



Trellix

Detecting unknown and Emerging threats

Trellix NDR

Presenter Name

Presenter Title

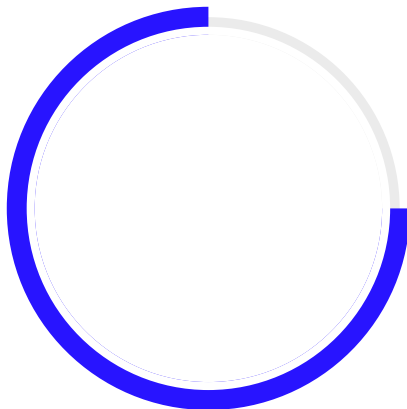
July 2, 2024

Welcome



Mohamed Negm

Solutions Engineer



Tanja Hofmann

Principal Solutions
Engineer



Owen Edwards

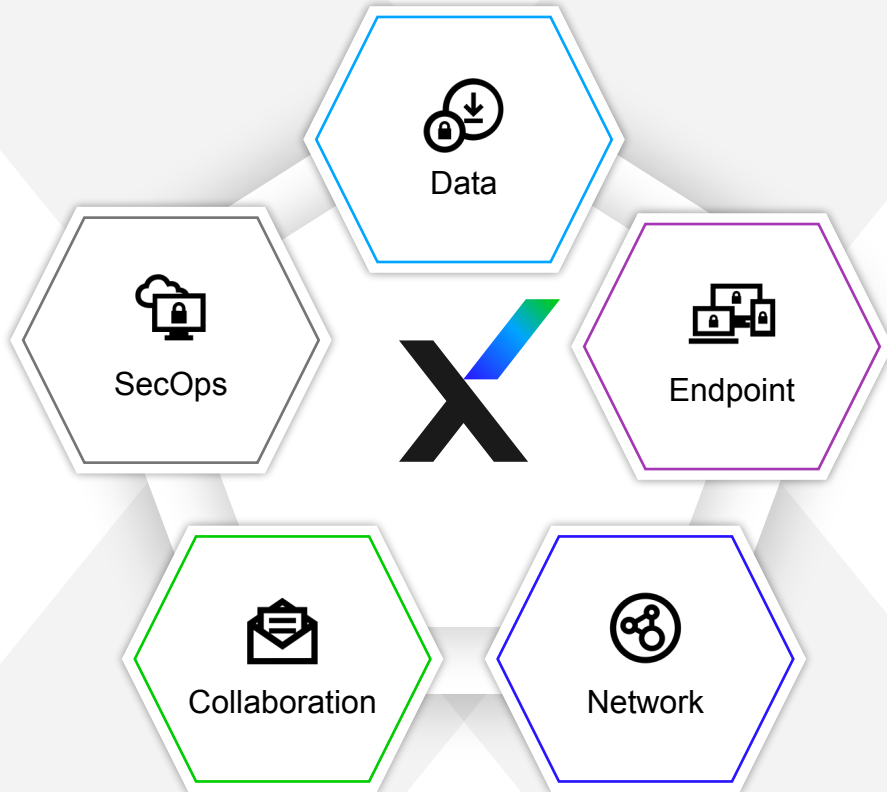
Director, Network Product
Management

Agenda

- NDR Introduction
- Trellix NDR
- NX, PX, IPS
- SOC Workflow
- Architecture
- Roadmap
- UX Research
- Gen-AI
- Use Cases
- Scenarios
- Demo
- Competitive



Trellix Security Platform



Today's Network Challenges

Security Blind Spots

Growing Assets:

133%

Increase in number of assets to protect

Persistent Attackers

Recurring Attacks

43%

Organizations hit by ransomware were hit more than once

Complex Investigations

Ignored Alerts:

35%

Security analysts who say alerts are ignored when the queue is full

69% of organizations reported unknown, poorly managed assets on the network



WHAT IS NDR?

Trellix



“Network detection and response (NDR) products detect abnormal system behaviours by applying behavioural analytics to network traffic data.

They continuously analyse raw network packets or traffic metadata between internal networks (east-west) and public networks (north-south).

NDR products include automated responses, such as host containment or traffic blocking, directly or through integration with other cybersecurity tools.

NDR can be delivered as a combination of hardware and software appliances for sensors, and a management and orchestration console in the form of an on-premises software or SaaS.”

////////////////////

Gartner Research

Applying Network-Centric Approaches for Threat Detection and Response

What is NDR?

NDR evolved out of Network Security

Today's network detection and response (NDR) has a long history, evolving out of network security and network traffic analysis (NTA). The historical definition of network security is to use a perimeter firewall and Intrusion Prevention Systems to screen traffic coming into the network, but as IT and security technology have evolved, the definition is much broader now due to modern attacks leveraging more complex approaches.

Today, network security is everything a company does to ensure the security of its networks, and everything connected to them. This includes the network, the cloud (or clouds), endpoints, servers, IoT, users and applications. Network security products seek to use physical and virtual preventive measures to protect the network and its assets from unauthorized access, modification, destruction and misuse.

What we are hearing

I need to detect emerging threats [MTTD]

I need to correlate (weak) signals across multiple threat vectors

I need to prioritize and investigate threats as quickly as possible to stop attacks before they do damage [MTTR]

I need to understand the scope of the attack, potential business impact etc

I need to proactively hunt for covert activity within my environment

I need to understand the most effective remediation steps

I need to respond confidently / I can't be wrong...

Customer Alternatives



Rely on traditional network security NGFW and IPS



Use a pure play behavioral detection NDR: Extrahop, Vectra, DarkTrace, etc...



Leverage a SIEM for event and log consolidation and correlation



Take advantage of a portfolio provider ELA: Cisco, Fortinet, PAN, etc...



Focus on EDR and XDR for detection and response



TRELLIX NDR

Trellix



The Trellix Approach

Eliminate blind spots

- Not just perimeter - N/S and E/W
- On prem/cloud/hybrid environment visibility
- Asset discovery and monitoring

Disrupt attackers at every stage

- Not just initial compromise
- Multi-layered ML based approach
- Detection of known, unknown, and emerging threats

Speed investigation and response

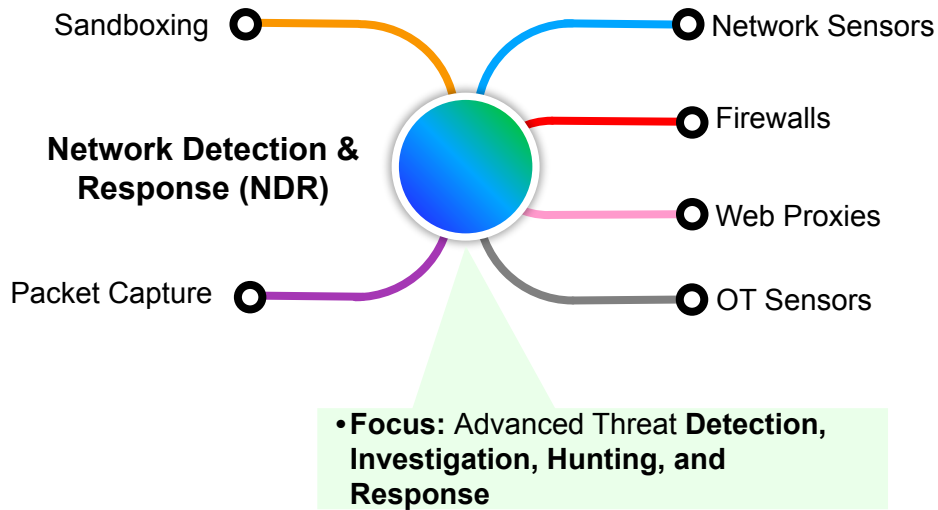
- Alert prioritization and enrichment
- Attack impact scoping
- Guided investigation and workflow
- Network based response



Built on a heritage of innovation in network threat detection and threat intelligence research

Network Detection and Response (NDR)

The Next Evolution In Security For Enterprise Networks



- Modern, Fully-Integrated NDR Architecture
- Reduced Complexity
- Real-Time In-Line Mitigation
- Streamlined Investigations
- Increased Mission Effectiveness
- Reduced Operational Costs

Trellix NDR Platform

High-fidelity, threat-based & AI-supported for effective SOC workflow

Threat Detection

ML/AI, Behavioral Analysis, Triggers & Expert Rules detect emerging threats across the kill chain

Visibility

Device detection, fingerprinting and risk profiling enable target profiling

Investigation

Automated enrichment with threat intel, MITRE techniques, analytics and Trellix WISE speeds investigations

Hunting

Event-based PCAP, L7 metadata, and flow data visibility for hunting, guided through Trellix WISE

Containment & Remediation

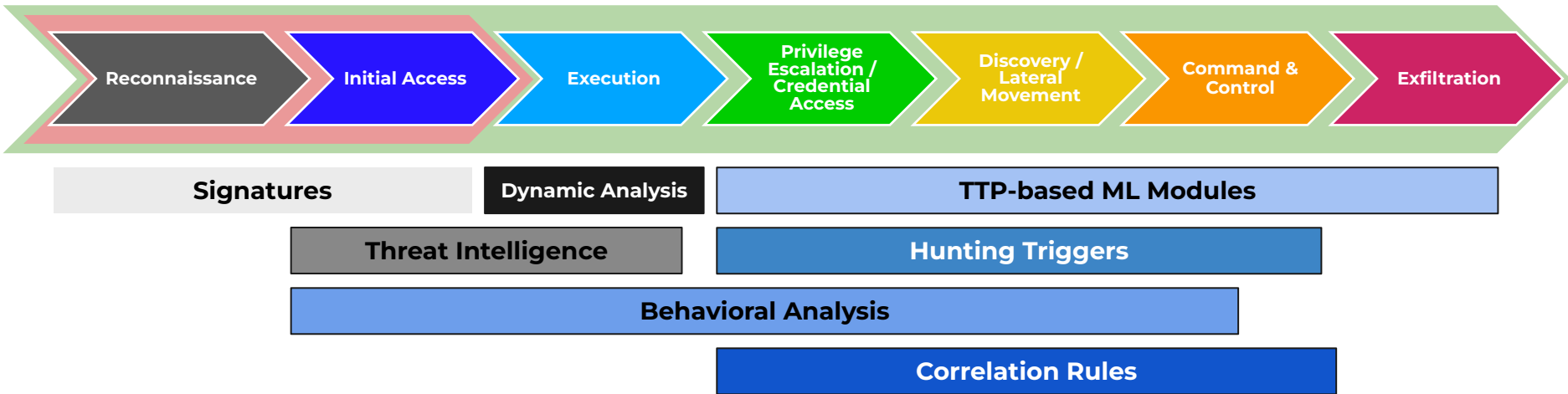
Expedite responses with XDR, SOAR playbooks and ticketing system integrations

Provides visibility and alert priority to respond quickly

NDR: Threat Detection

Traditional Network Perimeter Security

Trellix Network Detection and Response



Leveraging multiple detection and AI approaches

NDR Visibility

VISIBILITY

- Asset discovery
- Asset classification
- SSL / TLS 1.3
- TLC

The screenshot displays the Trellix Network Investigator interface. At the top, the navigation bar includes 'Trelix NETWORK INVESTIGATOR' and various menu items: Dashboard, Search, Alerts, Assets, Cases, Malware Analysis, Health Status, Manage, Tools, and a user profile icon. The current view is 'Assets', with a sub-tab for 'Devices' selected. A 'Show: Last 7 days' filter and a refresh button are visible. Below this, a summary shows '75272 Active Devices' with a breakdown: Mail Server (15), NTP Server (176), Web Server (338), Other (74346), PC (393), and Database (4). A search bar is present above the table. The table lists device details with columns for IP Address, Asset Name, Asset type, OS, Total Events, and Last Active. The first row shows an IP of 198.186.190.61, which is 'Not Available', with 1116 total events and a last active time of 2024-03-11T13:24:48. The table is paginated to show 10 entries.

IP Address	Asset Name	Asset type	OS	Total Events	Last Active
198.186.190.61	Not Available	Mail Server	Linux 2.6.x	1116	2024-03-11T13:24:48
10.14.1.148	Not Available	Mail Server	Not Available	85	2024-03-11T05:25:23
10.14.1.152	Not Available	Mail Server	Not Available	89	2024-03-11T05:25:23
10.14.1.68	Not Available	Mail Server	Not Available	108	2024-03-11T05:25:23
198.186.192.203	Not Available	Mail Server	Not Available	166	2024-03-11T13:25:33
208.87.35.104	Not Available	Mail Server	Not Available	53	2024-03-11T13:21:48
208.91.197.101	Not Available	Mail Server	Not Available	18	2024-03-11T09:24:48
208.91.197.26	Not Available	Mail Server	Not Available	43	2024-03-11T13:23:00
216.8.179.25	Not Available	Mail Server	Not Available	47	2024-03-11T13:23:45
217.12.11.66	Not Available	Mail Server	Not Available	267	2024-03-11T13:21:10

NDR Investigation

INVESTIGATION

- Context-rich detection
- Trellix Threat Intel
- Trellix WISE (Gen AI) (Early Access)

The screenshot displays the Trellix Network Investigator interface. At the top, the search criteria are: SOURCEIPV4ADDRESS: 198.186.190.11 OR DESTINATIONIPV4ADDRESS: 198.186.190.203, with a time range from 09/09/2024 4:21 AM to 08/09/2024 6:21 AM. The interface is currently on the 'FLOW ANALYSIS' tab. Below the search bar, it shows 'First Event: 2024-08-09T05:20:30.000Z', 'Last Event: 2024-08-09T05:34:43.000Z', and 'Total Records: 1713'. A 'Download PCAP' button is visible. The main section is titled 'Top Talkers By Bytes' and includes a 'Generate CSV' link. Below this is a table with the following data:

sourceIPv4Address	sourceTransportPort	destinationIPv4Address	destinationTransportPort	applicationName	Count	Bytes	Packets
198.186.190.12	40345	198.186.190.203	120	Unknown	1	56.20MB	39.74K
198.186.190.12	40352	198.186.190.203	120	Unknown	1	10.82MB	7.69K
198.186.190.105	37853	198.186.190.203	120	Unknown	1	74.09KB	1.44K
198.186.190.243	38431	198.186.190.203	2000	CiscoSkinny	1	43.55KB	0.75K
198.186.190.243	37660	198.186.190.203	2000	CiscoSkinny	1	36.08KB	0.68K
198.186.190.243	38101	198.186.190.203	2000	CiscoSkinny	1	35.84KB	0.61K
198.186.190.193	43232	198.186.190.203	2000	CiscoSkinny	1	34.41KB	0.67K
198.186.190.243	38336	198.186.190.203	2000	CiscoSkinny	1	33.59KB	0.60K
198.186.190.243	38198	198.186.190.203	2000	CiscoSkinny	1	31.48KB	0.58K
198.186.190.105	60533	198.186.190.203	120	Unknown	1	30.07KB	0.53K

At the bottom of the interface, there are two donut charts under the heading 'Protocol Classification'. The left chart shows two segments, one orange and one blue. The right chart shows a similar distribution with orange and blue segments.

NDR Hunting

HUNTING

- Event-based PCAP
- Session reconstruction
- OS change visibility
- Trellix WISE (GenAI) guidance

Reconstruct - 7cffa861-4a92-4bdc-999d-97025584046d

Success! 1 event(s) were analyzed and merged (MD5: 4109dc4e8e482c2f4f5f90b3d55209f1, SHA256: 8daf9509d1d8f20cf192f43cc1a4787601b292d55294a72b150135a3f6e633a).

PACKETS WEB EMAIL ARTIFACTS [Download merged PCAP](#) [Download selected artifacts](#) [Download all artifacts](#) [Store PCAP](#)

Connections

No.	Source	Source Port	Destination	Destination Port	Protocol	PCAP	Stream
0	10.14.65.230	56199	10.14.1.1	53	UDP	Download	Follow

Packets (packet undefined of 0)

Packet Details

- Frame 1: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
- Ethernet II, Src: 00:0c:29:e7:2d:74 (00:0c:29:e7:2d:74), Dst: 00:0c:29:37:94:46 (00:0c:29:37:94:46)
- Internet Protocol Version 4, Src: 10.14.1.1 (10.14.1.1), Dst: 10.14.65.230 (10.14.65.230)
- User Datagram Protocol, Src Port: 53 (53), Dst Port: 56199 (56199)
- Domain Name System (response)

Hex Details

```
00000000 00 0c 29 37 94 46 00 0c 29 e7 2d 74 08 00 45 00 |..)7.F..)-t..E.|
00000010 00 07 3e c4 00 00 3f 11 e5 9f 0a 0e 01 01 0a 0e |.|>..?.....|
00000020 41 e6 00 35 0b 07 00 73 a2 00 1c bd 95 03 00 01 |A.5...5.....|
00000030 00 00 00 01 00 00 04 77 70 61 64 03 61 73 08 06 ||.....mpad.ash.|
00000040 73 65 6c 61 62 73 07 66 69 72 65 65 79 65 03 63 |selabs.fireeye.c|
00000050 6f 6d 00 00 01 00 01 c0 11 00 06 00 01 00 00 01 |om.....|
00000060 00 00 32 0a 6c 61 62 63 6f 6e 73 6f 6c 65 00 0f |..2.labconsole..|
00000070 65 6d 65 61 2d 61 72 63 68 69 74 65 63 74 73 c0 |]emea-architects.|
00000080 1c 55 3e 1e 95 00 00 00 3c 00 00 00 24 00 00 07 |.U.....<...$.|
00000090 08 00 00 01 00 00 |.....|
```

NDR Response

RESPONSE ACTIONS

- Indicator Exchange
- CEF/SysLog event notification

The screenshot displays the Trellix Network Investigator interface. The top navigation bar includes 'Trellix', 'NETWORK INVESTIGATOR', and 'NDR EDITOR'. The main content area is divided into two panels. The left panel, titled 'Logic settings', contains two conditions. Condition 1 is a red box with the text 'The condition at top matches first condition and then terminate'. It has a sub-section 'Add conditions to the path' with the instruction 'If (Path executes only if this condition is satisfied)'. Below this are two 'AND' blocks, each containing two 'Fileproperties/size' fields with the value '1024'. Condition 2 is a yellow box with the text 'Add a name to the condition.' and a sub-section 'Add a name to the condition.' with the instruction 'Enter condition name : Default: Condition 2'. It also contains two 'AND' blocks, each with two 'Fileproperties/size' fields and the value '1024'. A 'Submit' button is at the bottom right of the logic settings panel. The right panel shows a flowchart with several nodes. The top node is 'Trellix Email Quarantine the device'. Below it is a green box labeled 'Conditon Name'. An 'Else' branch leads to another 'Trellix Email Quarantine the device' node. Below that is a blue box with a search icon. This box has two branches: 'Conditon 1' leading to a 'Transform Code for running the...' node, and 'Conditon 2' leading to a 'Trellix Email Create ticket' node. An 'Else' branch from the search icon node leads to a 'Trellix Email Quarantine the device' node. The bottom of the flowchart shows three nodes: a green box labeled '1 Name', a red box labeled 'Else', and a red box labeled '1 Name'. The bottom right corner of the interface shows 'LOCAL: 2024-08-21 16:48:39' and 'UTC: 2024-08-21 15:48:39'. The footer contains '© 2023 Trellix' and three footer links: 'Footer Link 1', 'Footer Link 2', and 'Footer Link 3'.

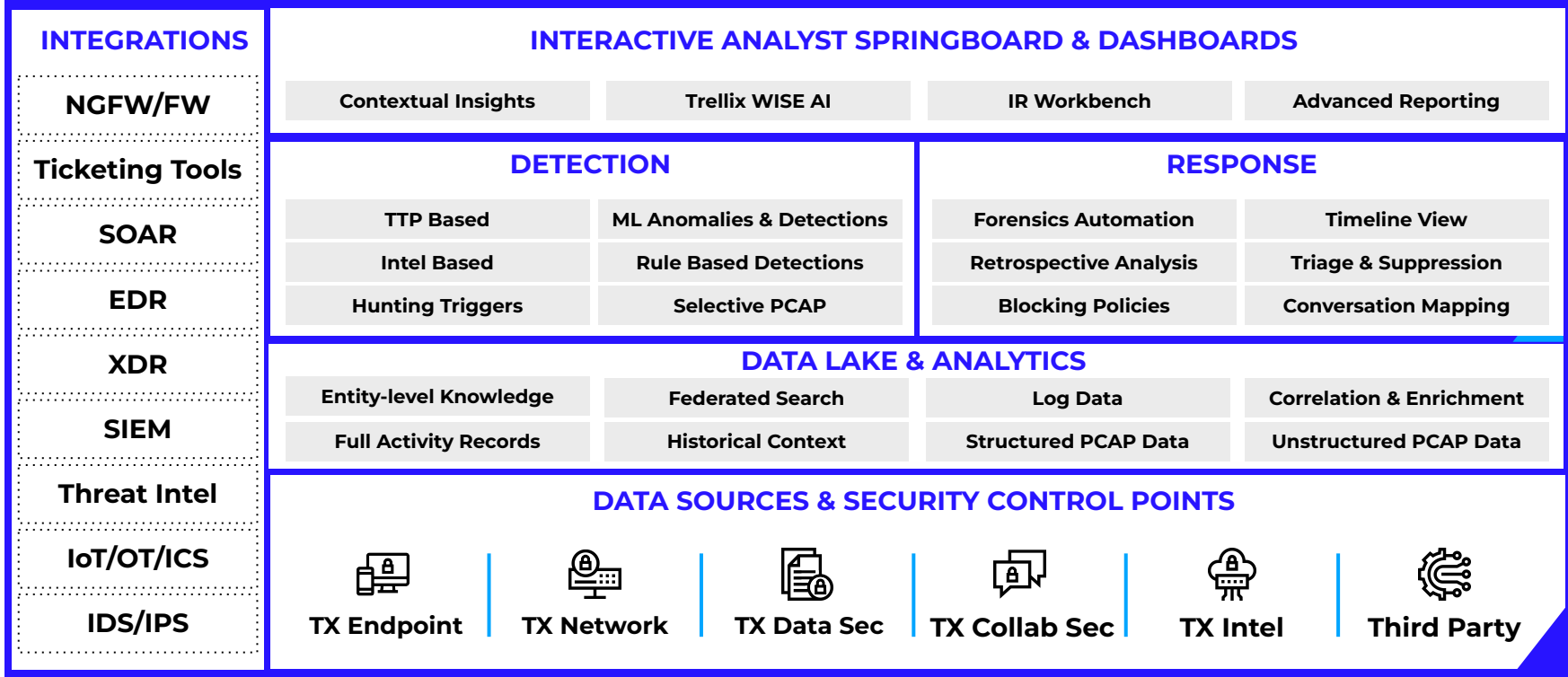


Architecture

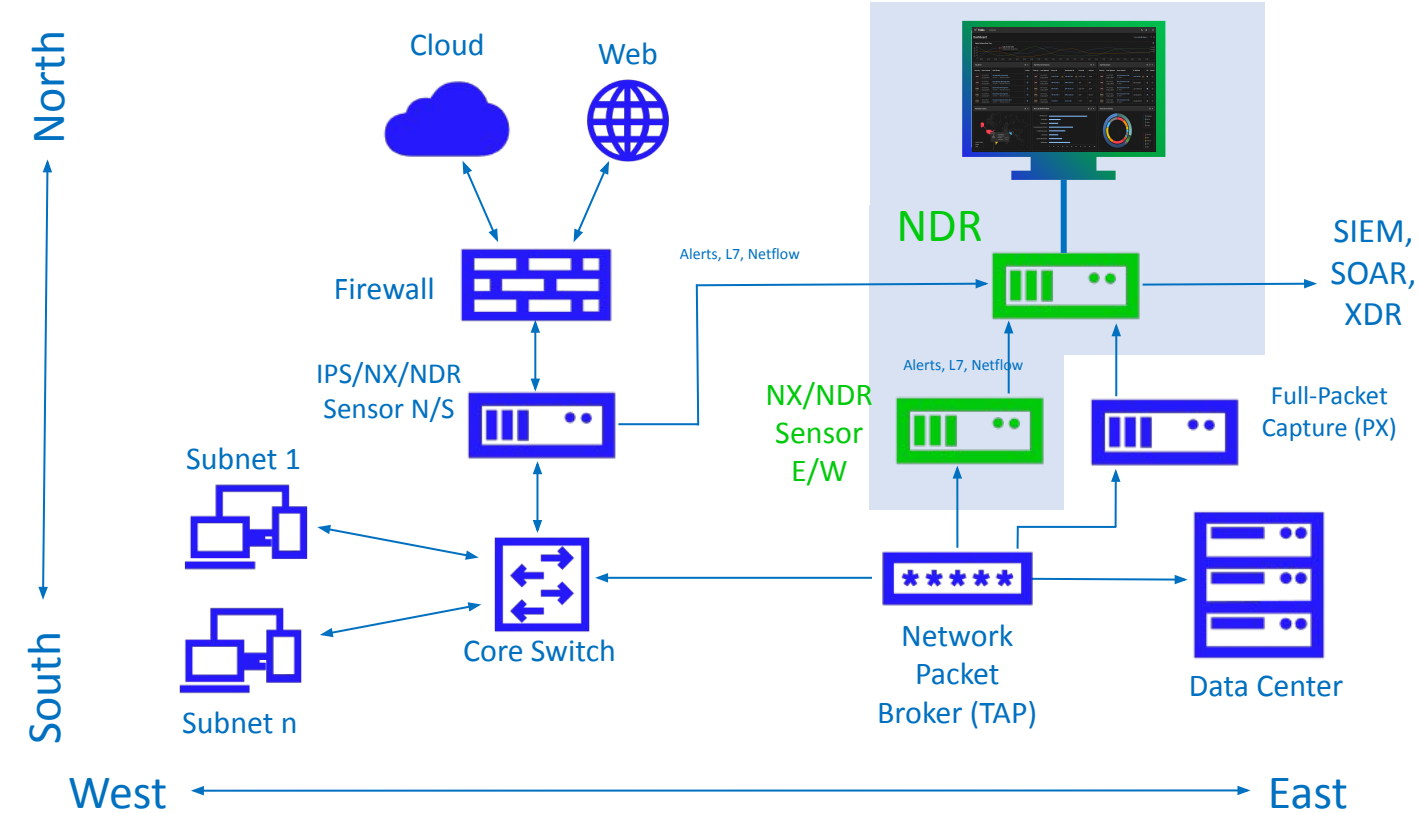
Trellix



Trellix NDR



NDR Architecture



- NDR Module / Console
 - Asset Discovery
 - ML Detections
 - Investigation
 - Hunting
 - Response
- NDR Sensor (HW, Virtual, Cloud)
- In-line / Passive Inspection
- N/S & E/W
- Full Packet Capture (with PX)
- IPS "NDR Ready"

Trellix NDR Sensors

Trellix Network Detection & Response (NDR) Platform

Trellix NDR Sensor (NX)

- NDR Focus
- HW, Virtual, Cloud
- Active NDR
- TLS Onboard
- Event generation & tagging
- Enhanced MITRE Detection
- Targeted PCAP
- Scaling to 40 Gbps

Trellix IPS "NDR Ready"

- Workload Protection Focus
- HW, Virtual, Cloud
- Full IPS
- Active NDR
- TLS Onboard (4Q)
- Event generation & tagging
- Scaling to 240 Gbps

Third Party

- Skyhigh SWG
- Firewall / Proxies
- OT Sensors

Multi-layered visibility, detection, investigation and response



TRELLIX NX

Trellix



Network Security (NX)

Detect the Undetectable



INTELLIGENCE DRIVEN

Infused intelligence with advanced technologies



SMARTVISION

Detect suspicious lateral network traffic and data exfiltration



MULTI-OS SUPPORT

Stop threats that target Windows, Linux, and OS X

Make Investments More Efficient



HIGH FIDELITY ALERTS

Low false positives to target alerts that matter



FLEXIBILITY

Scalable from 50Mbps to over 20 Gbps+ in multiple form factors



ORCHESTRATION

Pivot to Network Forensics or Helix Platform to automate tasks

Gain Additive Protection via Trellix Global Footprint



DYNAMIC THREAT INTEL

Automated protection gained from threats detected worldwide



BREACH EXPERTISE

Applied intelligence gained from the frontline



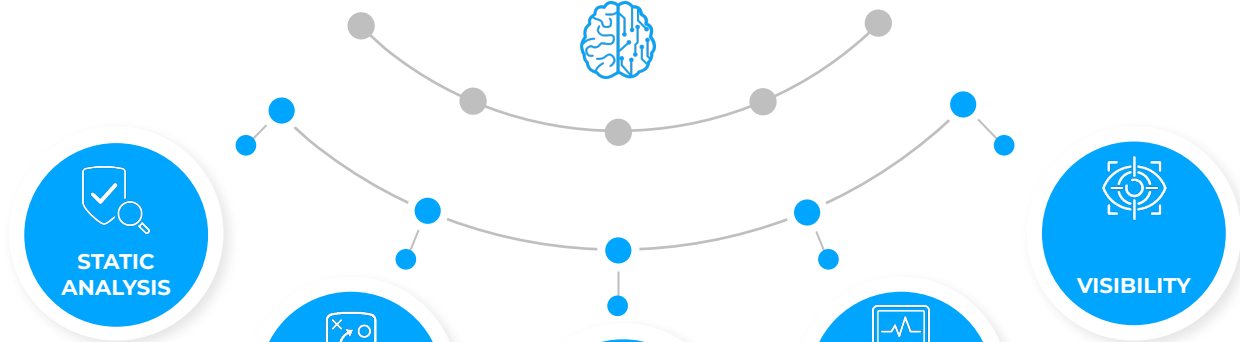
ATTACKER INSIGHT

Deep insight of attacker tactics, techniques, and procedures

Network Security – Detection & Protection Engines

DYNAMIC THREAT INTELLIGENCE

Content Updates – Signatures/ Threat Feeds
Cloud Assist – Cache for File & URL Analysis
Cloud Assist – File Sandboxing & Analysis



STATIC ANALYSIS

IPS
Proprietary/Custom Signatures (Snort, YARA)
Static Network Rules/Blacklists
Antivirus + Malware Guard

DYNAMIC ANALYSIS

Multi-Flow Analysis
Web Shell Detections
Server-Based Vulnerabilities
URL-based Phishing Attacks (Cloud-Assisted)
Malware Binaries Check (Cloud-Assisted)

FILE

Multi-Vector Execution (MVX)
Web Infection
Riskware
Callback Detection

ANALYTICS & MACHINE LEARNING

Analytics Rules
Lateral Movement
Data Exfiltration
Beacon Detection
Malicious C2 Communications

VISIBILITY

Protocol Application and Visibility
Metadata Generation
IoT Visibility
TLS/JA3 Fingerprinting
Endpoint Correlation



TRELLIX NETWORK FORENSICS

Trellix



Network Forensics



High-Performance Packet Capture

LOSSLESS PACKET CAPTURE

Vital to effective network forensic investigations

HIGH-PERFORMANCE

Record speeds of up to 20 Gbps

INTELLIGENT CAPTURE

Selective packet filtering for maximum efficiency



High-Fidelity Data Analysis

ULTRAFAST SEARCH

Leverage unique indexing architecture for fast answers

INTEGRATED INTELLIGENCE

Add rich context to IOCs and alerts

EASY DRILL DOWN

Quickly respond to alerts that matter



Grows with Your Network

EXTENSIVE VISIBILITY

Session decoder support for a myriad of protocols and file types

FLEXIBLE PLATFORM

Scales to meet distributed and large enterprise needs

THREAT HUNTING

Perform retrospective threat hunting and analysis



TRELLIX IPS

Trellix



Intrusion Prevention System (IPS)

Powerful Protection with Deep Packet Inspection

- Prevents initial incursion
- Prevents DoS, DDoS, C&C traffic and exfiltration
- Provides virtual patching preventing vulnerability exploit

High performance visibility

- 100% SSL visibility
- L7 Visibility and Analytics
- 100 Gbps throughput for high load north-south network traffic

Superior Architecture

- 300 Gbps throughput for high load north-south network traffic
- Multiple failover and HA deployment model
- Secure private, public and hybrid clouds



Reports via
network sensors
to centralized
console



Searches for
malicious activity
with a deep
network-packet
inspection

Trellix
IPS



Scans variety of
file types as they
travel across
the network



IPS - Signature + Signature-Less Technology

Signature Based DPI



User-defined, custom, Snort Signatures

STIX Allow list/block list

Threat Reputation



TIE / Global Threat Intelligence (GTI)

File, IP, and URL reputation

Deep File Analysis



Non-signature heuristic-based analysis

Adobe PDF, Flash, JavaScript, MS Office files inspection

Real-time Emulation



Gateway Anti-Malware Browser (GAM) Emulation

Viruses, worms, adware, spyware, riskware detection

Botnet Detection



0-day Botnet and malware callback protection

Protocol anomalies, port and stealth scans



Safe Harbor Statement

This slide deck may include roadmap information, projections or other information that might be considered forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ.



Trellix NDR Roadmap

Extending network threat visibility, broadening detections across the kill chain, and reducing the time to respond

Recent

- New dashboards
 - Threats
 - Visibility
 - MITRE ATT&CK
 - Assets
- ML detection porting
- Asset discovery and ID
- Global Threat Intelligence (GTI)
 - file reputation
- Sensor enhancements:
 - High performance appliances & virtual
 - Cloud-native integrations
 - Threat detections - AI & signature

Next

- ML detections
 - DNS tunneling exploits
 - SSL Anomalies (Expired, Weak Cipher, Self Signed)
 - Lateral movement from weak indicators
- Improved alert enrichment and summarization
- Analyst Springboard
 - Risk based aggregation
 - Quick identification of attack type, targets, and attacker
 - Rich context into the attack kill chain with related detections.
 - Drill down to forensic evidence.
- Sensor enhancements:
 - 10 Gbps virtual sensor (ESXi)
- Trellix Wise - actionable insights, summaries, and workflows

Exploring

- Guided SOC workflows
- Integrations:
 - ePO, HX, XDR
 - Chronicle
 - Nozomi Guardian
- ML detections
 - Behavioral anomalies
 - Traffic similar to known Malicious traffic (unblocked)
 - Newly registered domains
 - ToR Activity
- Visibility enhancements
- Sensor enhancements
 - 100 Gbps NDR sensor
 - OS Migration
 - IPv6-only network

NDR Asset Discovery

EXPLORING

Endpoint Integration

- Trellix ePO
- MS Defender

OT Sensor Integration

Risk Profiling

Attack Path Profiling

Trellix | Dashboard → Asset List

Asset List

Show: Last 24 Hours

Filter

Assets: All

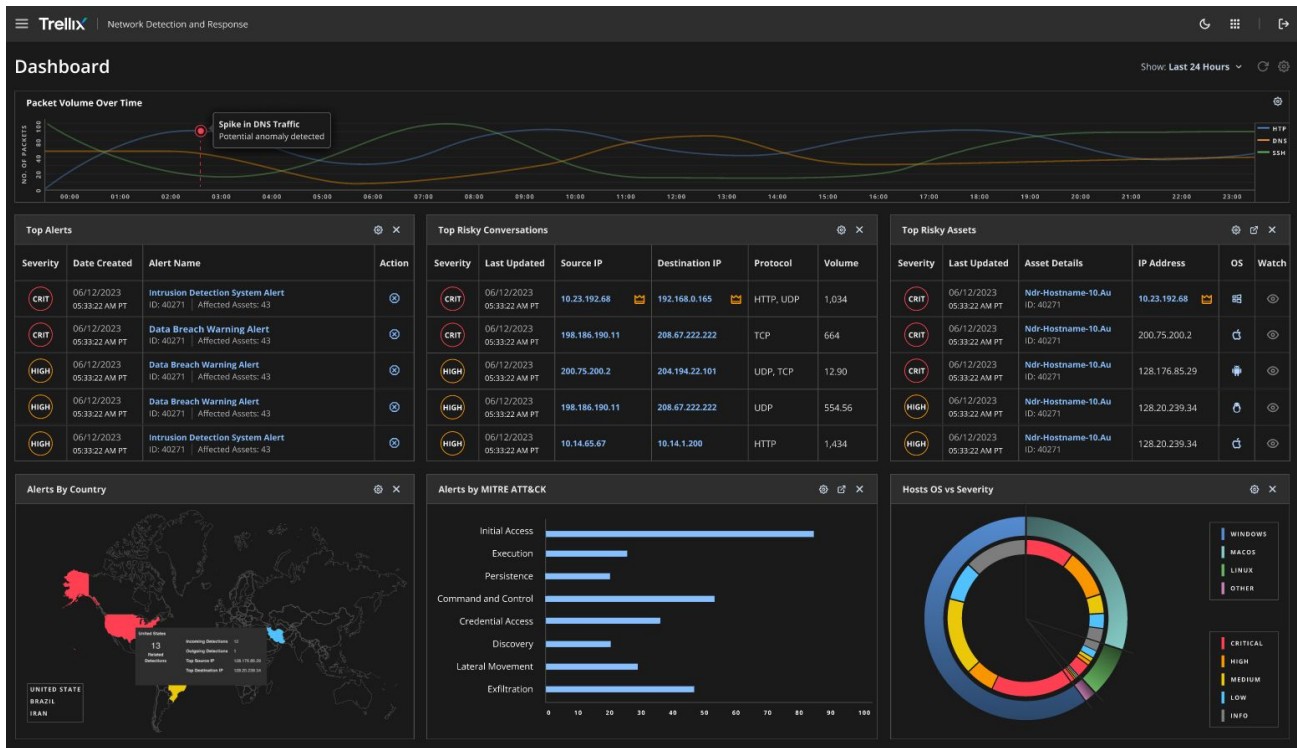
Showing 4 out of 13, results | Updated 5 min ago

<input type="checkbox"/>	Severity	Last Updated	Asset name	Asset Type	IP Address	OS	Total Event	
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	WS	443	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	WS	124	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Local-Hostname-10.Au ID: 40271	Server	204.194.22.101	WS	443	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	WS	124	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	WS	443	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Local-Hostname-10.Au ID: 40271	Server	204.194.22.101	WS	443	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	WS	443	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	WS	124	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Local-Hostname-10.Au ID: 40271	Server	204.194.22.101	WS	443	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	WS	443	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	WS	124	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	WS	443	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	WS	124	⋮
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	WS	124	⋮

NDR Investigation

EXPLORING

- Analyst “Springboard”
- Attack scoping from detection to root cause in a few clicks
- Endpoint Process integration
- Intel Graph



NDR Investigation

EXPLORING

- Analyst "Springboard"
- Attack scoping from detection to root cause in a few clicks
- Endpoint Process integration
- Intel Graph

The screenshot displays the Trellix NDR interface for an asset named 'LT-BCLINE-01 [PC]'. The interface is divided into several panels:

- Asset Details:** Shows IP address (10.23.192.68), operating system (Windows 10 Build 18363.476), location (London, UK), current active user (local/Administrator), and user history (3 users in last 7 days). It also shows 1,923 events and 105GB of network traffic.
- Timeline:** A horizontal timeline from 00:00 to 23:00 showing various events marked with colored icons.
- Alerts:** A table of alerts with columns for Occurrences, Latest Occurrence, First Occurrence, and Alert MITRE TTP. The primary alert is 'Connections to Abnormal Destination IPs' (CRIT), which occurred 5 times on 2020/12/12 at 03:45 PM. A secondary alert is 'Intrusion Detection System Alert' (HIGH), which occurred 6 times at the same time.
- Conversation Map:** A network diagram showing connections between various IP addresses. The central node is 10.23.192.68 (CRIT). Other nodes include 192.24.221.87 (LOW), 198.186.190.11 (LOW), 192.168.0.165 (CRIT), 182.40.221.17 (HIGH), 192.168.10.85 (LOW), and 182.24.221.56 (HIGH). Arrows indicate the direction of traffic, with labels like 'HTTP 41986' and 'HTTP 41986'.
- Events:** A table of network activity with columns for Date, Source IP, Destination IP, and Protocol. The event shown is a 'Beaconing Event' (HIGH) on 2020/12/12 at 03:45 PM, with source IP 10.23.192.68 and destination IP 192.168.0.165 over HTTP.

NDR Hunting

EXPLORING

- Single click reconstruction
- Hunting triggers
- Asset and Alert rule builder
- Selective packet capture

The screenshot displays the Trellix Network Detection and Response (NDR) interface. At the top, the 'Asset Details' section shows information for 'LT-BCLINE-01 [PC]' (Domain Controller) with IP address 10.23.192.68, running Windows 10 Build 18363.476, located in London, UK. The current active user is local/Administrator, and there have been 3 users in the last 7 days. The last 24 hours show 1,923 events and 105GB of network traffic.

The main area shows a 'Reconstruct' window for a specific event. A success message states: 'Success! 1 event(s) were analyzed and merged (MD5: 16ce495c746a327f5966c17db9624fb, SHA256: 1f20b49541b7d50ec1d0ce05cc22de2d02c24f1eece05f4c071413d7aea2d4c)'. Below this, there are tabs for 'PACKETS', 'WEB', 'EMAIL', and 'ARTIFACTS'. Action buttons include 'Download merged PCAP', 'Download selected artifacts', 'Download all artifacts', and 'Store PCAP'.

The 'Connections' table shows a single connection:

No.	Source	Source Port	Destination	Destination Port	Protocol	PCAP	Stream
0	128.176.85.29	55134	128.20.239.34	80	TCP	Download	Follow

The 'Packets' table shows several packets:

No.	Direction	Time	Source	Destination	Protocol
002	←	09/26/2024 09:10:45.109	128.20.239.34	128.176.85.29	HTTP
004	→	09/26/2024 09:10:45.115	128.176.85.29	128.20.239.34	HTTP
006	←	09/26/2024 09:10:45.409	128.20.239.34	128.176.85.29	HTTP
008	←	09/26/2024 09:10:45.409	128.20.239.34	128.176.85.29	HTTP
010	←	09/26/2024 09:10:45.409	128.20.239.34	128.176.85.29	HTTP
012	←	09/26/2024 09:10:45.409	128.20.239.34	128.176.85.29	HTTP

The 'Packet Details' section shows the following information:

- Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: 00:50:56:01:3b:33 (00:50:56:01:3b:33), Dst: 00:00:0c:9f:f8:0a (00:00:0c:9f:f8:0a)
- Internet Protocol Version 4, Src: 128.176.85.29 (128.176.85.29), Dst: 128.20.239.34 (128.20.239.34)
- Transmission Control Protocol, Src Port: 55134 (55134), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0

NDR Response

EXPLORING

- Automated action via integrations with Splunk, and more.
- No-code Orchestration & Response

The screenshot displays the Trellix Network Investigator interface. The top navigation bar includes 'Trellix', 'NETWORK INVESTIGATOR', 'NDR EDITOR', 'Response', and 'Edit Playbook'. The main area is divided into two panels. The left panel, titled 'Logic settings', contains two conditions. Condition 1 is a red box with the text 'The condition at top matches first condition and then terminate'. It has a sub-section 'Add conditions to the path' with the instruction 'If (Path executes only if this condition is satisfied)'. Below this are two 'AND' condition blocks, each containing two 'Fileproperties/size' fields with the value '1024'. Condition 2 is a yellow box with the same text and structure. At the bottom of the logic settings panel are an 'Add Condition' button and a checkbox for 'Else (Make it an escape route)'. The right panel shows a flowchart with several steps: a 'Trellix Email Quarantine the device' step, followed by an 'Else' branch leading to another 'Trellix Email Quarantine the device' step. Below this is a decision diamond with two paths: 'Condition 1' leading to a 'Transform Code for running the...' step, and 'Condition 2' leading to a 'Trellix Email Create ticket' step. An 'Else' path from the diamond leads to a third 'Trellix Email Quarantine the device' step. The flowchart also includes various control elements like a 'Name' field, a '75%' zoom indicator, and a 'Submit' button at the bottom right.

© 2023 Trellix

Footer Link 1 Footer Link 2 Footer Link 3



UX Research

Trellix

Trellix

Gen-AI with Trellix NDR

Detecting unknown and Emerging
threats



What is Trellix Wise

Trellix Wise relieves alert fatigue for security operations, enabling teams of any experience level to investigate 100% of their alerts and automate investigation and remediation. Trellix Wise makes decisions, offers guidance, and uses conversational AI so users can hunt threats while learning on the job



See everything
that matters



Make better,
faster decisions



Upskill and close
talent gaps

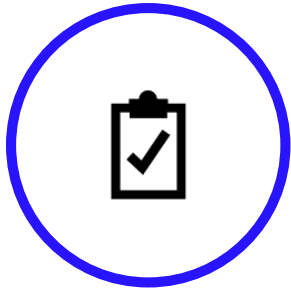


Prove value
rapidly

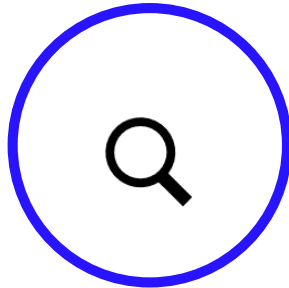
Why Trellix Wise

Gen-AI for your biggest security operations challenges

End alert fatigue



Make the right decisions, faster



Close security talent gaps



Prove ROI rapidly



Trellix Wise alerts Enrichment

		2024-09-22T04:59:02 Z	NX	smartvision-event
--	--	--------------------------	----	-------------------

smartvision-event

September 22nd 2024, 4:59:02 AM

Assets Details Attack Details JSON Intel Trellix Wise New

**Generated by AI, verify for accuracy*

[Summarize this alert](#) [Top affected entities](#) [MITRE findings](#) [Evidence](#)

[Remediation steps](#) [Knowledge graph](#)

[Sequence diagram](#) [Know more](#)

▼ Summarize this alert

Summary:

The alert indicates an "AnomalousUser-AgentIdentified" event, where a CertUtil URL Agent was detected accessing a URL on the host "me.pcsdl.com" from the source IP 10.14.10.70. This event is mapped to the MITRE ATT&CK technique T1071.001 (Application Layer Protocol: Web Protocols), which is associated with Command and Control activities. The most important event is the HTTP GET request to the URL "/short-uri-v2/000375404074/scenario/encfile__e3a64b37-4398-4132-b1a0-fb9ee8f8e1e3.txt" on the host "me.pcsdl.com" from the source IP 10.14.10.70. The investigation should start by analyzing the network traffic and the host activities related to this event. Suspicious events include the use of the "CertUtil URL Agent" user-agent, which is often associated with malicious activities, and the access to a potentially suspicious URL. The alert was first detected on the host with IP 10.14.10.70.

Key Points:

- The most suspicious process name is "CertUtil URL Agent", which is often associated with malicious activities.
- The events are related to a HTTP GET request from the source IP 10.14.10.70 to the URL "/short-uri-v2/000375404074/scenario/encfile__e3a64b37-4398-4132-b1a0-fb9ee8f8e1e3.txt" on the host "me.pcsdl.com".
- The use of the "CertUtil URL Agent" user-agent and the access to a potentially suspicious URL are the main suspicious and misinterpreted benign actions implied by the events.
- The alert was first detected on the host with IP 10.14.10.70, which should be the focus of the investigation.
- The MITRE ATT&CK mapping to T1071.001 (Application Layer Protocol: Web Protocols) suggests that this event is related to Command and Control activities, which should be further investigated.

Trellix Wise alerts Enrichment

smartvision-event
September 22nd 2024, 4:59:02 AM

Assets Details Attack Details JSON Intel Trellix Wise New

**Generated by AI, verify for accuracy*

Evidence

Summarize this alert Top affected entities MITRE findings

Remediation steps Knowledge graph

Sequence diagram Know more

Remediation steps

Based on the provided information, the following remediation steps can be taken:

- Investigate the suspicious HTTP request to the domain "me.pcsdl.com" with the user-agent "CertUtil URL Agent". This could indicate potential malicious activity, such as command and control communication.
- Review the network traffic and logs to identify any other similar suspicious activities or connections to the same domain or IP address.
- Analyze the HTTP response content and payload to determine if any malicious code or data was downloaded.
- Assess the risk and potential impact of the detected activity, and consider implementing appropriate security controls, such as network monitoring, web filtering, or endpoint protection, to mitigate the identified threats.
- Ensure that the affected system(s) are thoroughly investigated and remediated, if necessary, to prevent further compromise.
- Review and update the organization's security policies, procedures, and employee security awareness training to address the identified threats and prevent similar incidents in the future.

smartvision-event
September 22nd 2024, 4:59:02 AM

Assets Details Attack Details JSON Intel Trellix Wise New

MITRE_ID : T1071.001 - Application Layer Protocol: Web Protocols

Details

The alert indicates that an anomalous user-agent, "CertUtil URL Agent", was identified in an HTTP GET request to the domain "me.pcsdl.com". This behavior is mapped to the MITRE ATT&CK technique T1071.001 - Application Layer Protocol: Web Protocols, which is part of the Command and Control tactic.

The observed actions indicate that the user-agent "CertUtil URL Agent" was used to retrieve a file from the remote server, which could be an attempt to establish command and control communication. The use of an uncommon user-agent and the retrieval of a file from a potentially suspicious domain suggest that this activity may be part of a larger malicious campaign.

Adversary Insights:

- The use of an uncommon user-agent, "CertUtil URL Agent", suggests the adversary is attempting to bypass security controls and blend in with legitimate traffic.
- The retrieval of a file from a potentially suspicious domain, "me.pcsdl.com", indicates the adversary may be attempting to download additional malware or receive instructions from a command and control server.

Observed Actions:

- HTTP GET request to "me.pcsdl.com" with the user-agent "CertUtil URL Agent"
- Retrieval of a file from the remote server with the URL "/short-uri/v2/000375404074/scenario/encfile___e3a64b37-4398-4132-b1a0-fb9ee8be1e3.txt"

Related Tactics:

- Command and Control: The adversary may be using web protocols to establish command and control communication with a remote server.

Procedures Include:

- Use of uncommon user-agents to blend in with legitimate traffic
- Retrieval of files from potentially suspicious domains
- Establishment of command and control communication over web protocols
- Potential download of additional malware or receipt of instructions from a remote server

Trellix Wise alerts Enrichment

smartvision-event
September 22nd 2024, 4:59:02 AM

Assets Details Attack Details JSON Intel Trellix Wise New

**Generated by AI, verify for accuracy*

Summarize this alert Top affected entities MITRE findings
Remediation steps Knowledge graph
Sequence diagram Know more

▼ Sequence diagram

**Scroll on graph to zoom and drag to pan*

10.14.10.70 62.223.36.245 CertUtil.url-agent CertUtil.url-agent

Access http://[redacted] GET http://[redacted] HTTP 300.30

MITRE T1021.001 - Application Layer Protocol: Web Services

smartvision-event
September 22nd 2024, 4:59:02 AM

Assets Details Attack Details JSON Intel Trellix Wise New

**Generated by AI, verify for accuracy*

Summarize this alert Top affected entities MITRE findings
Remediation steps Knowledge graph
Sequence diagram Know more

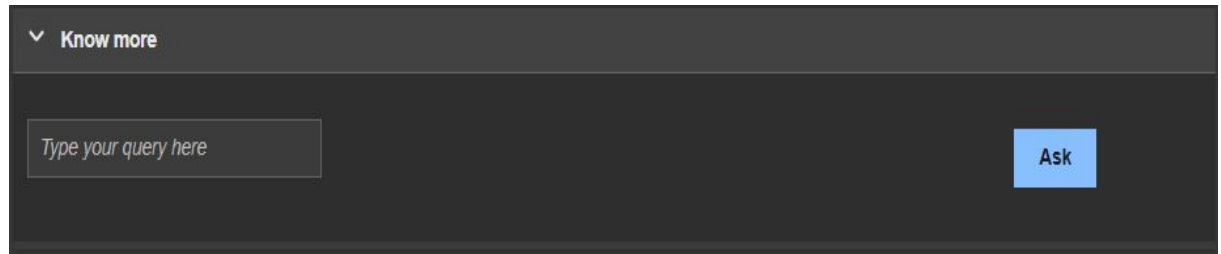
▼ Top affected entities

The top affected entities based on the provided information are:

1. Source IP Address: 10.14.10.70
2. Destination IP Address: 62.223.36.245
3. Destination Port: 80
4. HTTP User-Agent: CertUtil URL_Agent
5. HTTP URL: /short-uri-v2/000375404074/scenario/encfile__e3a64b37-4398-4132-b1a0-fb9ee0f8e1e3.txt

Trellix Wise Efficiency Improvement

Trellix Wise represents a paradigm shift in how SOCs approach data security and incident response. By leveraging GenAI and the power of the Trellix Platform, Trellix Wise streamlines the process of detecting, investigating, and responding to threats. It enables security teams to focus on high-level, human-centric activities while allowing machines to handle the repetitive, time-consuming tasks. With Trellix Wise, organizations can enhance their data security posture, improve operational efficiency, and stay ahead of evolving cyber threats



▼ Know more

Type your query here

Ask

Trellix

NDR Use Cases

Detecting unknown and Emerging threats



Use Case: Ransomware

Before Scenario

Organizations often face challenges in early detection and disruption of ransomware attacks, lacking the ability to identify and understand the sophisticated tactics, techniques, and procedures (TTPs) used in various stages of the attack lifecycle.

Negative Consequences

- The inability to detect and disrupt ransomware attacks at an early stage can lead to encryption or exfiltration of critical data, operational downtime, and significant financial losses.
- Recovery efforts can be costly and time-consuming, severely impacting business continuity and reputation.

Trellix Solutions

- Trellix NDR disrupts ransomware attacks by leveraging multi-layered detection aligned with the MITRE ATT&CK framework, enhancing threat detection efficacy across the cyber kill chain.
- Trellix identifies known, unknown, and emerging threats, including preventing initial compromise credential dumping, lateral movement thereby significantly reducing the risk of any ransomware damage.

Use Case: Investigation and Hunting

Before Scenario

Security teams often struggle to quickly identify and evaluate alerts, facing a deluge of potential threats with limited to zero context, making it challenging to triage, investigate, and respond effectively.

Negative Consequences

- Organizations face increased risk of significant breaches due to delayed response times.
- Analysts waste valuable time on false positives, while real threats linger undetected, potentially causing extensive damage to business operations and reputation.

Trellix Solutions

- Trellix's NDR solution streamlines the investigation and response process through automated alert enrichment and guided SOC workflows, enabling faster, more efficient responses.
- Trellix reduces investigation complexity and accelerates threat hunting and forensic analysis.

Use Case: Adding Value to EDR

Before Scenario

Organizations relying solely on Endpoint Detection and Response (EDR) face visibility limitations, missing unmanaged devices connecting to the network, critical network-level threat activities and interactions between endpoints across cloud, hybrid, and on-premises environments, thus hindering comprehensive threat detection.

Negative Consequences

- Relying exclusively on EDR without enhanced network visibility can leave enterprises vulnerable to sophisticated attacks that bypass endpoint security measures, or ignore attacker use of legitimate tools.
- This oversight can lead to unnoticed threat proliferation, risking data breaches and operational disruptions due to undetected network-level threats.

Trellix Solutions

- Trellix NDR amplifies EDR capabilities by providing extended network visibility, effectively eliminating blind spots, speeding up investigations and helping determine intent behind endpoint activity
- Trellix ensures a more holistic approach to threat detection and response, enhancing overall security posture.

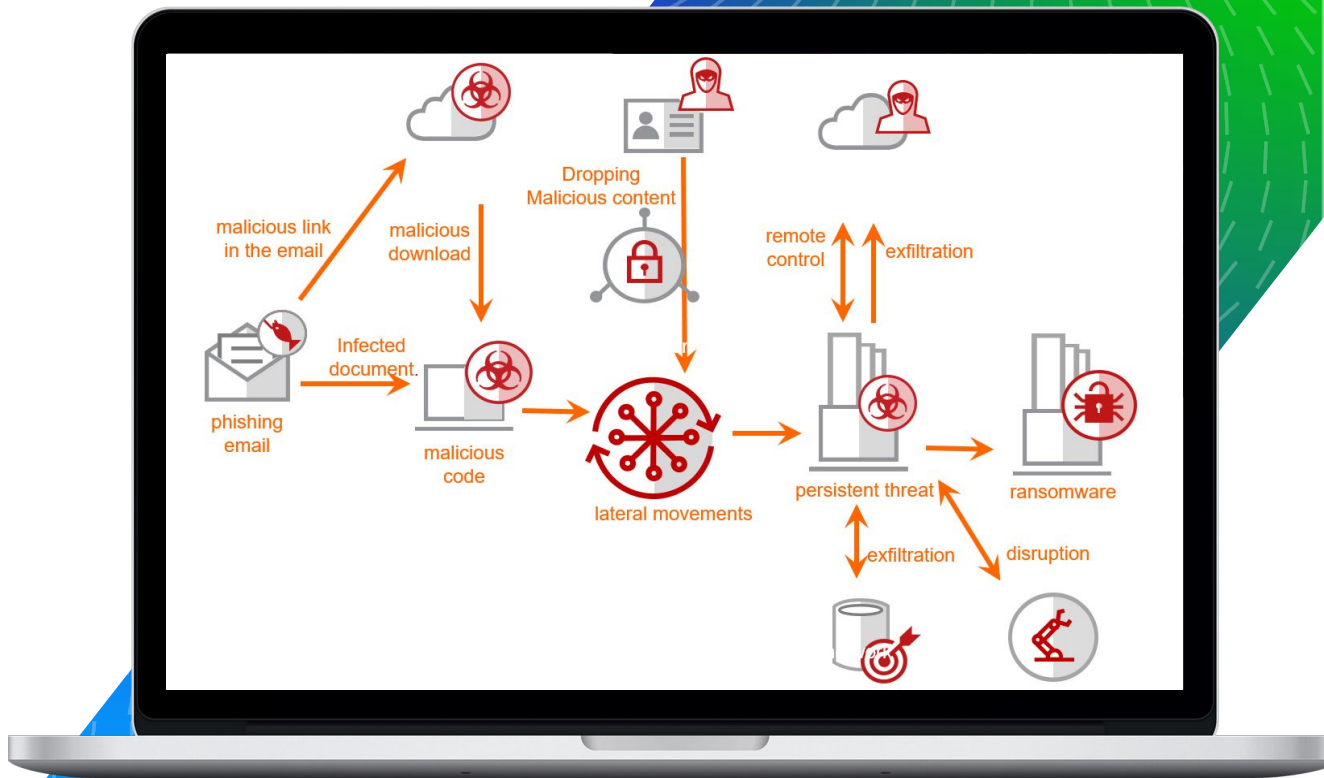
Trellix

NDR Scenario

Detecting unknown and Emerging threats



Anatomy of an attack



Anatomy of an Attack

Initial Access (malicious link through Email)

```
Received: from access.ash.selabs.fireeye.com (unknown [10.14.1.2])
    by ex02.ash.selabs.fireeye.com (Postfix) with ESMTP id 4XQdwQ314LzhXjt
    for <admin@bcc.ash.selabs.fireeye.com>; Sat, 12 Oct 2024 11:48:22 +0200 (EET)
Received: from ash.selabs.fireeye.com (ubuntu-master [10.14.1.1])
    by access.ash.selabs.fireeye.com (Postfix) with ESMTPS id 54F01A0009
    for <mohamedgamal.negm@ash.selabs.fireeye.com>; Sat, 12 Oct 2024 09:48:22 +0000 (UTC)
Date: Sat, 12 Oct 2024 09:48:22 +0000
X-Trellix: Malicious URL Found
From: mohamedgamal.negm@ash.selabs.fireeye.com
Reply-To: mohamedgamal.negm@ash.selabs.fireeye.com
To: mohamedgamal.negm@ash.selabs.fireeye.com
Message-ID: <670a45e64c675_8e52ab9d426498c44429@labconsole.mail>
Subject: Click to Win
Mime-Version: 1.0
Content-Type: text/html;
    charset=UTF-8
Content-Transfer-Encoding: 7bit

Dears

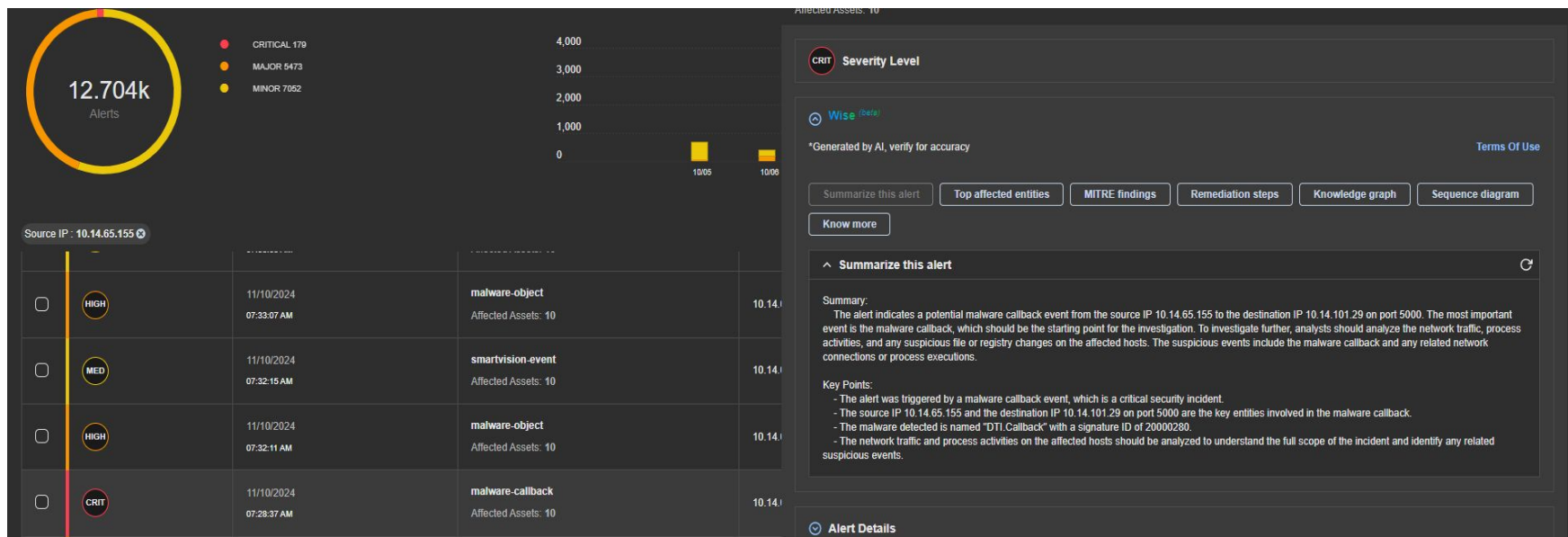
please Click below Link to Win

https://bigfile.mail.naver.com/download?fid=1PK1ax8X14dmK3YwFIY1aAK/HqUmKotwKAgZKA29KoU9HquXKqgdfqKwaxvjaxiSpoUrfXISKAtwMotwKoUXpxbZKzUq|
http://haleassetss.com:5000/m

Regards
Winning
```

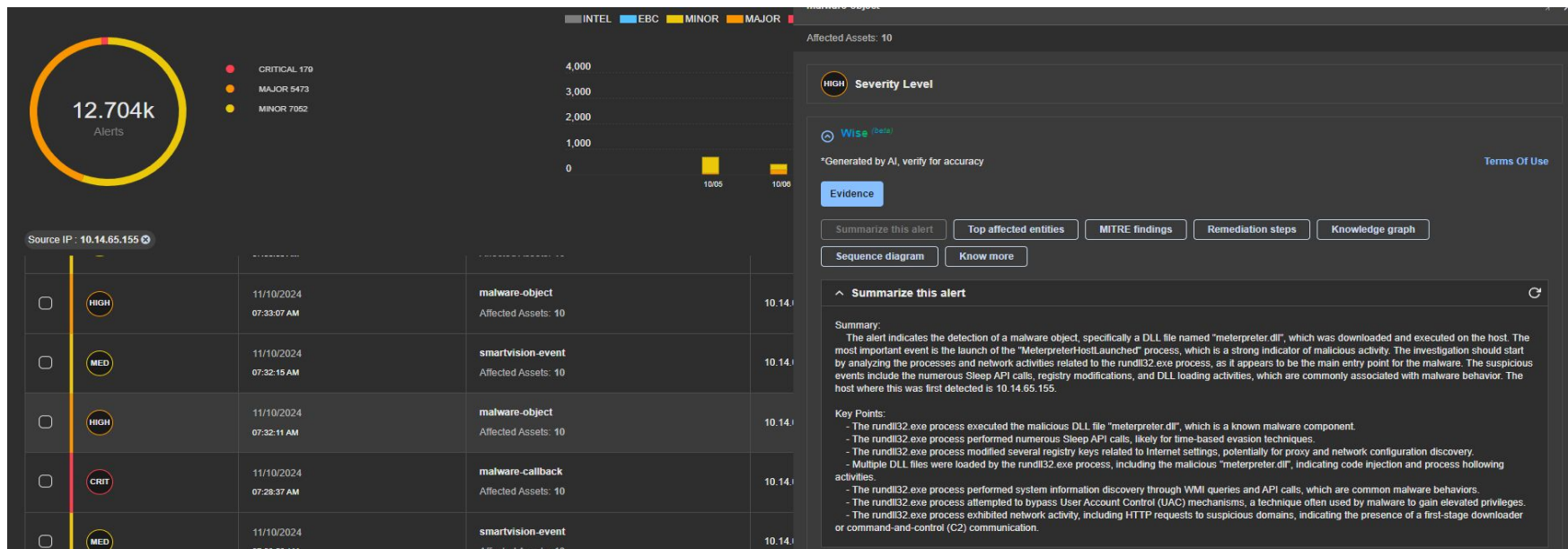
Anatomy of an Attack

Malicious Server Communication



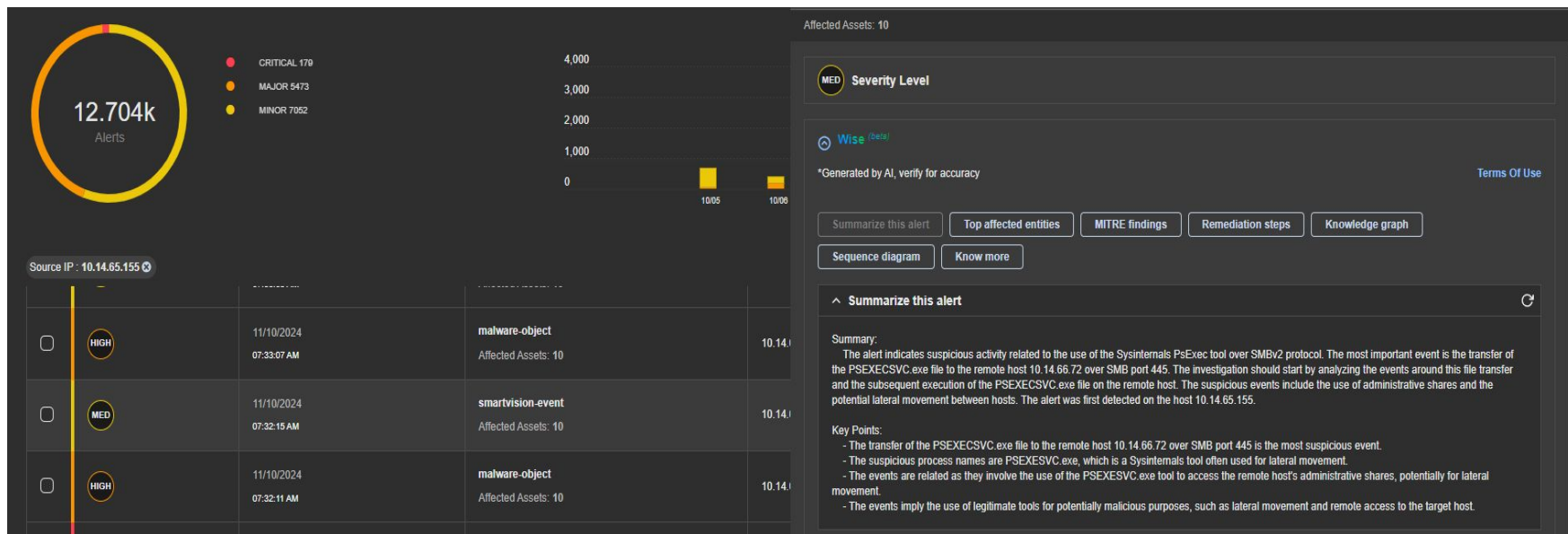
Anatomy of an Attack

Dropping of malicious DLL



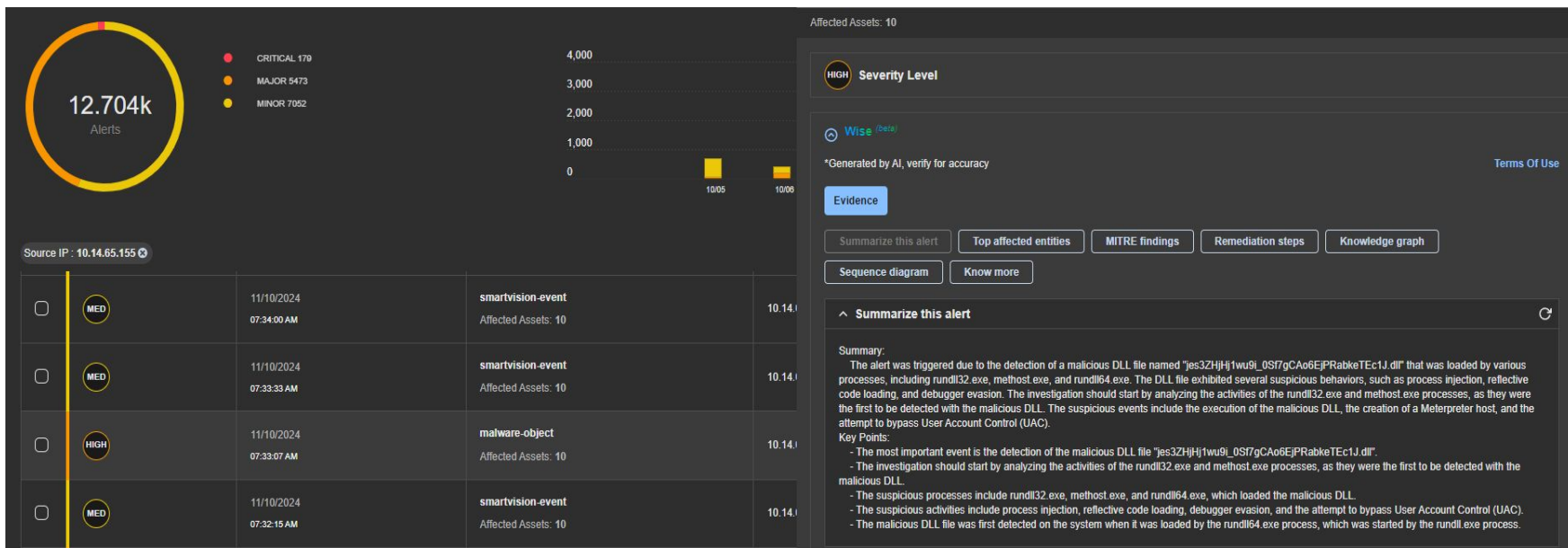
Anatomy of an Attack

Lateral Movement



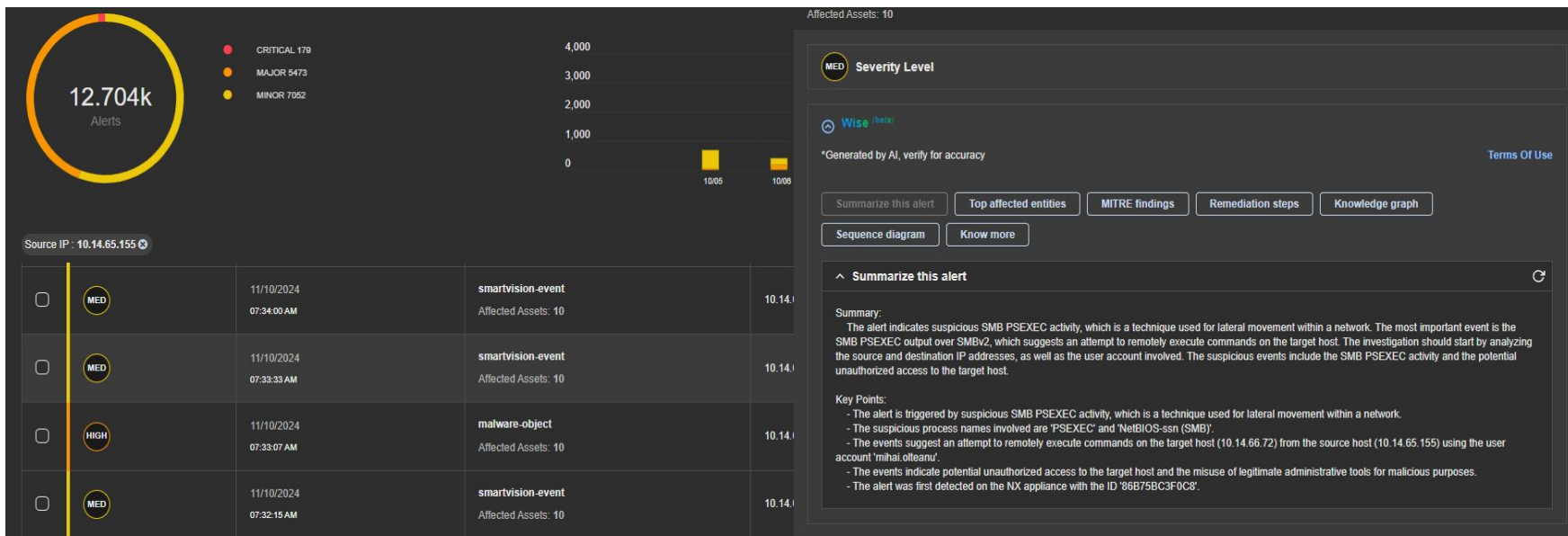
Anatomy of an Attack

Dropping DLL for privilege escalation



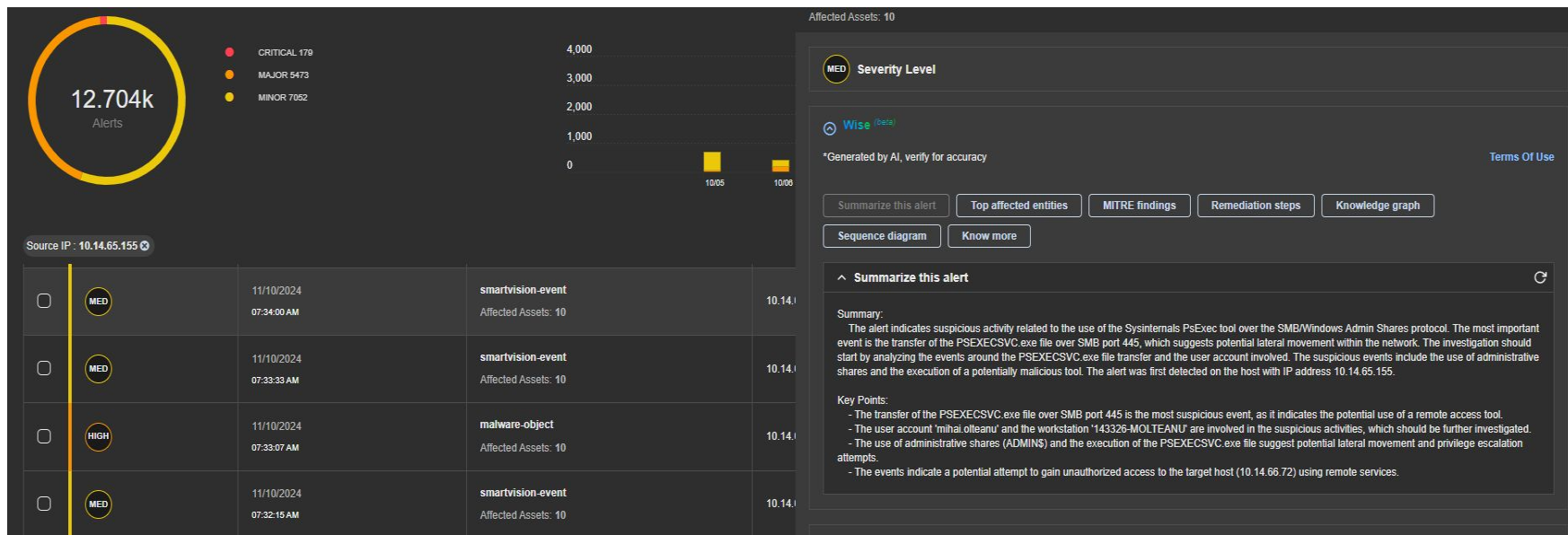
Anatomy of an Attack

Starting spreading Laterally to maintain presence



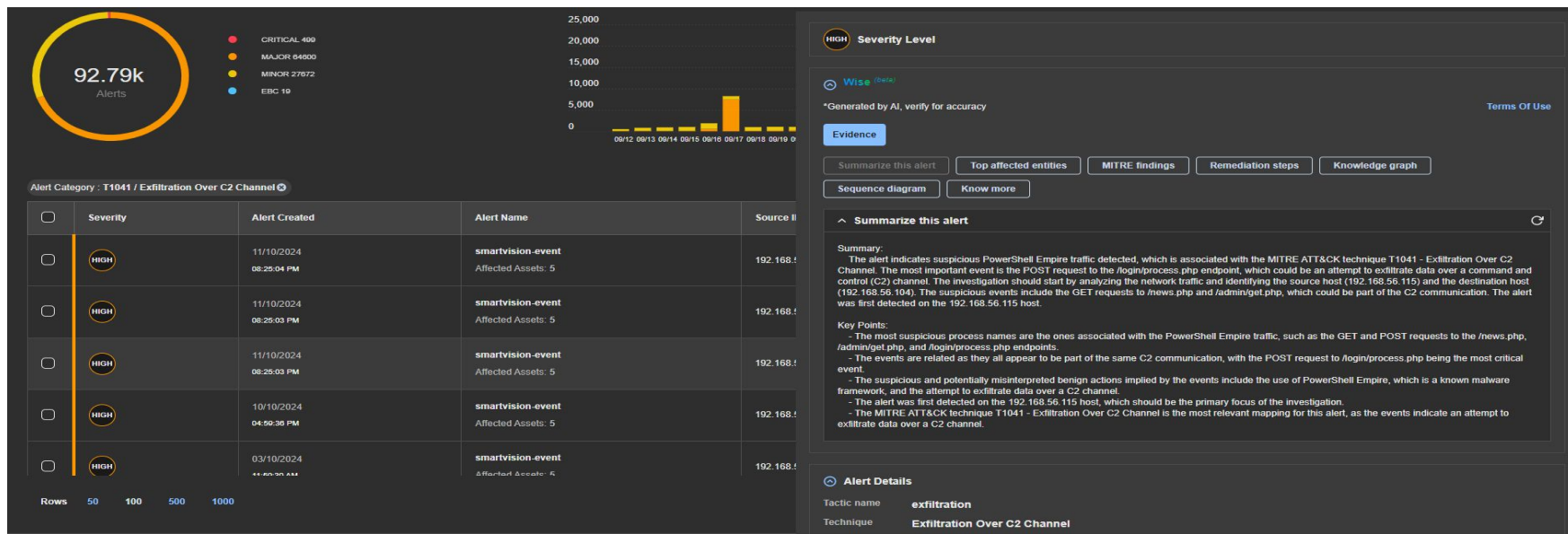
Anatomy of an Attack

Remote Execution

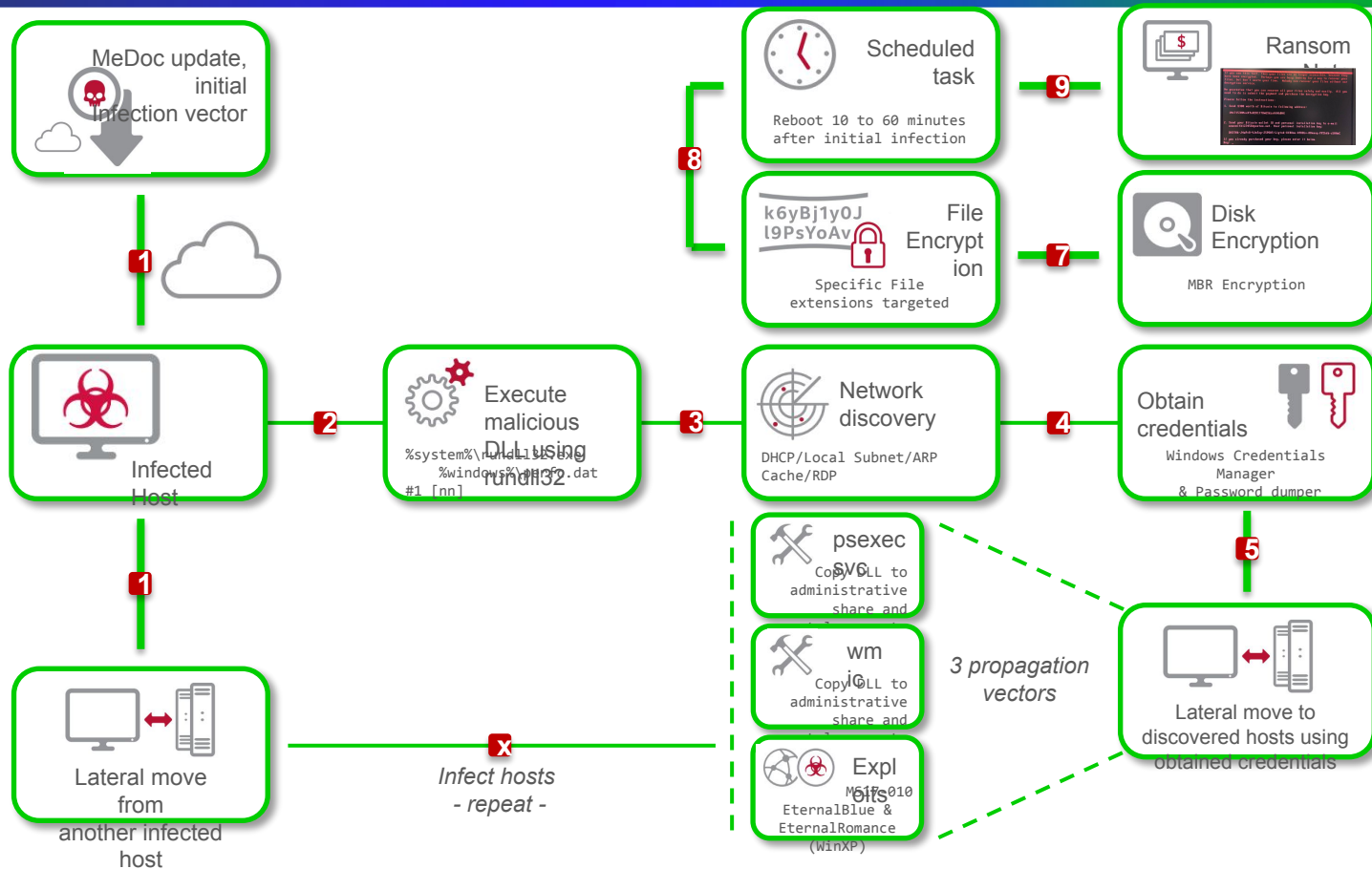


Anatomy of an Attack

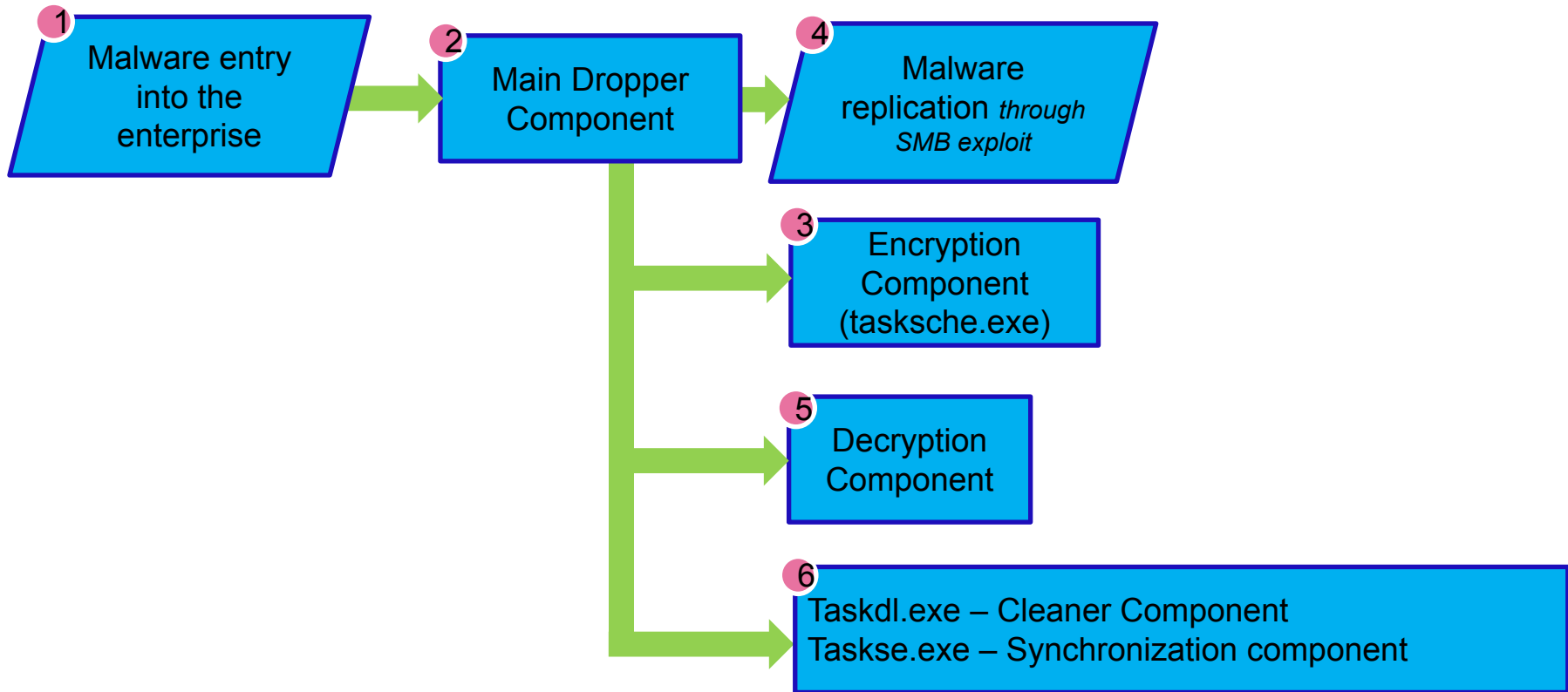
Data Exfiltration



Ransomware: Petya



WannaCry





DEMO

Trellix

Trellix

NDR Competitive Analysis

Detecting unknown and Emerging threats






Competitive Landscape

	Trellix	corelight	DARKTRACE	ExtraHop	VECTRA	
Threat Detection	IDPS Signatures	Yes	Open Source	No	Optional	Vectra Match
	Threat Intelligence Integration	Yes	No	Yes	No	Yes
	Dynamic Analysis Sandbox	Yes	No	No	No	No
	Anomaly Detection – Machine Learning	Yes	Cloud	OnPrem / Cloud	Cloud	Cloud
	Anomaly Detection – Behavioural	Yes	Cloud	Yes	Cloud	Cloud
	Encrypted Traffic Analysis	Yes	Yes	Yes	Yes	Yes
Visibility	IT Asset Discovery	Yes	Yes	Yes	Yes	Limited
	IOT / OT Asset Discovery	Roadmap	Yes	Yes	Yes	No
	SSL Traffic Decryption	Yes	No	No	Yes	No
Investigation	L7 Meta Data	Yes	Yes	Yes	Medium	Vectra Recall
	Netflow Records	Yes	Yes	Yes	Optional	Yes
	Risk Profiling	Roadmap	Yes	Yes	Medium	Yes
	Guided Investigation Workflow	Yes	Splunk	Medium	Yes	Yes
	GenAI Alert Summarisation	Yes	Yes	Yes	Yes	Yes
	MITRE ATT&CK Mapping	Yes	Yes	Yes	Yes	Vectra Recall
Hunting	Session Reconstruction	Yes	No	No	Yes	Vectra Recall
	Selective-packet capture and reconstruction	Roadmap	No	Yes	Yes	No
	Full-packet capture and reconstruction	Yes	3rd Party Tool	No	Yes	No

Competitive Landscape

	Trellix	corelight	DARKTRACE	ExtraHop	VECTRA
Containment & Remediation	In-line inspection	Yes	No	No	No
	Passive inspection				
	Real-time Blocking	Yes	Yes	Yes	Yes
	SOC Tool Integration	Yes	No	No	No
	Endpoint Integration	Yes	Yes	Yes	Yes
	On-prem, Cloud				
Deployment	Physical, Virtual	Roadmap	Falcon	Yes	Yes
	Security Expertise	Yes	Yes	Yes	Yes
	Professional Services	Yes	Yes	Yes	Yes
Support		Yes	Relies on open source	Weak	Yes
		Yes	3rd Party	No	Yes

Competitive Landscape

Key Competitor Overview	Trellix Strengths	Watch for	Countermeasure
 <ul style="list-style-type: none"> + Recognition with analysts + Flexible deployment + Visibility and Detection modules - Lacking threat intelligence and proven high-fidelity detections - Requires 3rd-party for XDR 	<ul style="list-style-type: none"> * Fast time to value with high-fidelity detections and actionable alerts from IPS, NX, and IVX. * Trellix ML models based on global threat intelligence incl. over 14 mil endpoints, email telemetry, and XDR * Trellix is a strategic security vendor for initiatives like XDR with coverage for endpoint, email, SecOps, and data. 	<p>As a pure play NDR vendor, ExtraHop is typically on an analyst shortlist as a strong solution. Varying modules appeal to network operations and SOC teams.</p>	<p>ExtraHop lacks comparable threat intelligence and highly proven high-fidelity detections that Trellix can offer. As NDR is increasingly adopted towards XDR efforts, customers with strategic XDR initiatives would better require a strategic security vendor for those initiatives like Trellix; as with pure play NDR vendors like ExtraHop, customers would require 3rd-party partnerships that would come with their own integration complexities.</p>
 <ul style="list-style-type: none"> + Graphical UI + AI Messaging Claims - Relies on AI, - high false positives, - poor detection 	<ul style="list-style-type: none"> * Fast time to value with high-fidelity detections and actionable alerts from IPS, NX, and IVX. * Trellix ML models based on global threat intelligence incl. over 14 mil endpoints, email telemetry, and XDR * Trellix is a strategic security vendor for initiatives like XDR with coverage for endpoint, email, SecOps, and data. 	<p>Darktrace leverages the AI buzzword frequently within their messaging as much of their value relies on AI.</p>	<p>Overly relying on AI results in high false positives and poor detection altogether - requiring customers to struggle with excessive fine-tuning. Conversely, with Trellix, customers won't have to worry about constant fine-tuning thanks to our high value, high-fidelity solutions.</p>
 <ul style="list-style-type: none"> + AI Messaging Claims + Flexible Deployment - Lacking threat intelligence and dynamic analysis capability - High effort to train/tune ML models 	<ul style="list-style-type: none"> * Fast time to value with high-fidelity detections and actionable alerts from IPS, NX, and IVX. * Trellix ML models based on global threat intelligence incl. over 14 mil endpoints, email telemetry, and XDR * Trellix is a strategic security vendor for initiatives like XDR with coverage for endpoint, email, SecOps, and data. 	<p>Akin to Darktrace, Vectra AI also focuses on AI messaging claims while leveraging their flexible deployment options that may appeal to a wider variety of customers.</p>	<p>Vectra AI lacks the integrated threat intelligence and dynamic analysis capability that Trellix can offer while anecdotal evidence points to the excessive need for high-effort fine tuning from customers to get more accurate detections they would've gotten with Trellix without need for fine tuning.</p>

Objection Handling

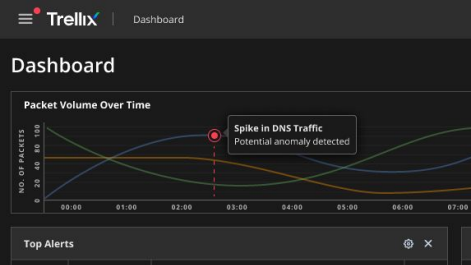
Objection	Response
Network traffic is encrypted, so why should I inspect it?	<ul style="list-style-type: none">• Trellix NDR enables flexible deployment options for decrypting and re-encrypting the traffic, detecting hidden threats and exploits, eliminating blind spots introduced by TLS and closes any opportunity for attackers.• In addition, Trellix NDR detects encrypted c2c traffic, known malware, interactive shell sessions utilizing multiple techniques including JA3 fingerprinting, domain reputation with GTI and IOC matching from extracted SNI information, lateral movement indicators utilising header information.
Replacing my current security tools will introduce risk.	<ul style="list-style-type: none">• Trellix NDR leverages the detections and alerts from existing Trellix Network Security solutions already deployed in your network, combining with advanced analytics providing increased visibility into attacker TTPs.• Trellix NDR uses L7 metadata and network flow records to discover assets, and identify critical and rogue nodes in the network environment.
NDR requires another alert management system to adopt requiring additional training for my team.	<ul style="list-style-type: none">• In fact, Trellix NDR will reduce the number of alert management systems required as it consumes alerts, netflow records and L7 metadata from NDR high-throughput sensors (NX, IPS, and PX) providing a single alert & investigation interface across all Trellix Network products.• Detections enriched with context and mapped to MITRE ATT&CK matrix enable Tier 1 Analysts to better carry out triage activities, as well as correlate with endpoint data

Objection Handling

Objection	Response
<p>NDR generates more alerts to triage as it detects anomalies in network traffic, which doesn't conform to an expected patterns of behaviour.</p>	<ul style="list-style-type: none">• Whereas most NDR solutions rely solely on anomaly-based detection, Trellix NDR utilizes a multi-layered approach consisting of signatures, signature-less, machine learning, behavioural and traffic analysis techniques to produce high-fidelity detections across the cyber kill chain.• SOC investigation workflows are focussed on alerts that matter by the correlation of detections from multiple sources and threat intelligence enrichment, reducing the effort in investigations and responses.• Trellix NDR utilizes a multi-layered detection methodology mapped to the MITRE ATT&CK matrix.
<p>There will be an impact on the performance of the NX or IPS sensors.</p>	<ul style="list-style-type: none">• There will be no performance impact on the sensors as the additional data analysis is performed on the NDR platform.• In fact, there is a potential for an increase in effective performance of the network sensors as advanced detections are delivered on the NDR platform freeing up capacity on the sensor.
<p>We already have network security, SIEM and firewalls.</p>	<ul style="list-style-type: none">• Trellix NDR works alongside existing security tools, elevating their effectiveness by helping to reduce blind spots across a given network.• Our NDR solution can also be integrated with other third party network nodes including firewalls and web gateways, on prem or in the cloud to provide incremental detections.

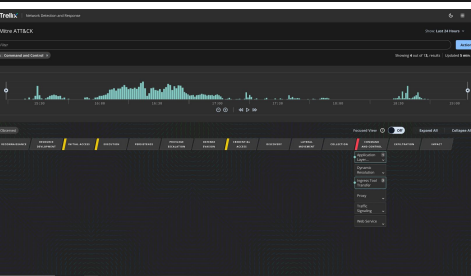
Objection Handling

Objection	Response
We already have EDR in place.	<ul style="list-style-type: none">• Trellix NDR is a perfect complement to EDR, revealing attacker movement throughout the enterprise, accelerating investigation and response.• It accelerates identification of compromised or targeted endpoints, reducing the effort required to collect and review endpoint data.• Trellix NDR uses L7 metadata and network flow records to identify assets in the network environment which may not be able to run an agent.



Top Alerts

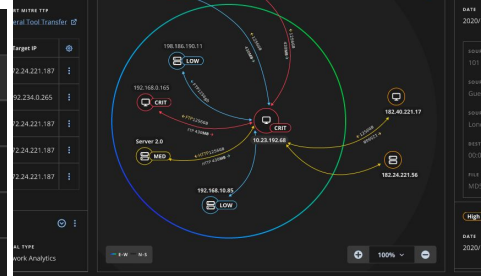
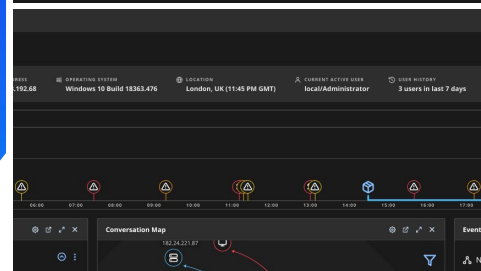
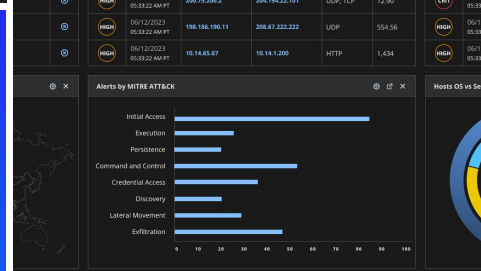
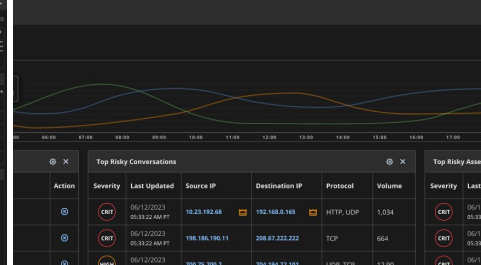
Severity	Date Created	Alert Name	Action
CRIT	06/12/2023 05:33:22 AM PT	ISC BIND RPZ Vulnerability ID: 40271 Affected Assets: 43	
CRIT	06/12/2023 05:33:22 AM PT	Data Breach Warning Alert ID: 40271 Affected Assets: 43	
HIGH	06/12/2023 05:33:22 AM PT	Data Breach Warning Alert ID: 40271 Affected Assets: 43	
HIGH	06/12/2023 05:33:22 AM PT	Data Breach Warning Alert ID: 40271 Affected Assets: 43	
HIGH	06/12/2023 05:33:22 AM PT	Intrusion Detection System Alert ID: 40271 Affected Assets: 43	



Trellix NDR

- Better Visibility
- Better Detection
- Better Investigation
- Better Response

Severity	Last Updated	Asset name
CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au
CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK
CRIT	06/12/2023 05:33:22 AM PT	Local-Hostname-10.Au
CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK

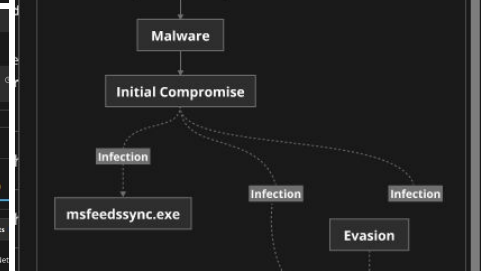


Packets

No.	Direction	Time
002	←	09/26/2024 09:18:45.109
004	←	09/26/2024 09:18:45.115
006	←	09/26/2024 09:18:45.409
008	←	09/26/2024 09:18:45.409
010	←	09/26/2024 09:18:45.409
012	←	09/26/2024 09:18:45.409

Packet Details

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: 00:50:56:01:3b:33 (00:50:56:01:3b:33), Dst: 00:00:0c:9f:f0:0a (00:00:0c:9f:f0:0a)
 Internet Protocol Version 4, Src: 128.176.85.29 (128.176.85.29), Dst: 128.20.239.34 (128.20.239.34)
 Transmission Control Protocol, Src Port: 55134 (55134), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0



Provide more details | Advise on possible next steps

Show related MITRE info | Show related breaches

Show device information | Show Knowledge Graph

The image features the Trellix logo in a bold, white, sans-serif font, centered on a background with a blue-to-green gradient. The background is decorated with two horizontal bands of white dashed lines that curve and taper towards the right side. The bottom right corner of the image is cut off at a 45-degree angle.

Trellix