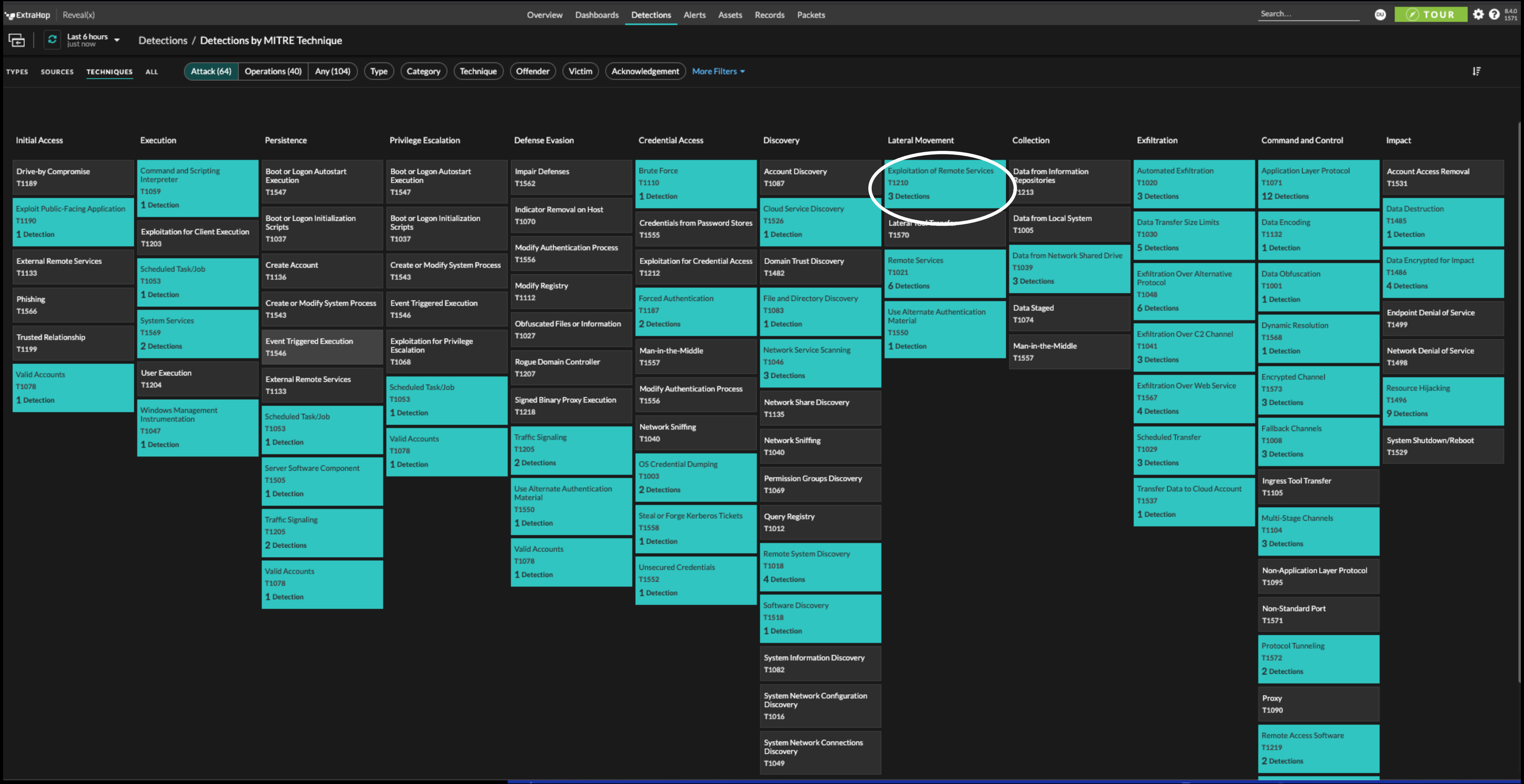
Command and Control

- Application Layer Protocol T1071 12 Detections
- Data Encoding T1132 1 Detection
- Data Obfuscation T1001 1 Detection
- Dynamic Resolution T1568 1 Detection
- Encrypted Channel T1573 3 Detections
- Fallback Channels T1008 3 Detections
- Ingress Tool Transfer T1105
- Multi-Stage Channels T1104 3 Detections
- Non-Application Layer Protocol T1095
- Non-Standard Port T1571
- Protocol Tunneling T1572 2 Detections
- Proxy T1090
- Remote Access Software T1219 2 Detections

Impact

- Account Access Removal T1531
- Data Destruction T1485 1 Detection
- Data Encrypted for Impact T1486 4 Detections
- Endpoint Denial of Service T1499
- Network Denial of Service T1498
- Resource Hijacking T1496 9 Detections
- System Shutdown/Reboot T1529

Network Data is Vital for Detecting MITRE ATT&CK Tactics



Detections / Detections by MITRE Technique

Initial Access

- Drive-by Compromise T1189
- Exploit Public-Facing Application T1190 1 Detection
- External Remote Services T1133
- Phishing T1566
- Trusted Relationship T1199
- Valid Accounts T1078 1 Detection

Execution

- Command and Scripting Interpreter T1059 1 Detection
- Exploitation for Client Execution T1203
- Scheduled Task/Job T1053 1 Detection
- System Services T1569 2 Detections
- User Execution T1204
- Windows Management Instrumentation T1047 1 Detection

Persistence

- Boot or Logon Autostart Execution T1547
- Boot or Logon Initialization Scripts T1037
- Create Account T1136
- Create or Modify System Process T1543
- Event Triggered Execution T1546
- External Remote Services T1133
- Scheduled Task/Job T1053 1 Detection
- Server Software Component T1505 1 Detection
- Traffic Signaling T1205 2 Detections
- Valid Accounts T1078 1 Detection

Privilege Escalation

- Boot or Logon Autostart Execution T1547
- Boot or Logon Initialization Scripts T1037
- Create or Modify System Process T1543
- Event Triggered Execution T1546
- Exploitation for Privilege Escalation T1068
- Scheduled Task/Job T1053 1 Detection
- Valid Accounts T1078 1 Detection

Defense Evasion

- Impair Defenses T1562
- Indicator Removal on Host T1070
- Modify Authentication Process T1556
- Modify Registry T1112
- Obfuscated Files or Information T1027
- Rogue Domain Controller T1207
- Signed Binary Proxy Execution T1218
- Traffic Signaling T1205 2 Detections
- Use Alternate Authentication Material T1550 1 Detection
- Valid Accounts T1078 1 Detection

Credential Access

- Brute Force T1110 1 Detection
- Credentials from Password Stores T1555
- Exploitation for Credential Access T1212
- Forced Authentication T1187 2 Detections
- Man-in-the-Middle T1557
- Modify Authentication Process T1556
- Network Sniffing T1040
- OS Credential Dumping T1003 2 Detections
- Steal or Forge Kerberos Tickets T1558 1 Detection
- Unsecured Credentials T1552 1 Detection

Discovery

- Account Discovery T1087
- Cloud Service Discovery T1526 1 Detection
- Domain Trust Discovery T1482
- File and Directory Discovery T1083 1 Detection
- Network Service Scanning T1046 3 Detections
- Network Share Discovery T1135
- Network Sniffing T1040
- Permission Groups Discovery T1069
- Query Registry T1012
- Remote System Discovery T1018 4 Detections
- Software Discovery T1518 1 Detection
- System Information Discovery T1082
- System Network Configuration Discovery T1016
- System Network Connections Discovery T1049

Lateral Movement

- Exploitation of Remote Services T1210 3 Detections
- Lateral Tool Transfer T1570
- Remote Services T1021 6 Detections
- Use Alternate Authentication Material T1550 1 Detection

Collection

- Data from Information Repositories T1213
- Data from Local System T1005
- Data from Network Shared Drive T1039 3 Detections
- Data Staged T1074
- Man-in-the-Middle T1557

Exfiltration

- Automated Exfiltration T1020 3 Detections
- Data Transfer Size Limits T1030 5 Detections
- Exfiltration Over Alternative Protocol T1048 6 Detections
- Exfiltration Over C2 Channel T1041 3 Detections
- Exfiltration Over Web Service T1567 4 Detections
- Scheduled Transfer T1029 3 Detections
- Transfer Data to Cloud Account T1537 1 Detection

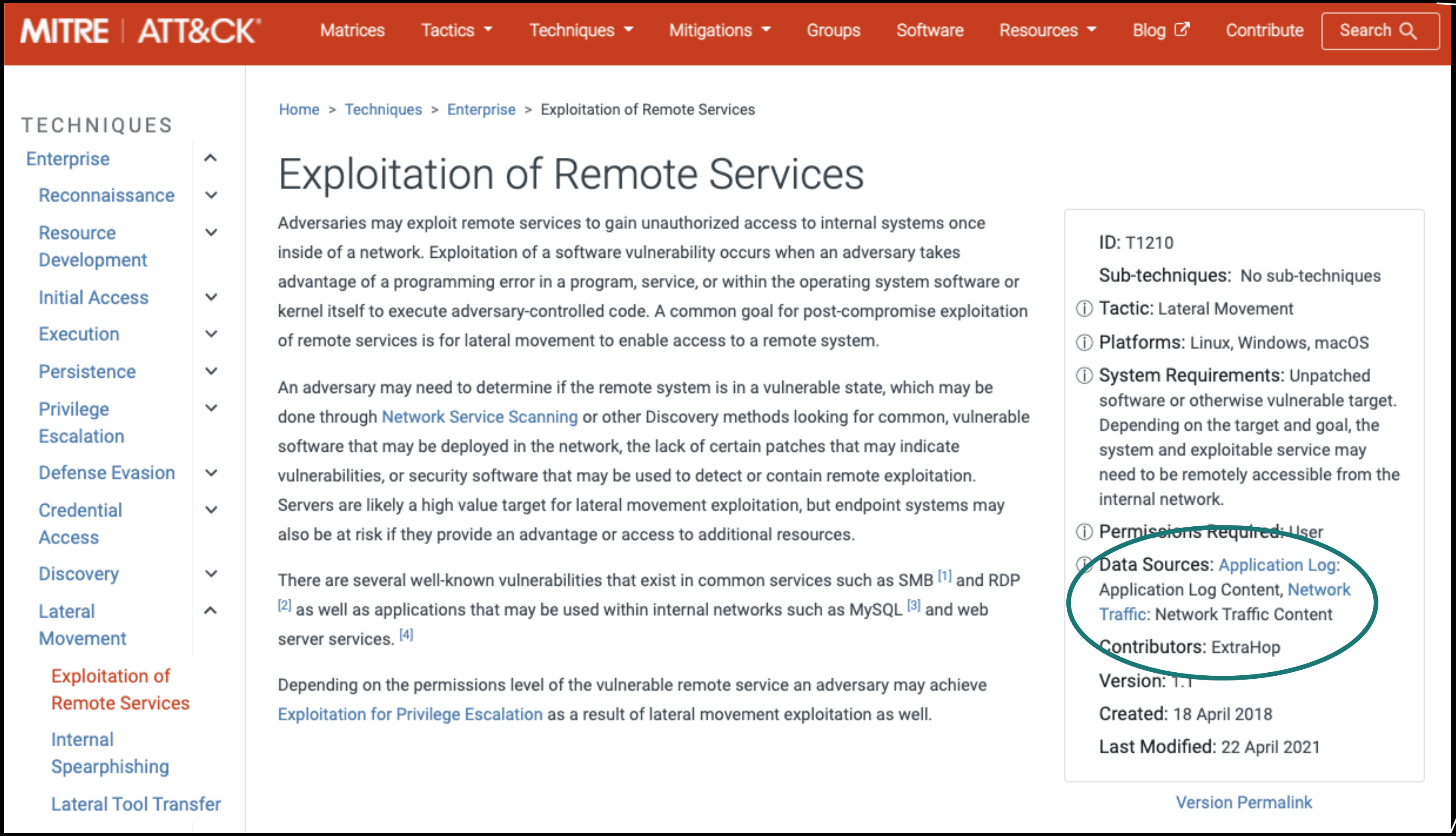
Command and Control

- Application Layer Protocol T1071 12 Detections
- Data Encoding T1132 1 Detection
- Data Obfuscation T1001 1 Detection
- Dynamic Resolution T1568 1 Detection
- Encrypted Channel T1573 3 Detections
- Fallback Channels T1008 3 Detections
- Ingress Tool Transfer T1105
- Multi-Stage Channels T1104 3 Detections
- Non-Application Layer Protocol T1095
- Non-Standard Port T1571
- Protocol Tunneling T1572 2 Detections
- Proxy T1090
- Remote Access Software T1219 2 Detections

Impact

- Account Access Removal T1531
- Data Destruction T1485 1 Detection
- Data Encrypted for Impact T1486 4 Detections
- Endpoint Denial of Service T1499
- Network Denial of Service T1498
- Resource Hijacking T1496 9 Detections
- System Shutdown/Reboot T1529

Network Data is Vital for Detecting MITRE ATT&CK Tactics



Home > Techniques > Enterprise > Exploitation of Remote Services

Exploitation of Remote Services

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through Network Service Scanning or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB [1] and RDP [2] as well as applications that may be used within internal networks such as MySQL [3] and web server services. [4]

Depending on the permissions level of the vulnerable remote service an adversary may achieve Exploitation for Privilege Escalation as a result of lateral movement exploitation as well.

ID: T1210

Sub-techniques: No sub-techniques

ⓘ Tactic: Lateral Movement

ⓘ Platforms: Linux, Windows, macOS

ⓘ System Requirements: Unpatched software or otherwise vulnerable target. Depending on the target and goal, the system and exploitable service may need to be remotely accessible from the internal network.

ⓘ Permissions Required: User

ⓘ Data Sources: Application Log: Application Log Content, Network Traffic: Network Traffic Content

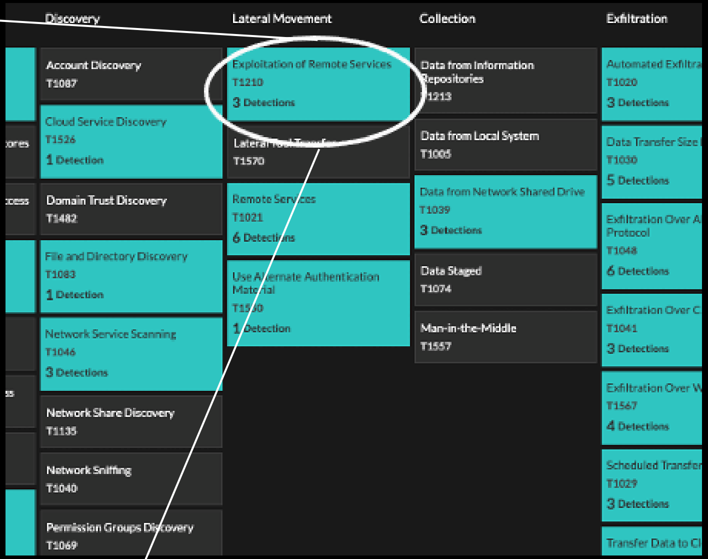
Contributors: ExtraHop

Version: 1.1

Created: 18 April 2018

Last Modified: 22 April 2021

Version Permalink

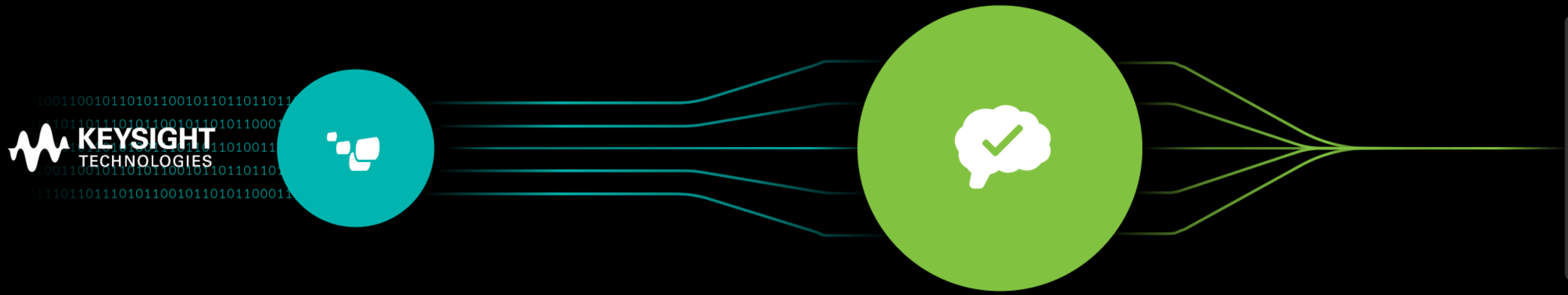


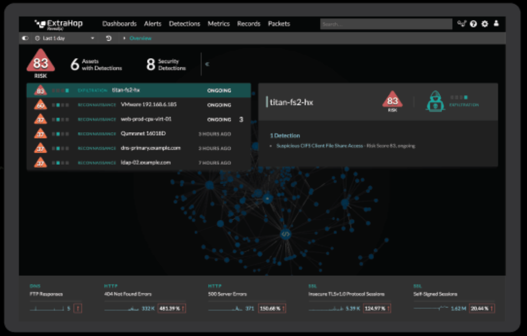
Discovery	Lateral Movement	Collection	Exfiltration
Account Discovery T1087	Exploitation of Remote Services T1210 3 Detections	Data from Information Repositories T1213	Automated Exfiltra T1020 3 Detections
Cloud Service Discovery T1526 1 Detection	Lateral Tool Transfer T1570	Data from Local System T1005	Data Transfer Size T1030 5 Detections
Domain Trust Discovery T1482	Remote Services T1021 6 Detections	Data from Network Shared Drive T1039 3 Detections	Exfiltration Over A Protocol T1048 6 Detections
File and Directory Discovery T1083 1 Detection	Use Alternate Authentication Material T1550 1 Detection	Data Staged T1074	Exfiltration Over C T1041 3 Detections
Network Service Scanning T1046 3 Detections		Man-in-the-Middle T1557	Exfiltration Over W T1567 4 Detections
Network Share Discovery T1135			Scheduled Transfer T1029 3 Detections
Network Sniffing T1040			Transfer Data to Cl
Permission Groups Discovery T1069			

NETWORK DATA ANALYSIS

Fundamental Breakthrough in ML and Analytics

PROVIDING ANSWERS IN REAL-TIME AND AT SCALE





ExtraHop Dashboards Alerts Detections Metrics Records Packets

Last 1 day · Overview

83 RISK · 6 Assets with Detections · 8 Security Detections

83	EXFILTRATION	titan-fs2-hx	ONGOING
60	RECONNAISSANCE	VMware 192.168.6.185	ONGOING
37	RECONNAISSANCE	web-prod-cps-virt-01	ONGOING 3
37	RECONNAISSANCE	Qumranet 16018D	3 HOURS AGO
37	RECONNAISSANCE	dns-primary.example.com	3 HOURS AGO
37	RECONNAISSANCE	ldap-02.example.com	7 HOURS AGO

titan-fs2-hx · 83 RISK · EXFILTRATION

1 Detection
- Suspicious CIFS Client File Share Access - Risk Score 83, ongoing

DNS	HTTP	HTTP	SSL	SSL
FTP Responses	404 Not Found Errors	500 Server Errors	Insecure TLSv1.0 Protocol Sessions	Self-Signed Sessions
5 ↑	332 K 481.39 % ↑	371 150.68 % ↑	5.39 K 124.97 % ↑	1.62 M 20.44 % ↑

UNSTRUCTURED PACKETS

AUTO-DISCOVERY AND CLASSIFICATION

STREAM PROCESSING

MACHINE LEARNING

INSIGHT AT 100 GBPS

IMMEDIATE ANSWERS

Threat Signals Extracted From The Network in Real Time

HTTP INTEL

- 121.35.232.13 □ 192.168.1.3:80
- http://www.extrahop.com/login
- 35s response time – **95% server delay**
- **500 server error**
- SessionID: ACD53332
- Cookie: …..
- UserName: john_smith
- OrderID: 3838383
- User agent: Firefox53/Windows10

SMB/CIFS INTEL

- User: \\WORKGROUP\jsmith
- File: \\WS1\Desktop\ **a.ppt.encrypted**
- Method: WRITE
- Access Time: 520 ms
- Network Transfer Time: 10 s
- Bytes Transferred: 500 MB
- UserName: john_smith

DATABASE INTEL

- 192.168.23.5 □ 192.168.25.8:1521
- User: **sa**
- Query: select * from accounts
- 20s response time – **90% server delay**
- Bytes Transferred: 100 KB
- Network Transfer Time: 0.5 ms
- Error: **ORA-00942 table or view does not exist**

KERBEROS INTEL

- 192.168.23.2 □ 10.1.3.5:88
- User: ptdaniels
- Message Type: TGS Request
- Server Realm: sa.local
- 20 ms response time
- Bytes Transferred: 119 B
- Network Transfer Time: 0.5 ms
- Error: KDC_ERR_CLIENT_REVOKED

Example - Command & Control - App Layer Protocol (MITRE ATT&CK T1071)

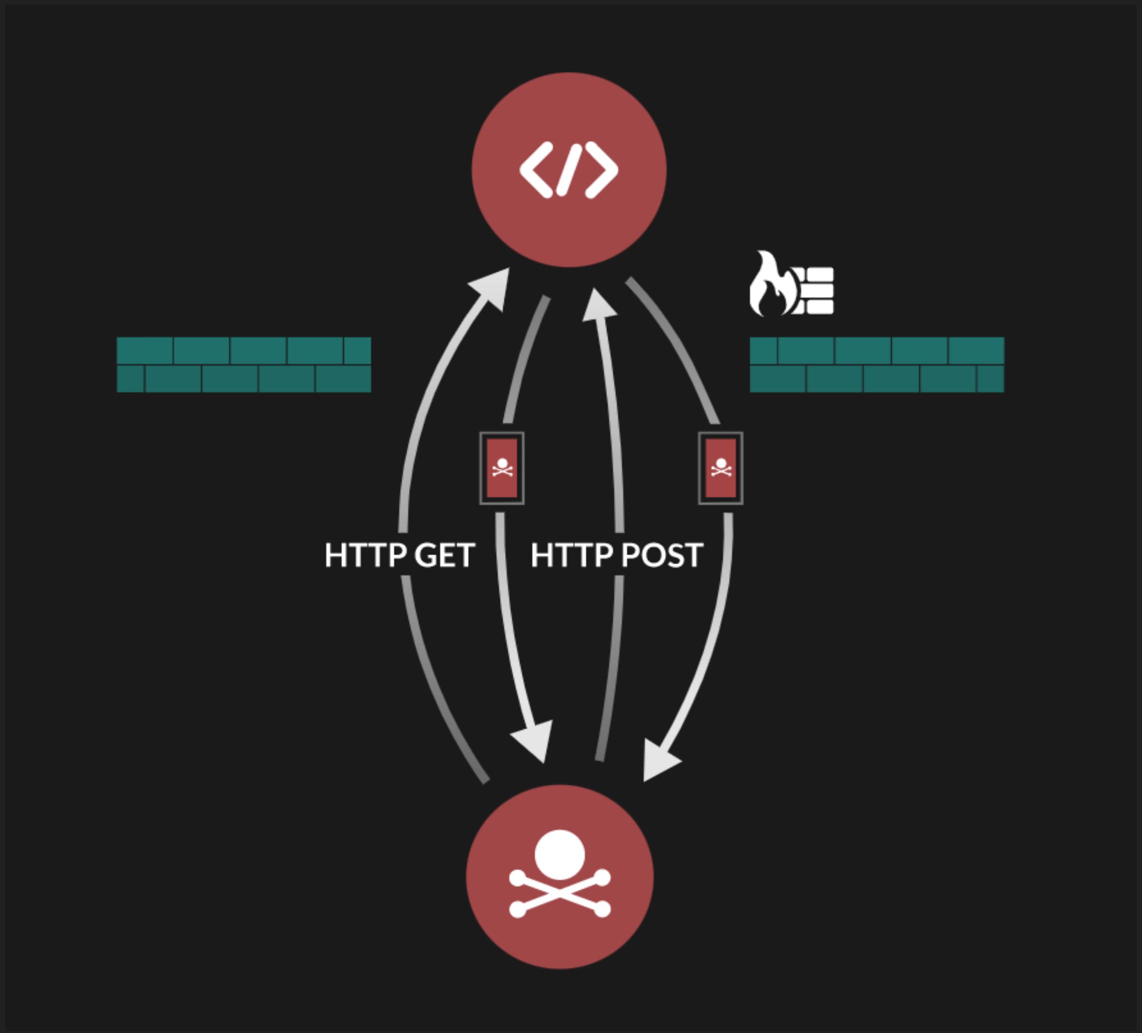
Command & Control

Once an attacker has compromised an internal host on their target network, they establish a command & control mechanism to control that host's behavior and use it for further reconnaissance, credential access, and lateral movement.

- Command & Control activity is often disguised in normal, chatty network protocol activity, such as DNS, HTTP, and even FTP

Network derived Signals:

- Unusual behavior across common C2 protocols like DNS & HTTP
- NG-IDS can detect specific malware leveraging C2 tactics



ExtraHop Full-Spectrum Detection

HYGIENE

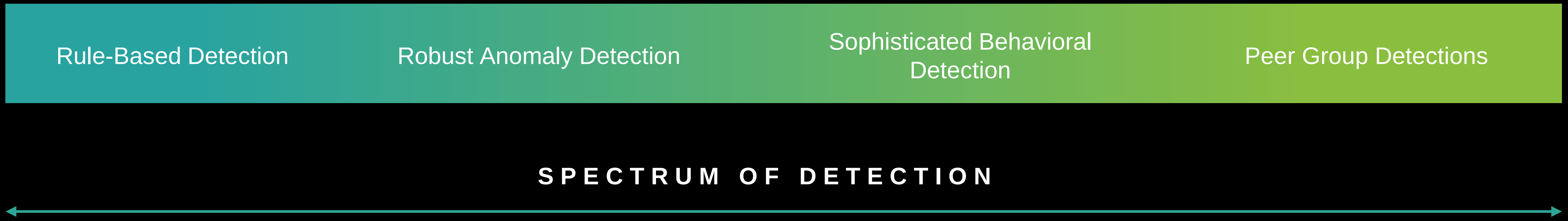
Activity that represents risk: ports, protocols, cryptographic compliance, and vulnerable or non-compliant services

KNOWN ATTACKS

IP addresses, domains, file names, payload strings, or protocol behavior observed in past attacks (including intelligence feeds)

UNKNOWN ATTACKS

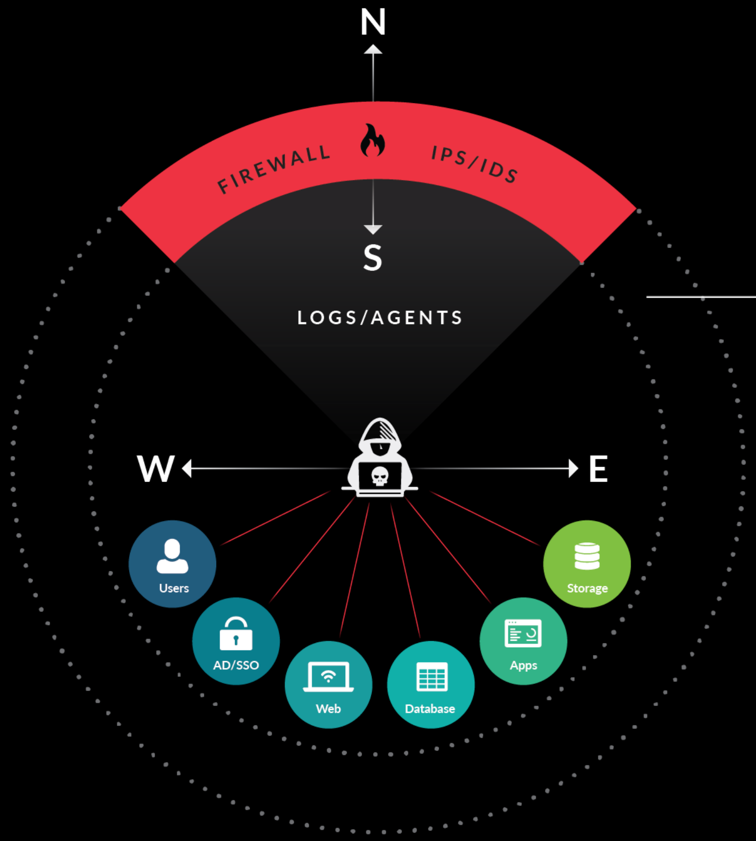
Attacks that do not have a previously known identifier, but exhibit anomalous behavior that can be linked to part of the attack lifecycle



MITRE | ATT&CK™ NIST CIS Controls™

Network Data is Critical For Detecting Advanced Threats

If you were compromised, how would you know?



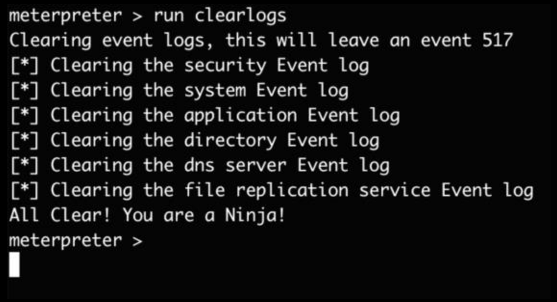
70% DARKSPACE

Attackers bypass defenses and have free rein

67% ENCRYPTED TRAFFIC
Malicious traffic is often encrypted

56 DAYS OF DWELL TIME
Median before attackers are found

72% DESTRUCTION OF LOGS
Attackers easily cover their tracks



```
meterpreter > run clearlogs
Clearing event logs, this will leave an event 517
[*] Clearing the security Event log
[*] Clearing the system Event log
[*] Clearing the application Event log
[*] Clearing the directory Event log
[*] Clearing the dns server Event log
[*] Clearing the file replication service Event log
All Clear! You are a Ninja!
meterpreter >
```

Keysight Technologies: You can’t secure traffic which you don’t see

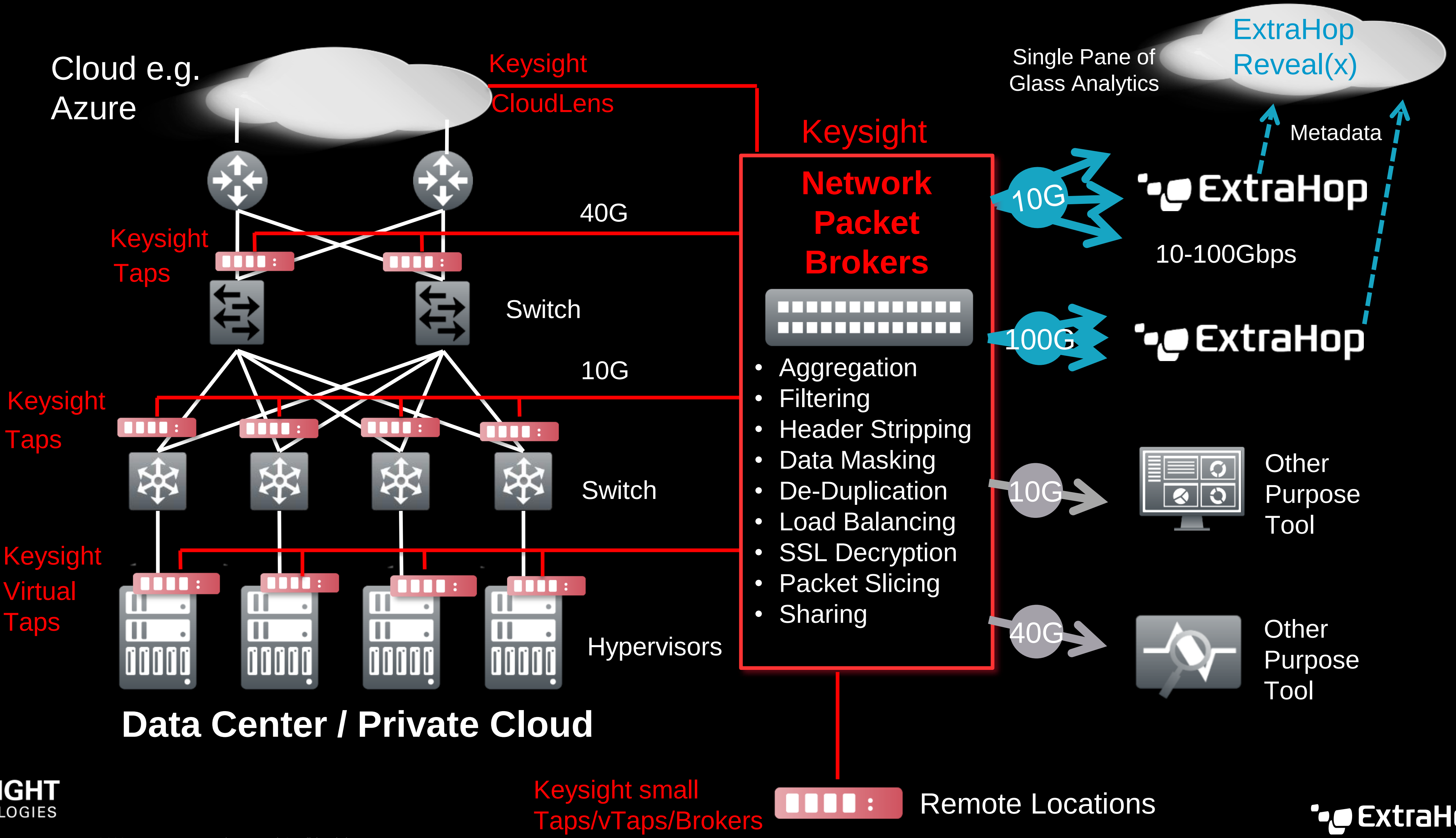
- Network data is the richest data source available for NetOps and SecOps
- Collected Network Data must be reliable and complete
- Data must collected and aggregated before it can be analyzed for security threats
- Grooming to optimize the wire data feed
- Decryption of Traffic (in 2019 87% traffic was encrypted)
- Keysight Visibility Solution complements Extrahop by delivering all the data needed for MITRE analysis

KEYSIGHT TECHNOLOGIES

Keysight Visibility Solution

- Keysight Taps
- Keysight Virtual Taps
- Keysight Network Packet Brokers
- Keysight CloudLens

Keysight Visibility: Single Data Collection Solution for all Network Data

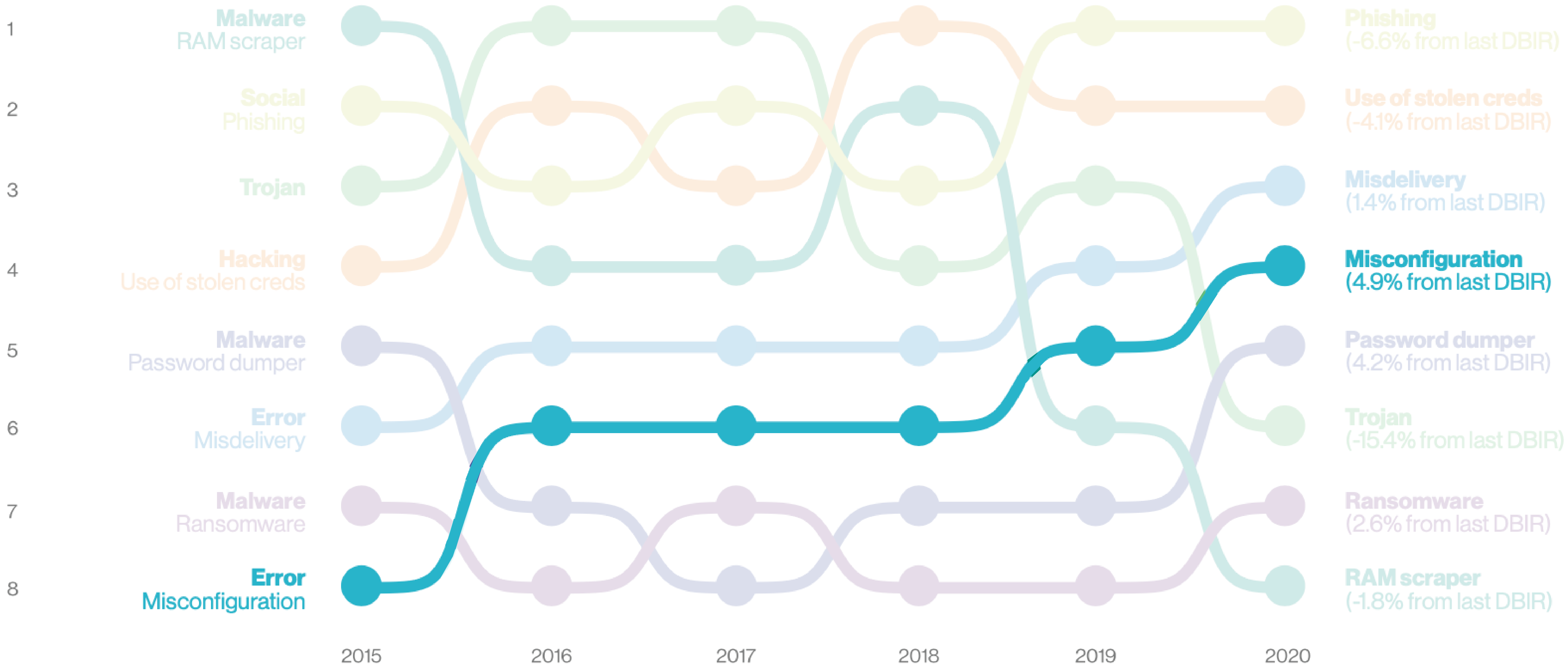


KEYSIGHT TECHNOLOGIES

ExtraHop

Best Practice: Continuous Security Validation

Misconfiguration is another complementary and increasingly important area



**2020 Verizon Data Breach Investigation Report*

Reduce Misconfiguration Risk with Keysight Threat Simulator

AUTOMATED, SAFE, AND CONTINUOUS ASSESSMENT

Improve security by ensuring proper configuration

- Maximize your security tool investment and effectiveness
- Quickly/easily identify misconfigurations and gaps

Easily remediate gaps in your coverage

- Step-by-step instructions for fixes and optimal configuration
- Risk/exposure measurements make it easy to prioritize

Safely simulate the entire kill chain

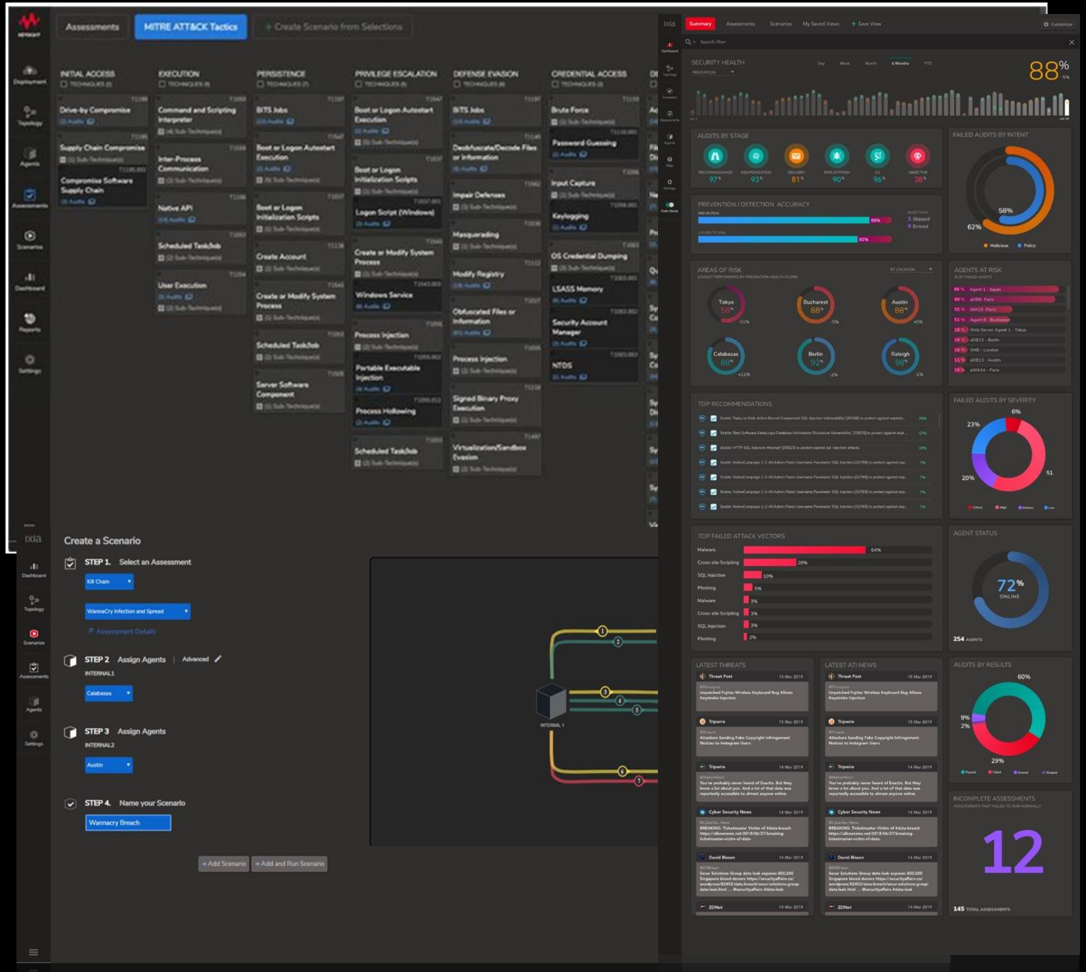
- Real-world malware and techniques e.g. **MITRE ATT&CK**
- e.g. Simulate SUNBURST attack and get recommended fixes.

Assess your detection/blocking capabilities

- Quantify exposure to specific threat vectors
- Seamless SIEM integration

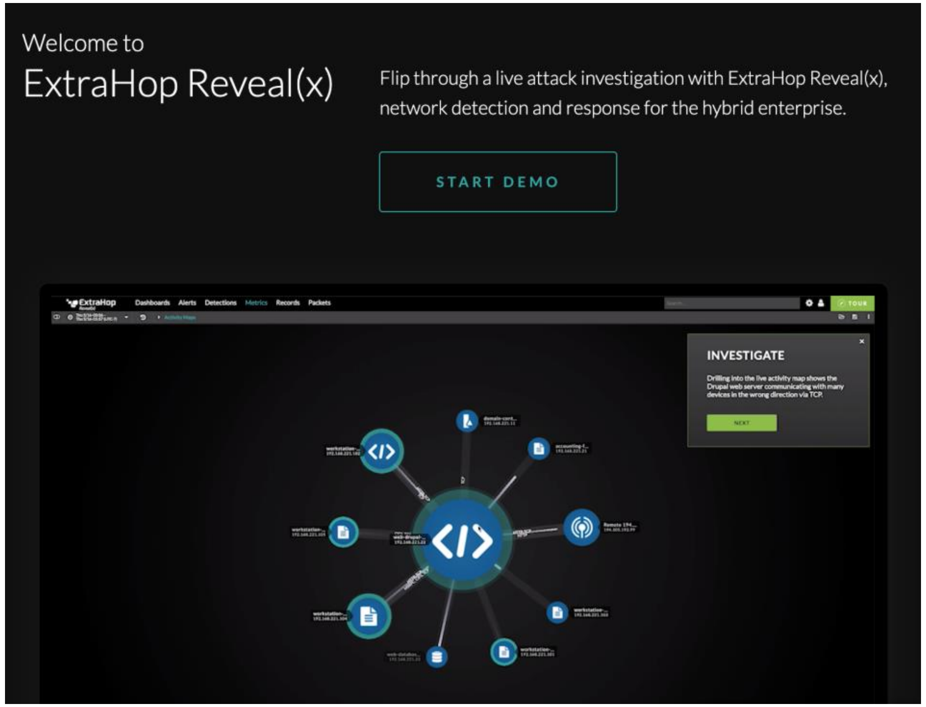
Stay ahead of the curve

- Continually reassess (ex. configuration changes or new threats)



Complements ExtraHop live traffic network detection and response

Next Steps



Welcome to

ExtraHop Reveal(x)

Flip through a live attack investigation with ExtraHop Reveal(x), network detection and response for the hybrid enterprise.

INVESTIGATE

Drilling into the live activity map shows the Drupal web server communicating with many devices in the wrong direction via TCP.

[Try The Online Demo of Reveal(x) 360 Cloud Native NDR]

SOLUTIONS

Network Visibility

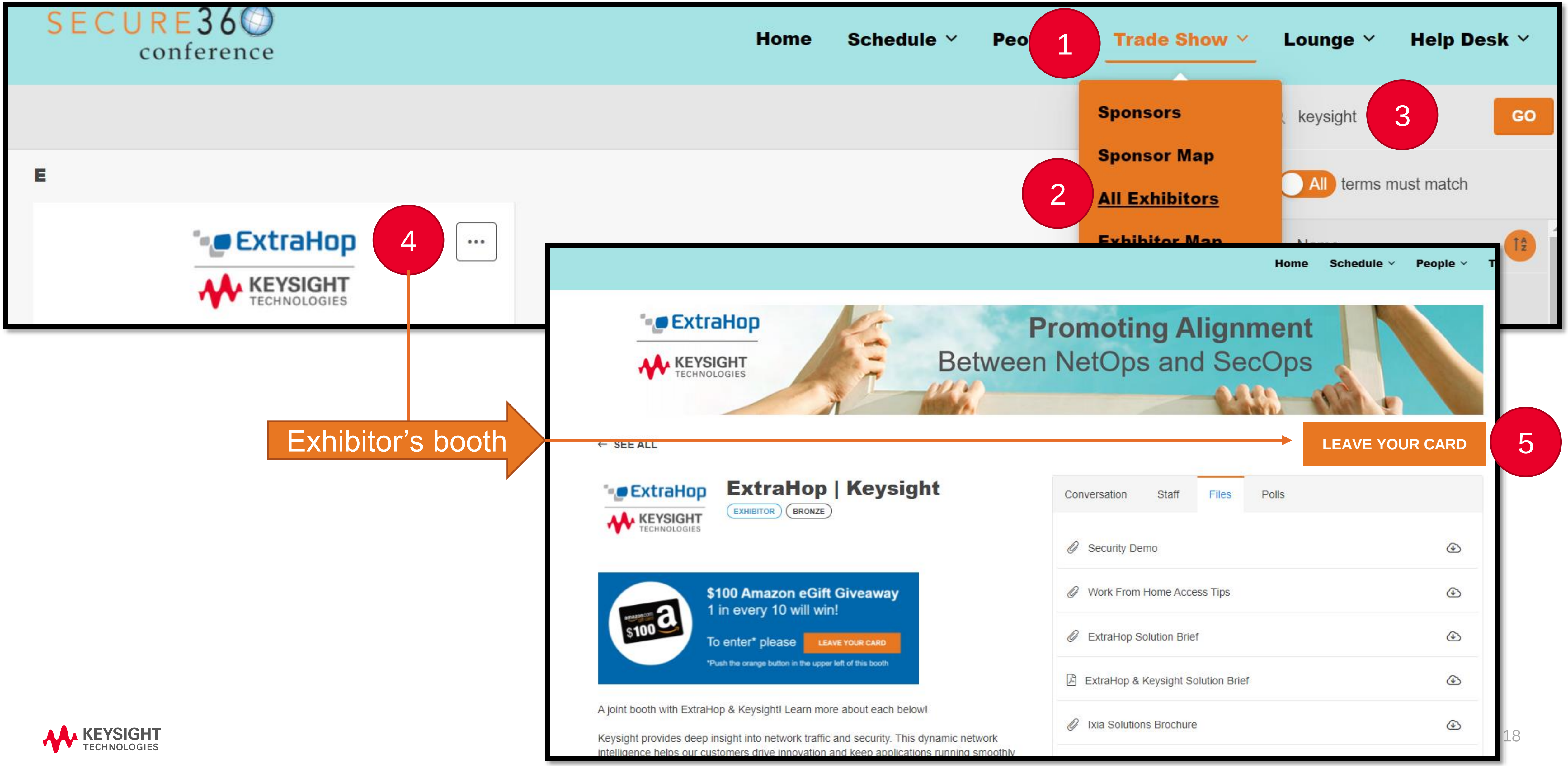
Improve your network security and monitoring insights

[Learn More About Keysight Network Visibility]

Question & Answer

- Please submit your questions via the Q&A chat.
- Leave your business card at our booth if you:
  - Did not get your question answered
  - Want a copy of this presentation
  - Want to enter to win the giveaway

Enter to WIN: Leave your business card at our booth



$100 Amazon eGift Giveaway
1 in every 10 will win!

To enter* please LEAVE YOUR CARD

*Push the orange button in the upper left of this booth

A joint booth with ExtraHop & Keysight! Learn more about each below!

Keysight provides deep insight into network traffic and security. This dynamic network intelligence helps our customers drive innovation and keep applications running smoothly

KEYSIGHT
TECHNOLOGIES