Trellix

# Insider Threats - A Silent Killer in Financial Security
# 内部威胁 - 金融资安中的无声 杀手

## Enhancing Security for Taiwan

Jeff Yeo, CISSP,CISM,CCSP, ITIL, COBIT, CSM
Senior Manager ASIA

# About your Speaker

Jeff Yeo is a seasoned regional technical leader at Trellix, driving presales excellence across the Asia Pacific region. With over 17 years of IT experience, he has held various roles at Cisco, Aruba (HPE), Citrix, BT Global Services, and GovTech (IDA). Jeff specialises in security, cloud, and software technologies, with a proven track record in project management, technical sales, and partner ecosystem development. His expertise spans enterprise mobility, SSE, Identity, ITDR and Zero Trust solutions. A strategic [illegible]ker with extensive [illegible] experience.

Jeff Yeo 是一位資深的區域技術領導者，現任 Trellix，致力於推動亞太地區的售前卓越表現。擁有超過 17 年的 IT 經驗，他曾在 Cisco、Aruba (HPE)、Citrix、BT Global Services 和 GovTech (IDA) 擔任多種職位。Jeff 專精於安全、雲端及軟體技術，並在專案管理、技術銷售及合作夥伴生態系統發展方面擁有卓越的成績。他的專業領域涵蓋企業行動性、SSE、身份管理、ITDR 和零信任解決方案。作為一位具有戰略思維的專家，他擁有廣泛的區域經驗。

Trellix

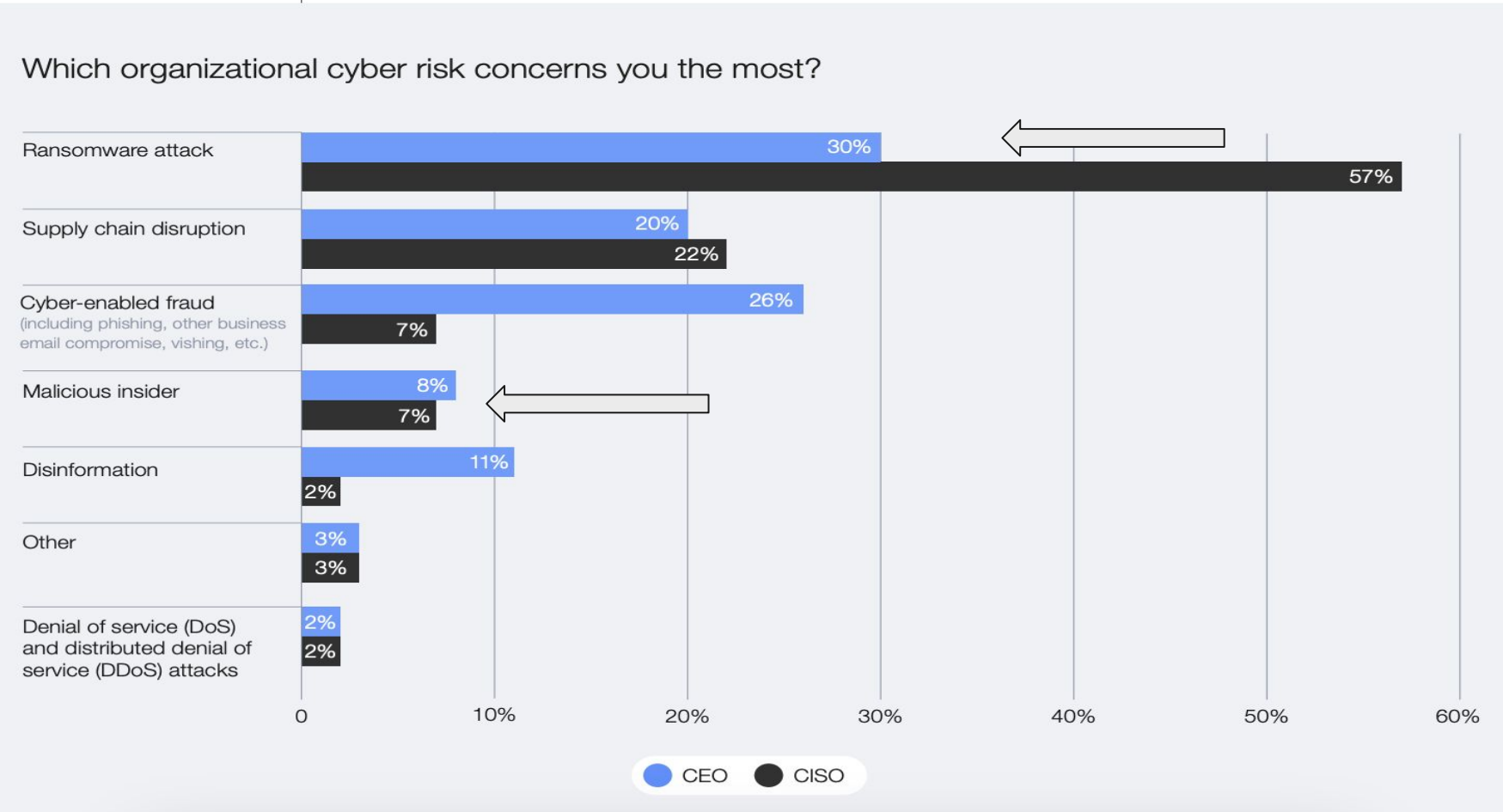
# Overview

## Table of Contents

# The Cyberthreat Landscape

## Key Insights

FIGURE 4 | **Organizational cyber risk – CEO and CISO views**




*Source: Global Cybersecurity Outlook 2025, World Economic Forum

### Key Insights

- Ransomware remains the top organizational cyber risk year on year, with 45% of respondents
- GenAI tools are lowering the cost of the phishing and social engineering campaigns that give attackers access to organizations.
- Malicious Insider remains a top threat in many customer's environment
- 勒索軟體連年位居組織最主要的資安風險，45% 的受訪者表示曾受到影響。
- 生成式 AI 工具正在降低釣魚攻擊與社交工程的成本，使攻擊者更容易入侵組織。
- 惡意內部人員依然是許多客戶環境中的重大威脅。

# Trellix Threat Intelligence Solutions

**市場上最廣泛且最深入的威脅情報之一**

**數以百萬計的感測器分布於關鍵向量（端點、電子郵件、網頁與網路）**

**可部署於雲端與地端環境**

- Global Threat Intelligence (GTI)
- Trellix Insights
- Trellix Intelligence Exchange (TIE)
- Intelligence as-a-Service
- Advanced Threat Landscape Analysis System (ATLAS)
- Private GTI


https://www.trellix.com/en-us/platform/threat-intelligence.html

Trellix

# Taiwan's Specific Cyber Attack Trends

## THREAT ACTORS HACKED TAIWAN-BASED CHUNGHWA TELECOM

Pierluigi Paganini March 04, 2024

## Threat actors stole sensitive and confidential data from the telecom giant Chunghwa Telecom Company, revealed the Ministry of National Defense.

INDUSTRY NEWS • 2 min read •

## TSMC Refuses to Pay $70 Million Ransom after Lockbit Falsely Claims Its Affiliates Hacked the Giant Chipmaker

Filip TRUȚĂ
July 03, 2023




馬偕紀念醫院遭駭客以勒索病毒攻擊要求交付贖金。刑事局證實主嫌為中國籍羅姓駭客，目前全案移送台北地檢署，4月1日發布通緝。記者廖炳棋/翻攝

## 親俄駭客對臺DDoS手法大公開，安碁資訊解析HTTP洪水攻擊防禦之道

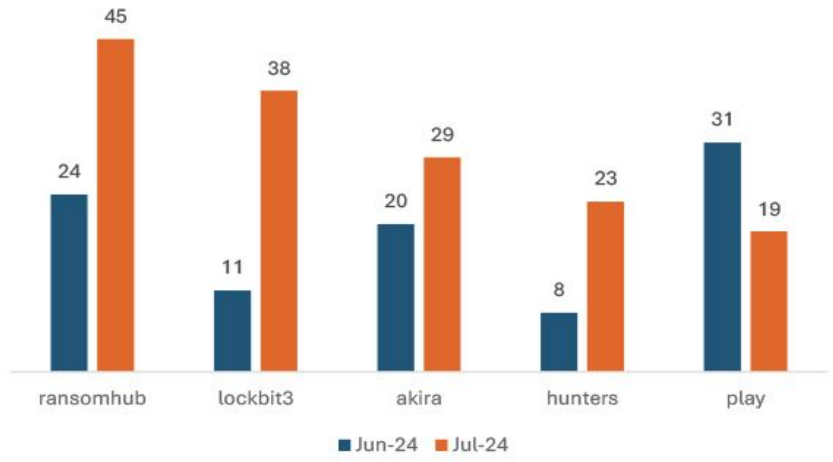
針對今年下半親俄駭客組織NoName057對臺發動DDoS攻擊，近日安碁資訊對其攻擊手法做出完全解析，指出該組織不僅利用VPS虛擬主機或VPN隱匿其攻擊背後的IP位址，並是使用消耗資源的HTTP洪水攻擊來癱瘓網站服務，而非消耗頻寬的洪水攻擊，只集中針對特定4到10個URL頁面攻擊就能奏效

文/ 羅正漢 | 2024-12-06 發表

讚 121 分享

## TREND COMPARISON OF JULY 2024's TOP 5 RANSOMWARE GROUPS WITH JUNE 2024.

Throughout July 2024, there was notable activity from several ransomware groups. Here are the trends regarding the top 5:



# Today's Data Security Challenges
# 當今的資料安全挑戰

## Malicious Actors

**19%**
Of breaches were a malicious insider attack

資安漏洞是由惡意 內部人員所造成的攻擊

## Financially Motivated

**80%**
Of malicious insiders were financially motivated.[2]

內部人員的違法行為出於財務動機

## Time to Detect

**200 Days**
Average time to detect and contain data breaches.[2]

偵測並遏止資料外洩的平均所需時間

*1 - Verizon DBIR 2024*
*2- Averages -IBM, Verizon DBIR*

**The majority of insider data leaks are the result of unintentional or accidental information sharing. 大多數的內部資料外洩是因為無意或意外地分享資訊所造成的。**

# Trellix Solution Strategy 解決策略

## Eliminate blind spots 消除盲點

- Not just perimeter - N/S and E/W
- On prem/cloud/hybrid environment visibility
- Asset discovery and monitoring 資訊產品之識別與持續性監控

## Disrupt attackers at every stage在各個階段瓦解攻擊者行動

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

## Speed investigation and response 加快調查與應對速度

- 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**

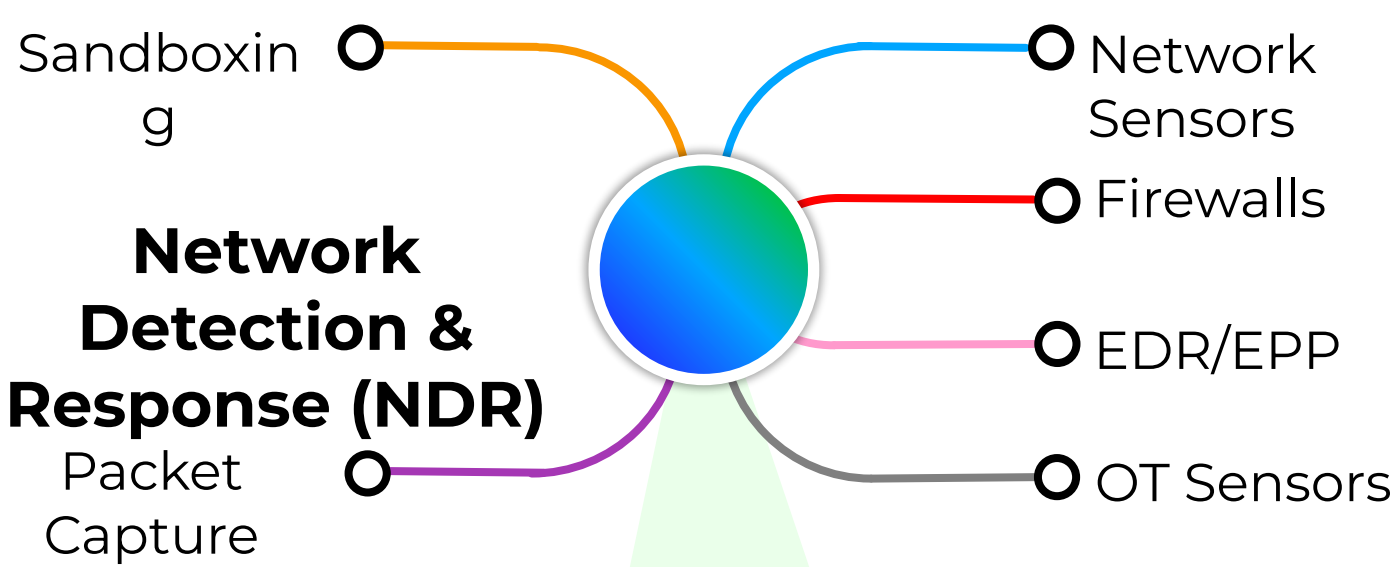
Trellix

# TRELLIX NDR

Trellix

# Trellix NDR - Solution

## Trellix Network Detection & Response (NDR)




- **Focus:** Advanced Threat **Detection, Investigation, Hunting, and Response**

**Trellix NDR Sensor (NX)**

**Trellix IPS "NDR Ready"**

Trellix

# Why Use NDR ?

## Network Detection and Response Module

**Digital Forensics and Incident Response Dashboard**

Intuitive visualization of traffic patterns on attacker scope and techniques. Integration with Threat Intel and MiTRE Mapping

**直觀式視覺化攻擊者範圍和技術上的流量模式。與威脅情報和MiTRE映射的整合**

**數位鑑識與事件回應儀表板**

**Visibility Dashboard**

Track changes in Network Activity, Explore Ports, Protocols and Assets for advanced threat hunting

**追蹤網絡活動變化，探索端口、協議和資產，以進行進階的威脅狩獵**

**Beaconing detection**

ML based identification of potential malicious activity

**基於機器學習的潛在惡意活動識別**


**通過監控和基準化網路活動来偵測數據竊取行爲**

**Data Exfiltration**

Detecting data thefts by monitoring and baselining the network activity

**基於機器學習的技術，用於檢測可疑和惡意的回調活動**

**Domain Generation Algorithm**

ML based technique in detecting suspicious and malicious callback activity

**Asset Discovery**

Extend visibility and automatically map discovered assets to device type, including new devices. Additional correlation with sensor telemetry data

**擴展能見度並自動將發現的資 產映射到設備地圖，包括新增的設備。與傳感器遙測數據的額外關聯**

Trellix

# Trellix NDR - Critical Capabilities Review

## INTEGRATIONS

- NGFW/FW
- Ticketing Tools
- SOAR
- EDR
- XDR
- SIEM
- Threat Intel
- IoT/OT/ICS
- IDS/IPS

## INTERACTIVE ANALYST SPRINGBOARD & DASHBOARDS

| | | | |
|---|---|---|---|
| Contextual Insights | Trellix WISE AI | IR Workbench | Advanced Reporting |

## DETECTION

| | |
|---|---|
| TTP Based | ML Anomalies & Detections |
| Intel Based | Rule Based Detections |
| Attack Path Discovery | Smart & Full PCAP |

## RESPONSE

| | |
|---|---|
| Forensics Automation | Timeline View |
| Retrospective Analysis | Triage & Suppression |
| Blocking Policies | Conversation Mapping |

## DATA LAKE & ANALYTICS

| | | | |
|---|---|---|---|
| Entity-level Knowledge | Federated Search | Log Data | Correlation & Enrichment |
| Full Activity Records | Historical Context | Structured PCAP Data | Unstructured PCAP Data |

## DATA SOURCES & SECURITY CONTROL POINTS


TX Endpoint


TX Network


TX Data Sec


TX Collab Sec


TX Intel


Third Party

Trellix

# NDR: Threat Detection

**Traditional Network Perimeter Security**

**Trellix Network Detection and Response**


Signatures 標誌

Dynamic Analysis 動態分析

Threat Intelligence 威脅情報

TTP-based ML Modules

Hunting Triggers 行跡捕捉與反應

Behavioral Analysis 行為分析

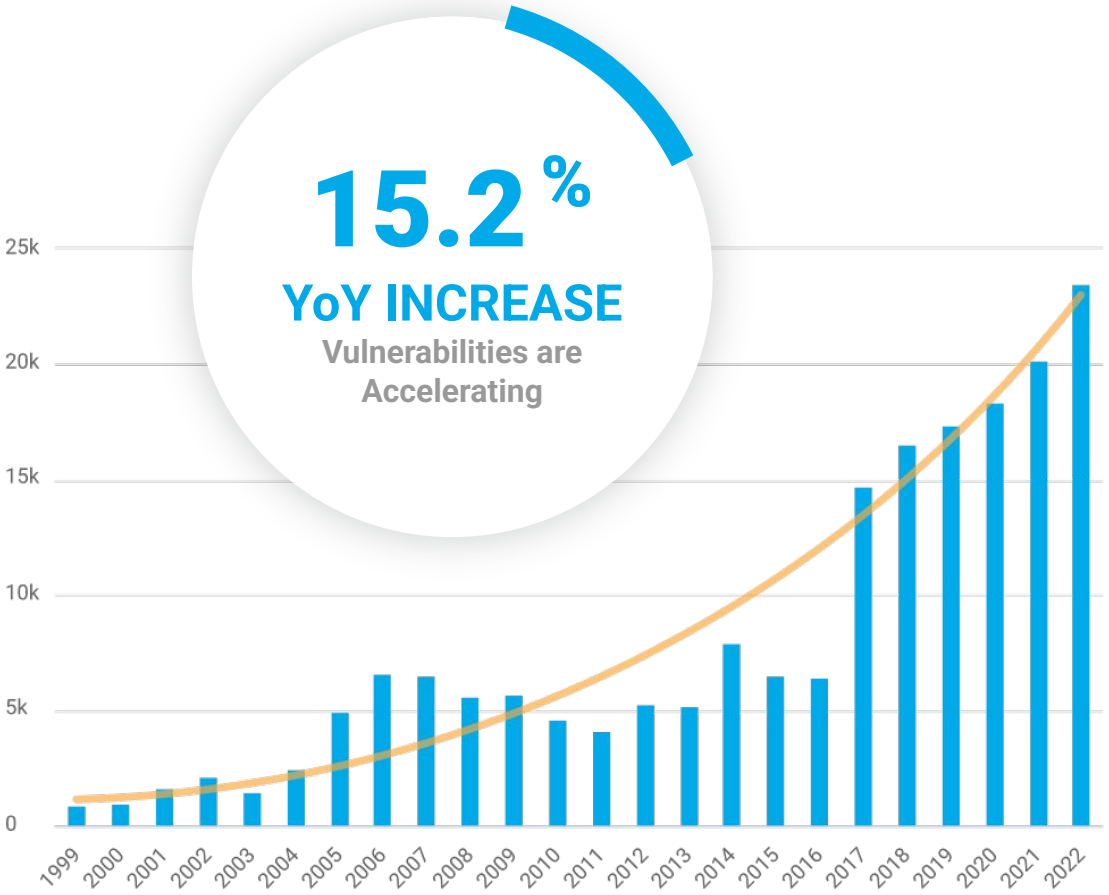
Correlation Rules 關聯規則

**Leveraging multiple detection and AI approaches**

Trellix

# Trellix NDR Attack Path Discovery(APD)

# NDR : Visibility & Vulnerability Sprawl




- **每月超過 2000 個漏洞（CVE），且數量持續增加；其中有 300 到 500 個與各種規模的組織都息息相關。**
- **漏洞掃描工具在判定優先性方面表現不佳 ——採用一體適用的指標，導致大量積壓，且無法準確反映實際攻擊與勒索軟體的發生方式。**
- **目前僅有三種選擇：人工分析、自行建立優先順序系統，或嘗試修補所有漏洞。**
- **新的資產（短暫性／臨時性／未受管理的）會在未遵循正規流程的情況下出現 ——誰知道它們的存在？**

- Over 2000 vulnerabilities (CVEs) **every month** and growing; 300-500 applicable to every organization regardless of size
- Vulnerability scanners do a poor job of prioritizing – one-size-fits-all metrics that leave huge backlogs and **fail to capture how breaches/ransomware happen**
- Three options – manual analysis, roll your own prioritization system, or try to patch everything
- New assets ( transient/ephemeral/unmanaged) pop-up without following due process - who is aware?

Trellix

# NDR : Attack Path Discovery[APD]攻擊路徑發現

## Trellix Endpoint Security(ENS)

- File Permissions
- Network Topology
- Assets
- Access Rights
- Application Usage
- Active Directory
- Cloud Services
- User Activity
- Asset Criticality

## Vulnerabilitie

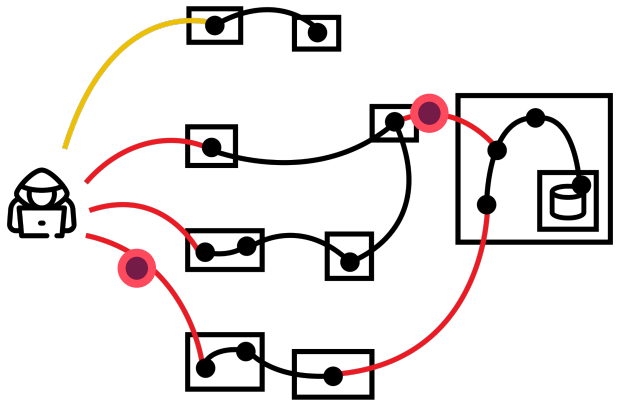
RAPID7

tenable

Qualys.

## Trellix NDR - Attack Path Discovery

Automated Blast Radius Modeling
自動化爆炸半程建模



Context Aware Prioritization
情境感知優先級

Attack Scenarios Database
攻擊場景資料庫

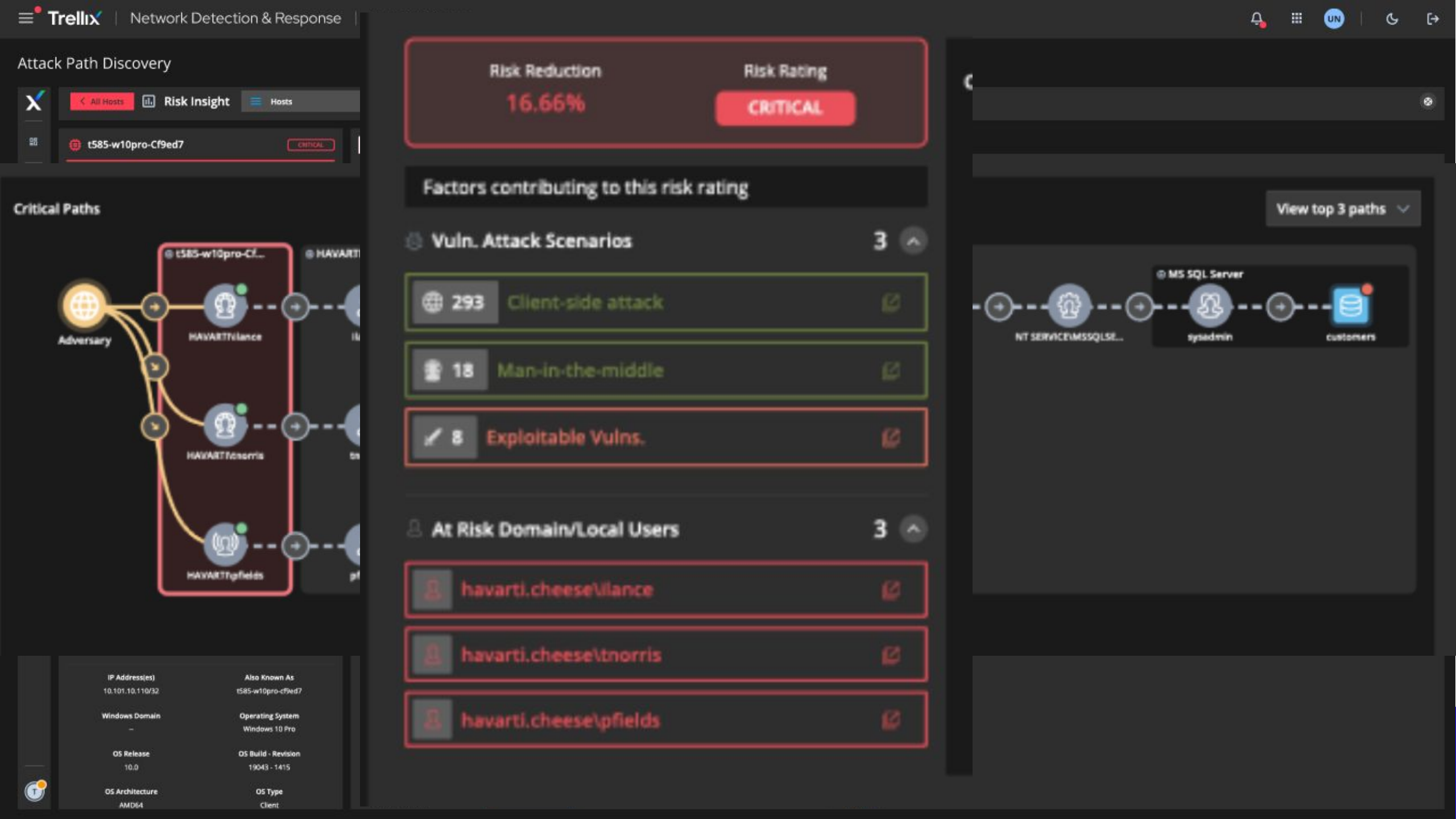
Not Exploitable
Deprioritized
(25% – 50%)

## Results

Prioritize Vulnerabilities Daily

Track Business Risk Over Time

Automate Your Remediation Workflow


Trellix | Network Detection & Response
Attack Path Discovery
All Hosts
Risk Insight
Hosts
t585-w10pro-Cf9ed7
CRITICAL
Critical Paths
Adversary
HAVARTT\ilance
HAVARTT\tnorris
HAVARTT\pfields
IP Address(es)
10.101.10.110/32
Also Known As
t585-w10pro-cf9ed7
Windows Domain
–
Operating System
Windows 10 Pro
OS Release
10.0
OS Build - Revision
19043 - 1415
OS Architecture
AMD64
OS Type
Client
Risk Reduction
16.66%
Risk Rating
CRITICAL
Factors contributing to this risk rating
Vuln. Attack Scenarios
3
293
Client-side attack
18
Man-in-the-middle
8
Exploitable Vulns.
At Risk Domain/Local Users
3
havarti.cheese\ilance
havarti.cheese\tnorris
havarti.cheese\pfields
View top 3 paths
MS SQL Server
NT SERVICE\MSSQLSE...
sysadmin
customers

Trellix

# Gen-AI with Trellix NDR

## Detecting unknown and Emerging threats

# Why Trellix Wise

Trellix Wise 透過減輕警報疲勞，幫助安全營運團隊，無論經驗水準如何，都能調查 100% 的警報並自動化調查和修復。Trellix Wise 做出決策，提供指導，並使用對話式 AI，讓使用者在工作中進行威脅狩獵，同時學習。

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

Trellix

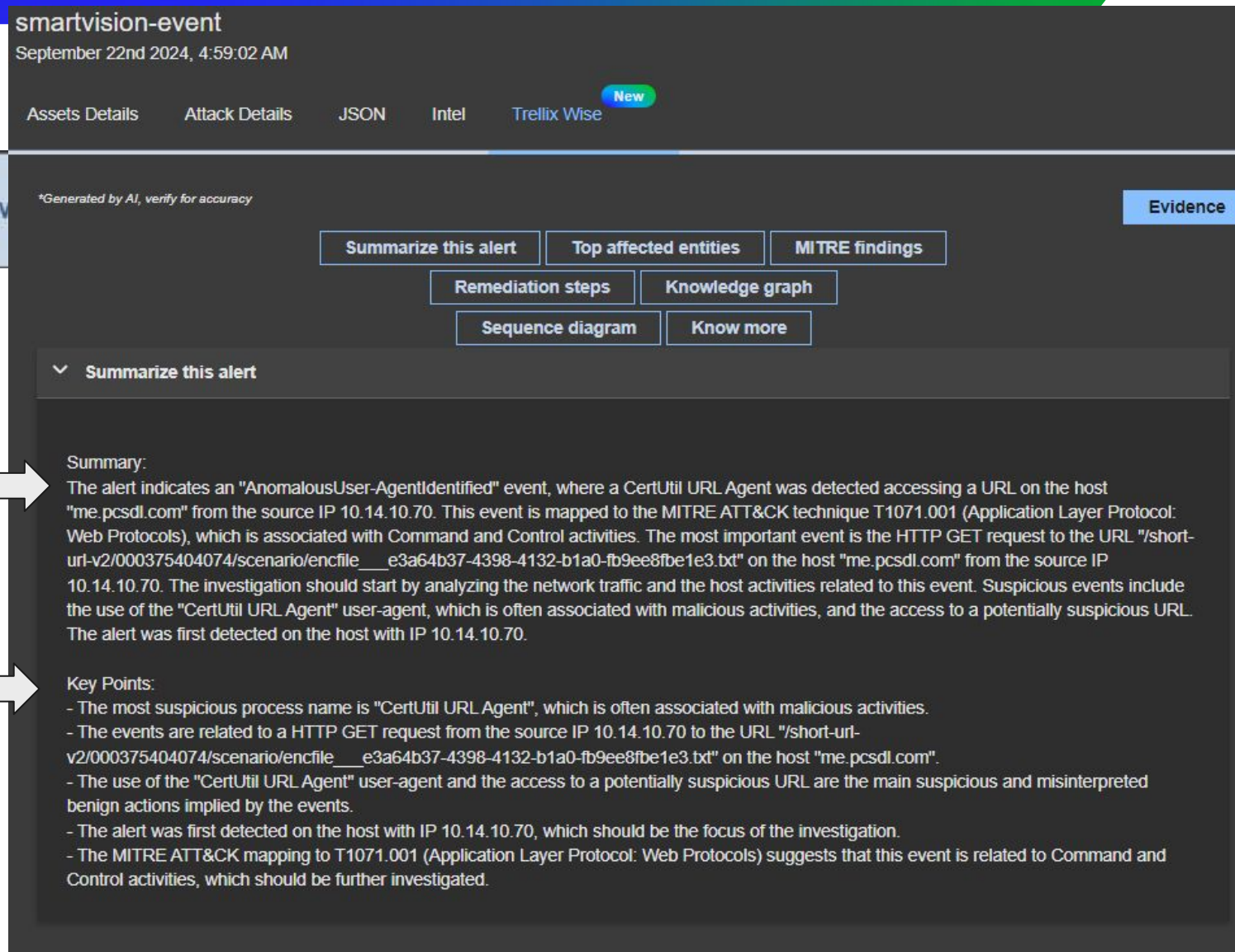
# Trellix Wise Alert Enrichment

| | | | |
|---|---|---|---|
| Med | 2024-09-22T04:59:02 Z | NX | smartvision-ev |

**Trellix SmartVision 是 Trellix 網路安全方案中的先進關聯與分析引擎。**

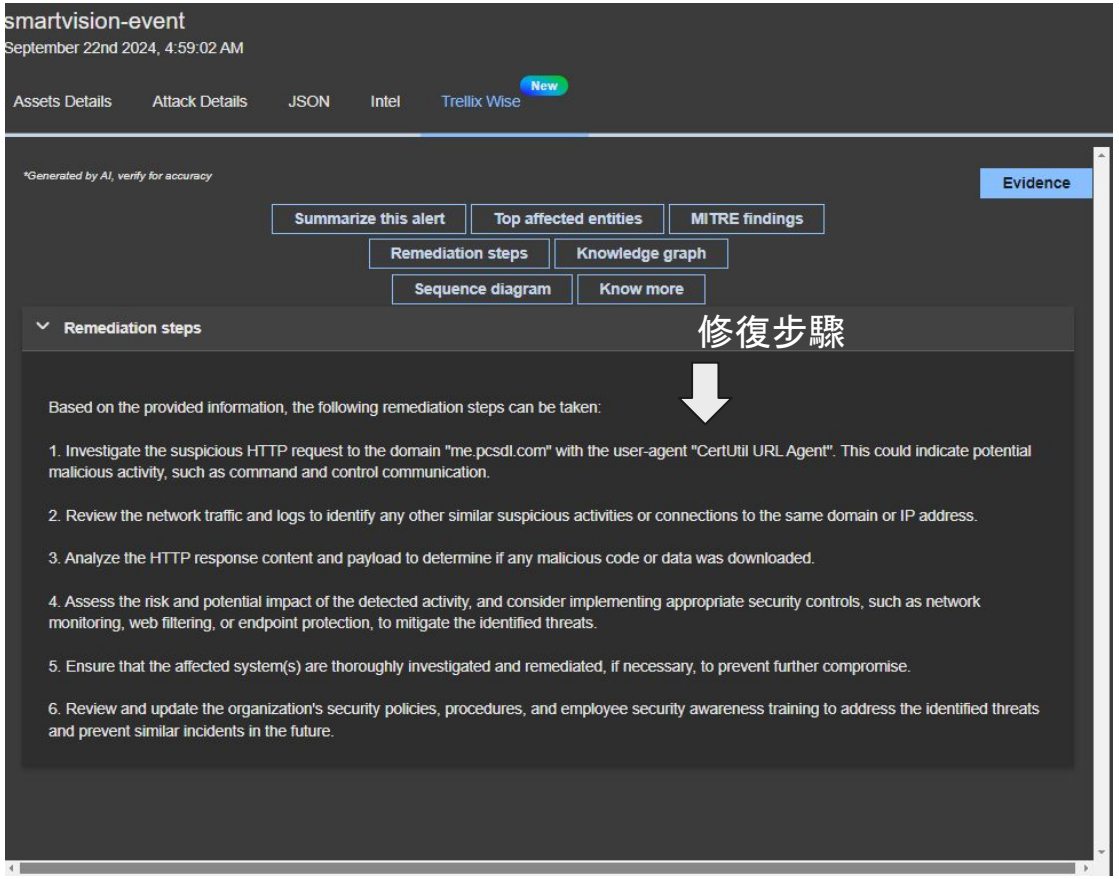
**即刻總結**

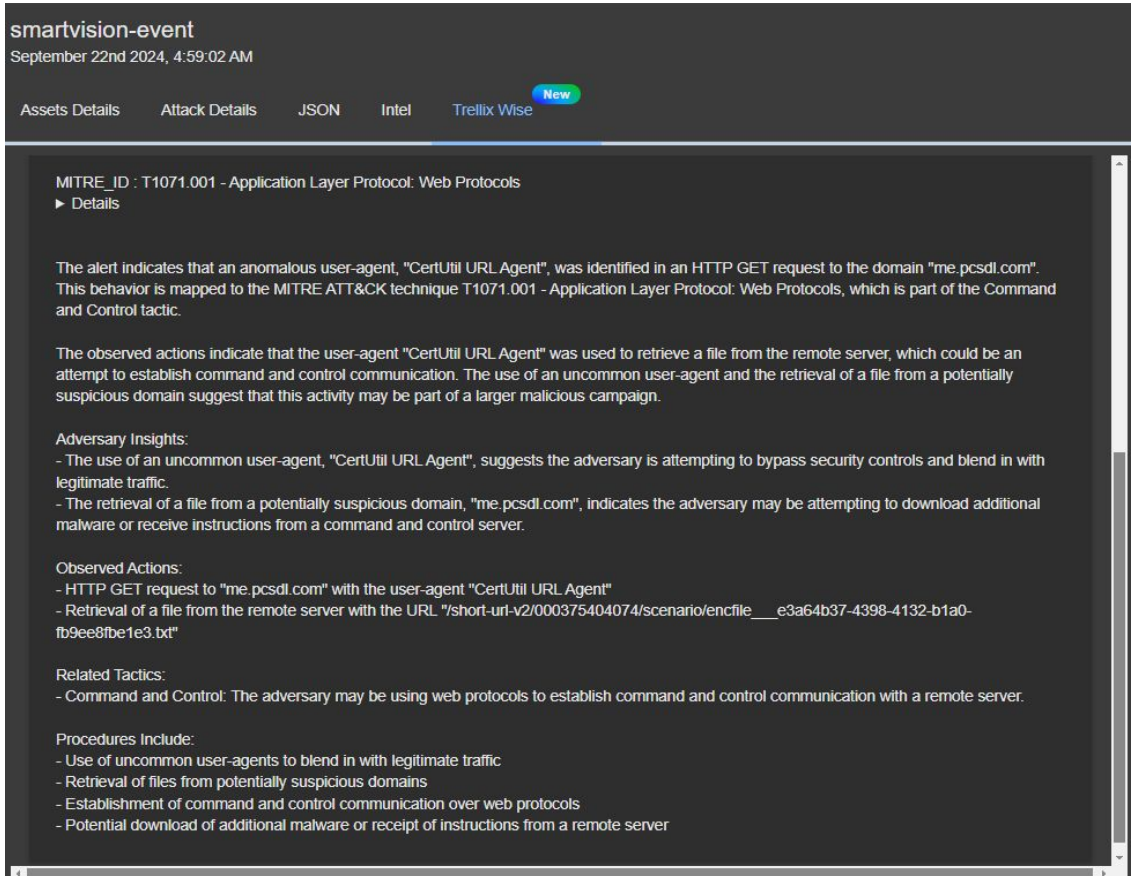
**攻擊事件的關鍵要點**




Trellix

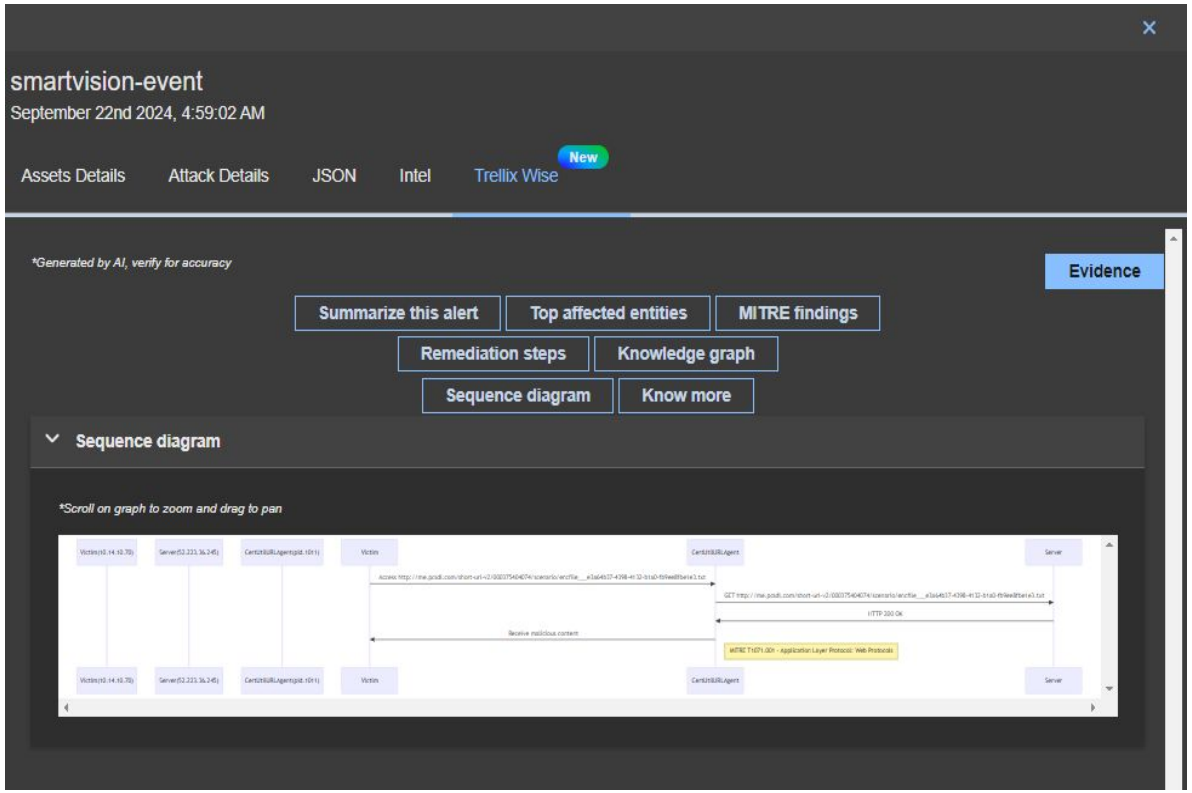
# Trellix Wise Alert Enrichment

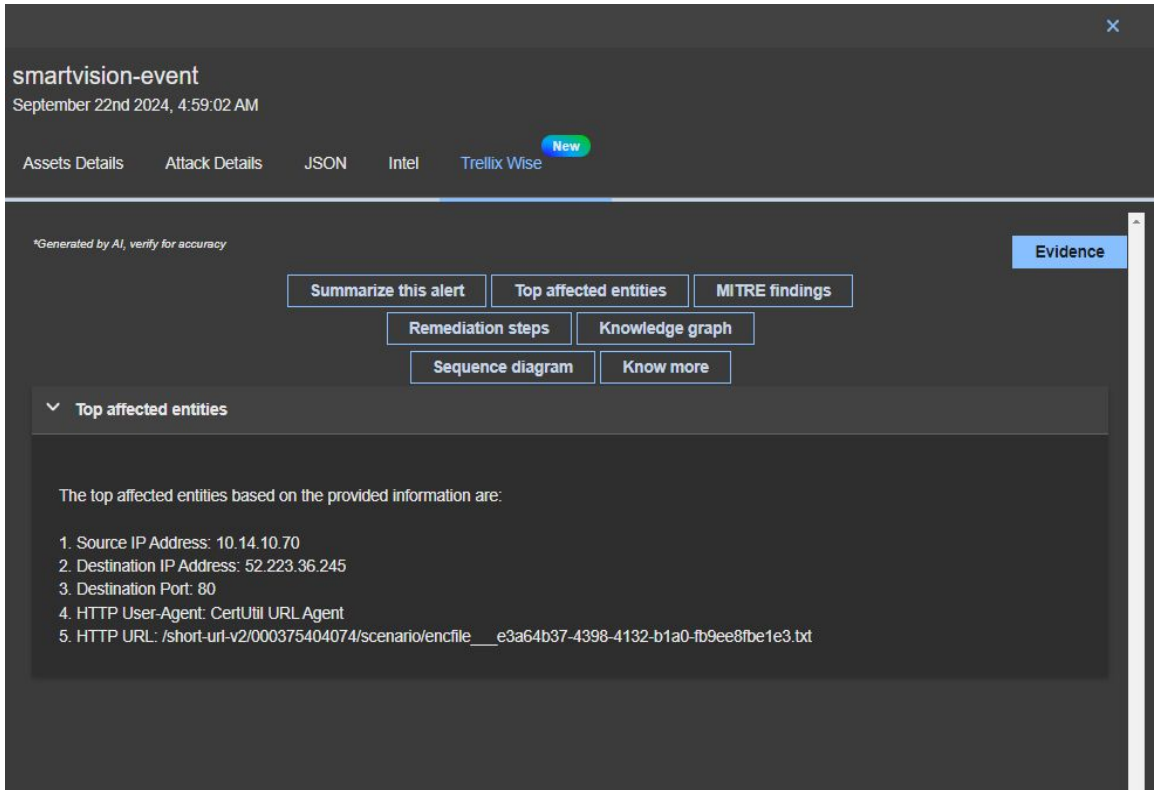



Trellix

# Trellix Wise Alert Enrichment




Trellix

Trellix

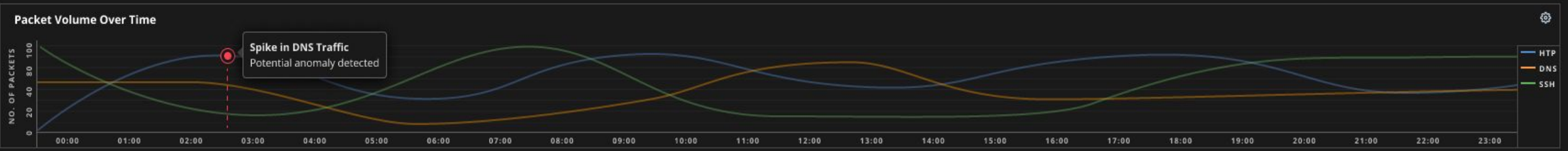
# NDR Use Cases - Real-World Applications for FSI

# NDR 使用案例 – 金融服務行業的實際應用

# Dashboard

Show: Last 24 Hours

## Packet Volume Over Time




## Top Alerts

| Severity | Date Created | Alert Name | Action |
|---|---|---|---|
| CRIT | 22/11/2024 01:10:00 AM PT | ISC BIND RPZ Vulnerability ID: 40271 \| Affected Assets: 43 | |
| CRIT | 22/11/2024 01:50:00 AM PT | SC DNSSEC Validation Failure... ID: 2347 \| Affected Assets: 43 | |
| HIGH | 22/11/2024 02:29:00 AM PT | Data Breach Warning Alert ID: 40271 \| Affected Assets: 43 | |
| HIGH | 22/11/2024 02:40:00 AM PT | BIND DNS Query Flood Attack... ID: 1342 \| Affected Assets: 43 | |
| HIGH | 22/11/2024 04:50:00 AM PT | SC DNSSEC Configuration Error... ID: 6739 \| Affected Assets: 43 | |

## Top Risky Conversations

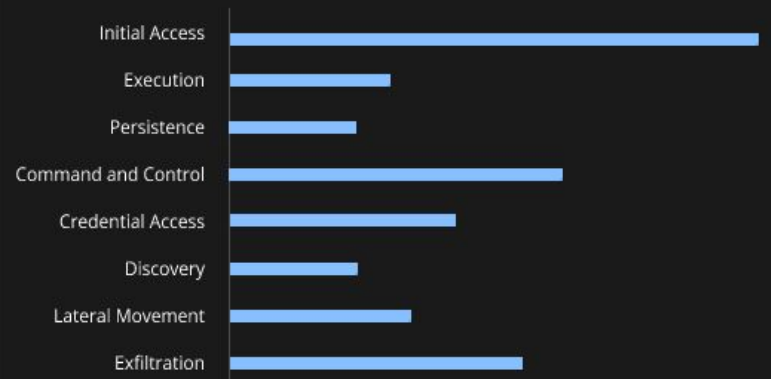
| Severity | Last Updated | Source IP | Destination IP | Protocol | Volume |
|---|---|---|---|---|---|
| CRIT | 22/11/2024 02:10:00 AM PT | 10.23.192.68 | 192.168.0.165 | HTTP, UDP | 4.50 Mb |
| CRIT | 22/11/2024 04:03:00 AM PT | 198.186.190.11 | 208.67.222.222 | TCP | 66 Mb |
| HIGH | 22/11/2024 04:47:00 AM PT | 200.75.200.2 | 204.194.22.101 | UDP, TCP | 12.90 Mb |
| HIGH | 22/11/2024 05:10:00 AM PT | 198.186.190.11 | 208.67.222.222 | UDP | 5.54 Mb |
| HIGH | 22/11/2024 05:30:00 AM PT | 10.14.65.67 | 10.14.1.200 | HTTP | 1.4 Gb |

## Top Risky Assets

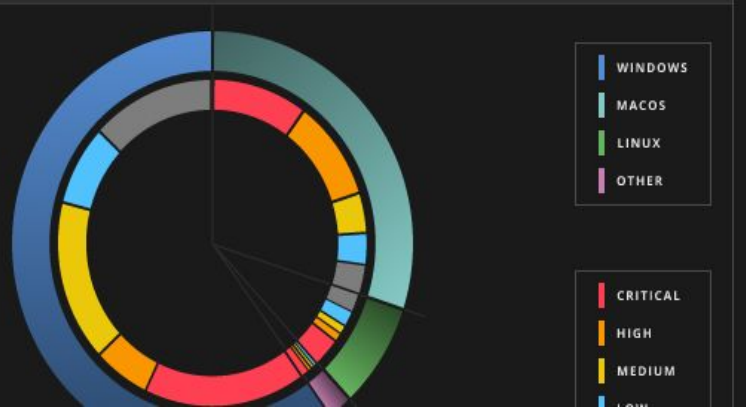
| Severity | Last Updated | Asset Details | IP Address | OS | Watch |
|---|---|---|---|---|---|
| CRIT | 22/11/2024 02:10:00 AM PT | Ndr-Hostname-10.Au ID: 40271 | 10.23.192.68 | | |
| CRIT | 22/11/2024 04:03:00 AM PT | Ndr-Router-Delta-04.A... ID: 40271 | 200.75.200.2 | | |
| CRIT | 22/11/2024 04:47:00 AM PT | Ndr-Vm-Sigma-14.Au ID: 40271 | 128.176.85.29 | | |
| HIGH | 22/11/2024 05:10:00 AM PT | Ndr-Mailserver-Rho-19... ID: 40271 | 128.20.239.34 | | |
| HIGH | 22/11/2024 05:30:00 AM PT | Ndr-Hostname-10.Au ID: 40271 | 128.20.239.34 | | |

## Alerts By Country


## Alerts by MITRE ATT&CK




## Hosts OS vs Severity



10.23.192.

Displaying **2** results for the selected matching criteria

Alerts **(0)**

Assets **(2)** View Found Assets

10.23.192.68

10.23.192.255

## Top Alerts

| Severity | Date Created | Alert Name | Action |
|---|---|---|---|
| CRIT | 22/11/2024 01:10:00 AM PT | ISC BIND RPZ Vulnerability ID: 40271 \| Affected Assets: 43 | |
| CRIT | 22/11/2024 01:50:00 AM PT | SC DNSSEC Validation Failure... ID: 2347 \| Affected Assets: 43 | |
| HIGH | 22/11/2024 02:29:00 AM PT | Data Breach Warning Alert ID: 40271 \| Affected Assets: 43 | |
| HIGH | 22/11/2024 02:40:00 AM PT | BIND DNS Query Flood Attack... ID: 1342 \| Affected Assets: 43 | |
| HIGH | 22/11/2024 04:50:00 AM PT | SC DNSSEC Configuration Error... ID: 6739 \| Affected Assets: 43 | |

## Top Risky Conversations

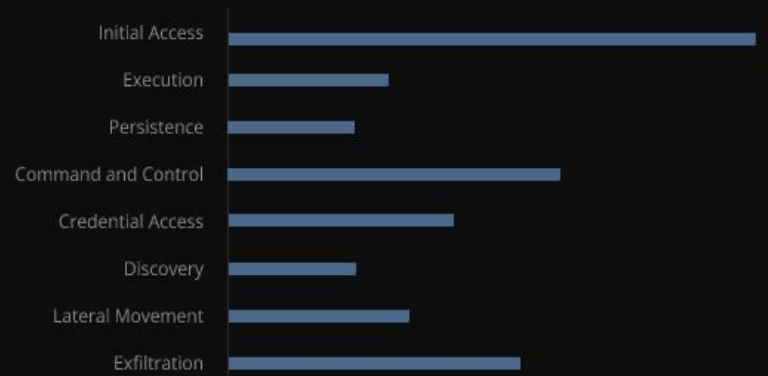
| Severity | Last Updated | Source IP | Destination IP | Protocol | Volume |
|---|---|---|---|---|---|
| CRIT | 22/11/2024 02:10:00 AM PT | 10.23.192.68 | 192.168.0.165 | HTTP, UDP | 4.50 Mb |
| CRIT | 22/11/2024 04:03:00 AM PT | 198.186.190.11 | 208.67.222.222 | TCP | 66 Mb |
| HIGH | 22/11/2024 04:47:00 AM PT | 200.75.200.2 | 204.194.22.101 | UDP, TCP | 12.90 Mb |
| HIGH | 22/11/2024 05:10:00 AM PT | 198.186.190.11 | 208.67.222.222 | UDP | 5.54 Mb |
| HIGH | 22/11/2024 05:30:00 AM PT | 10.14.65.67 | 10.14.1.200 | HTTP | 1.4 Gb |

## Top Risky Assets

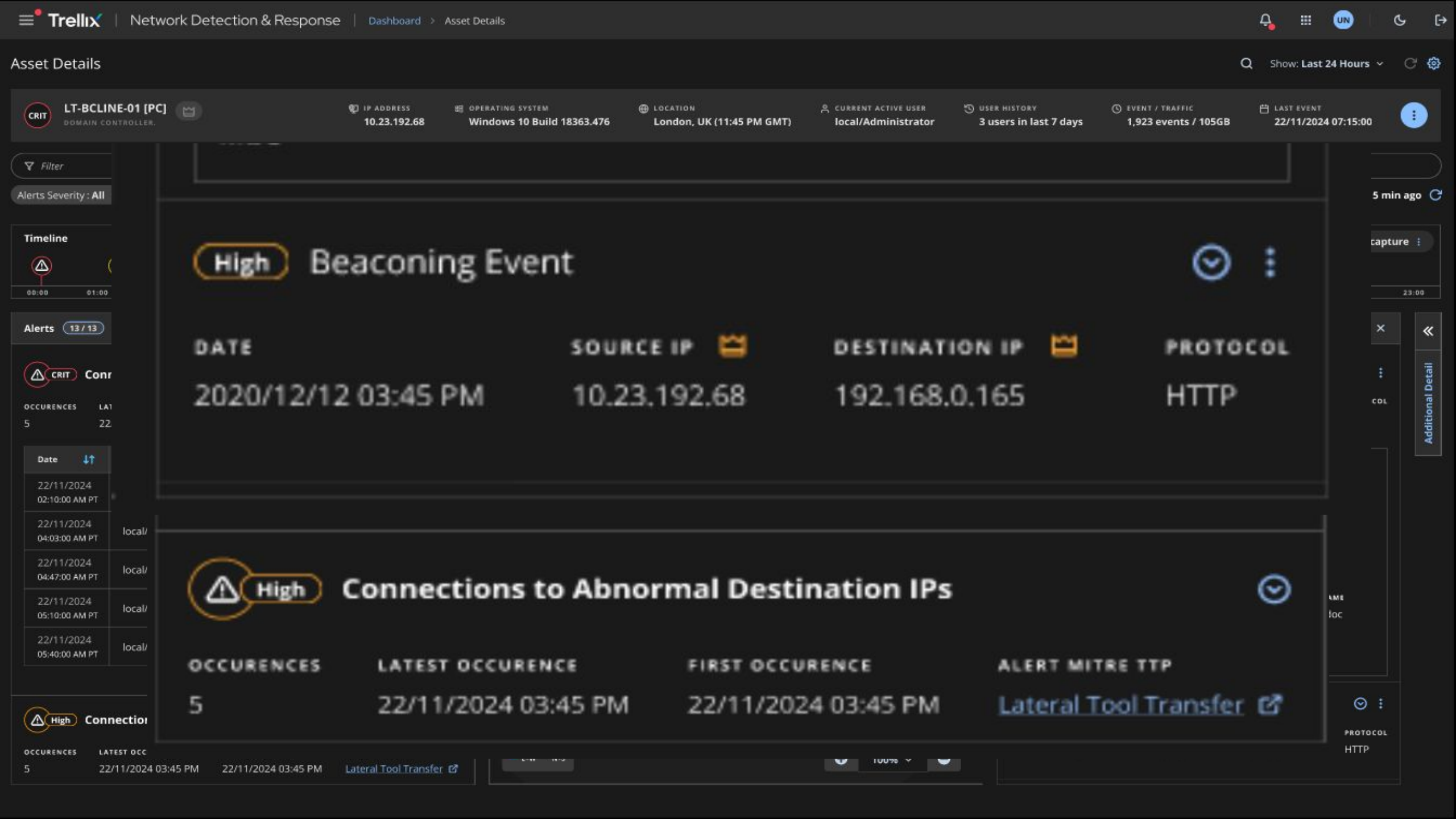
| Severity | Last Updated | Asset Details | IP Address | OS | Watch |
|---|---|---|---|---|---|
| CRIT | 22/11/2024 02:10:00 AM PT | Ndr-Hostname-10.Au ID: 40271 | 10.23.192.68 | | |
| CRIT | 22/11/2024 04:03:00 AM PT | Ndr-Router-Delta-04.A... ID: 40271 | 200.75.200.2 | | |
| CRIT | 22/11/2024 04:47:00 AM PT | Ndr-Vm-Sigma-14.Au ID: 40271 | 128.176.85.29 | | |
| HIGH | 22/11/2024 05:10:00 AM PT | Ndr-Mailserver-Rho-19... ID: 40271 | 128.20.239.34 | | |
| HIGH | 22/11/2024 05:30:00 AM PT | Ndr-Hostname-10.Au ID: 40271 | 128.20.239.34 | | |

## Alerts By Country


## Alerts by MITRE ATT&CK




## Hosts OS vs Severity


Trellix
Network Detection & Response
Dashboard
Asset Details
Asset Details
Show: Last 24 Hours
CRIT
LT-BCLINE-01 [PC]
DOMAIN CONTROLLER
IP ADDRESS
10.23.192.68
OPERATING SYSTEM
Windows 10 Build 18363.476
LOCATION
London, UK (11:45 PM GMT)
CURRENT ACTIVE USER
local/Administrator
USER HISTORY
3 users in last 7 days
EVENT / TRAFFIC
1,923 events / 105GB
LAST EVENT
22/11/2024 07:15:00
Filter
Alerts Severity : All
Timeline
Alerts 13 / 13
5 min ago
High
Beaconing Event
DATE
2020/12/12 03:45 PM
SOURCE IP
10.23.192.68
DESTINATION IP
192.168.0.165
PROTOCOL
HTTP
Additional Detail
High
Connections to Abnormal Destination IPs
OCCURENCES
5
LATEST OCCURENCE
22/11/2024 03:45 PM
FIRST OCCURENCE
22/11/2024 03:45 PM
ALERT MITRE TTP
Lateral Tool Transfer
Date
22/11/2024 02:10:00 AM PT
22/11/2024 04:03:00 AM PT
22/11/2024 04:47:00 AM PT
22/11/2024 05:10:00 AM PT
22/11/2024 05:40:00 AM PT
PROTOCOL
HTTP

# Asset Details

Show: **Last 24 Hours**

**CRIT** LT-BCLINE-01 [PC]
DOMAIN CONTROLLER.

| IP ADDRESS | OPERATING SYSTEM | LOCATION | CURRENT ACTIVE USER | USER HISTORY | EVENT / TRAFFIC | LAST EVENT |
|---|---|---|---|---|---|---|
| 10.23.192.68 | Windows 10 Build 18363.476 | London, UK (11:45 PM GMT) | local/Administrator | 3 users in last 7 days | 1,923 events / 105GB | 22/11/2024 07:15:00 |

Filter

Alerts Severity : **All** | Alert MITRE TTP : **Undefined**

Updated **5 min ago**

**Timeline**

Packet capture

00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00

## Alerts 13 / 13

### CRIT Connections to Abnormal Destination IPs

| OCCURENCES | LATEST OCCURENCE | FIRST OCCURENCE | ALERT MITRE TTP |
|---|---|---|---|
| 5 | 22/11/2024 03:45 PM | 22/11/2024 03:45 PM | Lateral Tool Transfer |

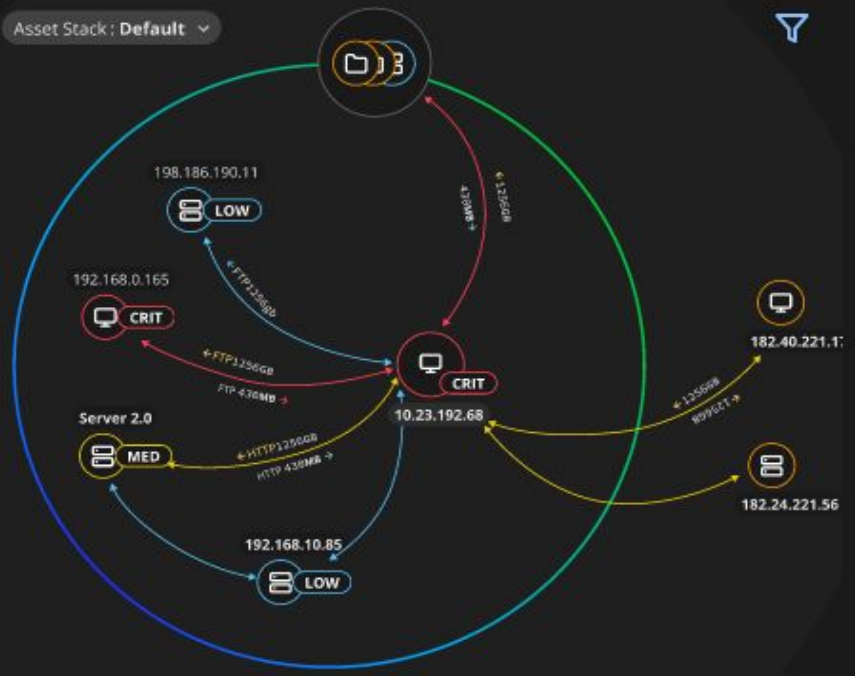
| Date | User | Source IP | Destination IP |
|---|---|---|---|
| 22/11/2024 02:10:00 AM PT | local/Administrator | 10.23.192.68 | 172.24.221.187 |
| 22/11/2024 04:03:00 AM PT | local/PowerUser | 192.168.0.165 | 192.234.0.265 |
| 22/11/2024 04:47:00 AM PT | local/ServiceAccount | 204.194.22.101 | 200.75.200.2 |
| 22/11/2024 05:10:00 AM PT | local/ITSupport1 | 192.168.0.165 | 204.194.22.101 |
| 22/11/2024 05:40:00 AM PT | local/Manager2024 | 200.75.200.2 | 10.23.192.68 |

### High Connections to Abnormal Destination IPs

| OCCURENCES | LATEST OCCURENCE | FIRST OCCURENCE | ALERT MITRE TTP |
|---|---|---|---|
| 5 | 22/11/2024 03:45 PM | 22/11/2024 03:45 PM | Lateral Tool Transfer |

## Conversation Map

Asset Stack : **Default**




## Additional Detail

### ePO On-prem

### Tenable Security Center

| | |
|---|---|
| VULNERABILITY AGE | 60 - 180 days |
| CVSSV3 IMPACT SCORE | 5.9 |
| EXPLOIT CODE MATURITY | Unproven |
| PREDICTED IMPACT SCORE | false |
| PRODUCT COVERAGE | Low |
| THREAT INTENSITY | Low |
| THREAT RECENCY | 7 To 30 Days |
| CVE ID(s): | CVS-2017-3140 |

# Alert Details

Show: **Last 24 Hours**

CRIT **DNS: Microsoft Windows Internet Connection Sharing Deni...**

| SOURCE IP | DESTINATION IP | OPERATING SYSTEM | STATUS | DATE | CURRENT ACTIVE USER | LAST EVENT |
|---|---|---|---|---|---|---|
| 192.168.0.165 | 128.176.85.29 | Windows 10 Build 18363.476 | New | 2024-08-26 07:15:00Z | local/Administrator | 22/11/2024 07:15:00 |

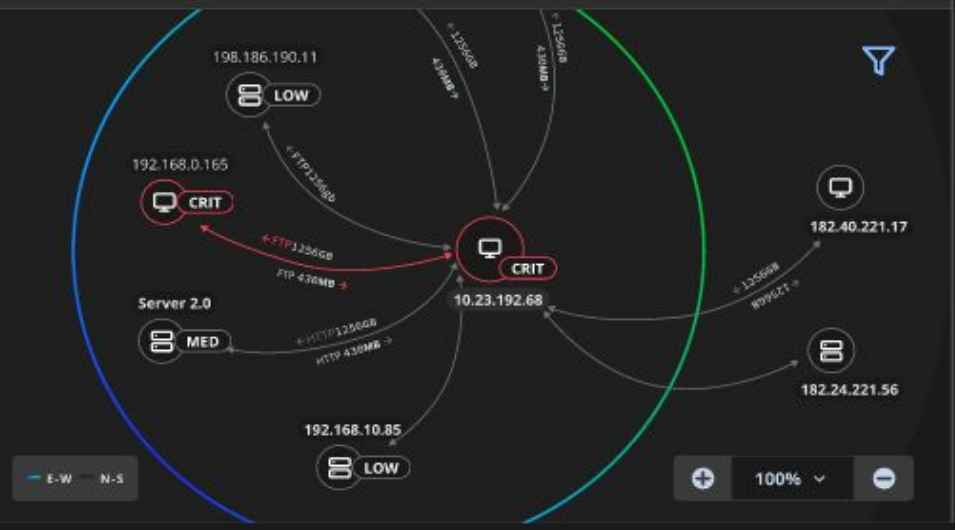
## Alert Details

| | |
|---|---|
| Attack Category | **Exploit** |
| Detection | **Signature** |
| CVE ID | CVE-2017-3140 +3 |
| Intelligence IOCs | -- |
| MITRE ATT&CK TTP | T1498 - Network Denial of Service +3 |

## Asset Details

| | |
|---|---|
| Source User | **local/Administrator** |
| Source Host | **LT-BCLINE-01 [PC]** |
| Source Port | **201** |
| Source Geolocation | **11** |
| Destination User | **--** |
| Destination Host | **ehost.by** |
| Destination Port | **80** |
| Destination Geo Location | **Belarus** |

## Conversation Map




## Impacted Assets 10

| Severity | Date | Source IP | Destination IP |
|---|---|---|---|
| CRIT | 22/11/2024 01:14:39 AM PT | 10.1.2.3 | 172.16.0.10 |
| CRIT | 22/11/2024 03:45:22 AM PT | 192.168.45.12 | 190.75.200.2 |
| MED | 22/11/2024 05:33:22 AM PT | 172.20.15.30 | 192.168.40.10 |
| MED | 22/11/2024 06:33:22 AM PT | 10.200.50.5 | 172.19.120.200 |
| LOW | 22/11/2024 07:33:22 AM PT | 192.168.90.150 | 10.125.200.240 |
| LOW | 22/11/2024 | 172.18.45.78 | 192.168.50.101 |

## Events 19

### Network Activity: Process:x733cd url:http...

| DATE | SOURCE IP | DESTINATION IP | PROTOCOL |
|---|---|---|---|
| 22/11/2024 03:45 PM | 10.23.192.68 | 192.168.0.165 | HTTP |

| SOURCE USER | SOURCE HOST | SOURCE PORT | SOURCE MAC ADDRESS |
|---|---|---|---|
| Guest User | LT-BCLINE-01 [PC] | 13596 | 00:0B:6C:BA:C4:FF |

| SOURCE GEOLOCATION | DESTINATION USER | DESTINATION HOST | DESTINATION PORT |
|---|---|---|---|
| London, UK | -- | ehost.by | 80 |

| TARGET MAC ADDRESS | DESTINATION GEOLOCATION | NETWORK TRAFFIC VOLUME |
|---|---|---|
| 00:0c:7D:BA:C4:EE | Belarus | 5.5 MB |

| FILE NAME | FILE HASH |
|---|---|
| Proc.doc | MD5 |

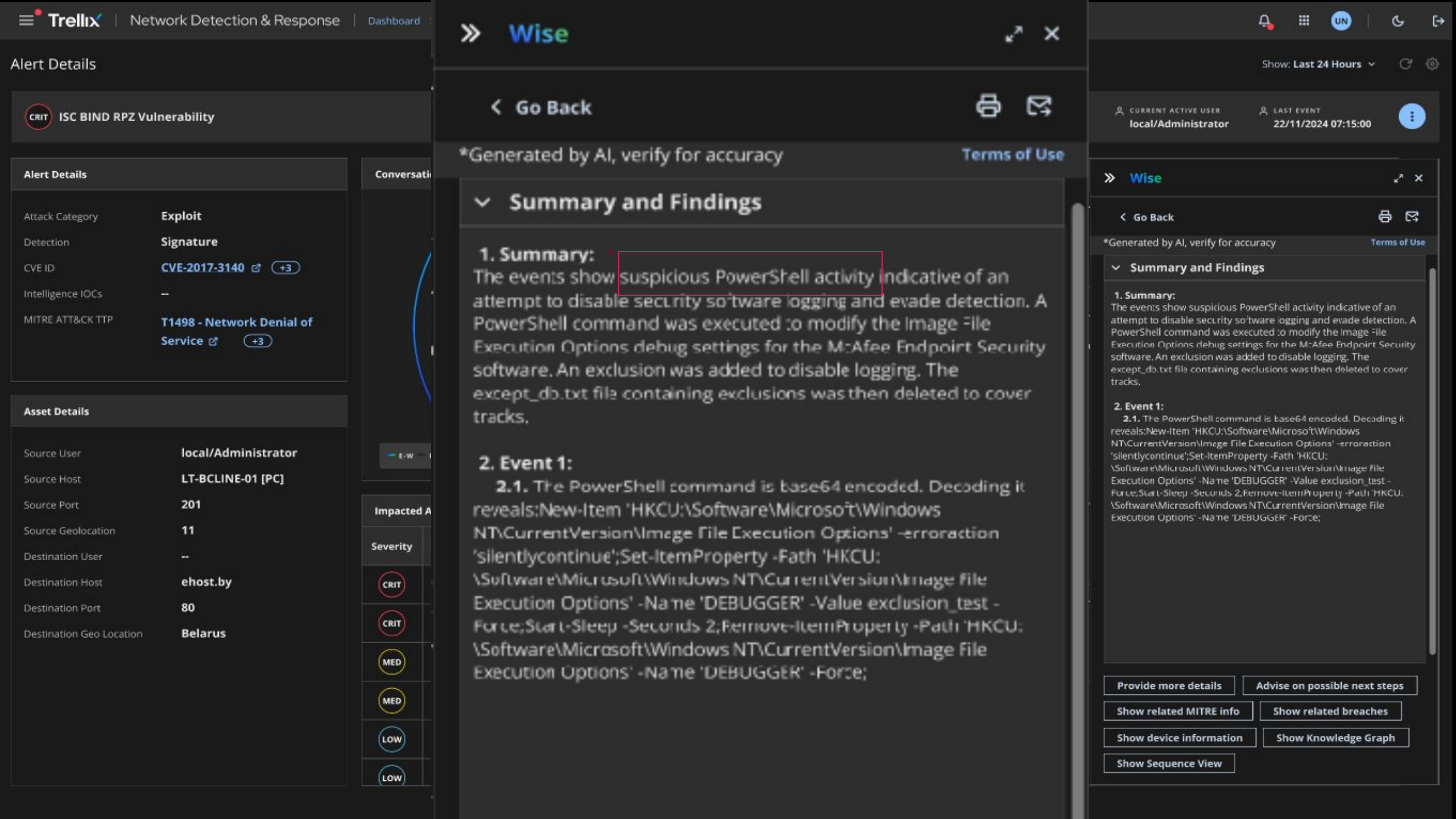
### HIGH Beaconing Event

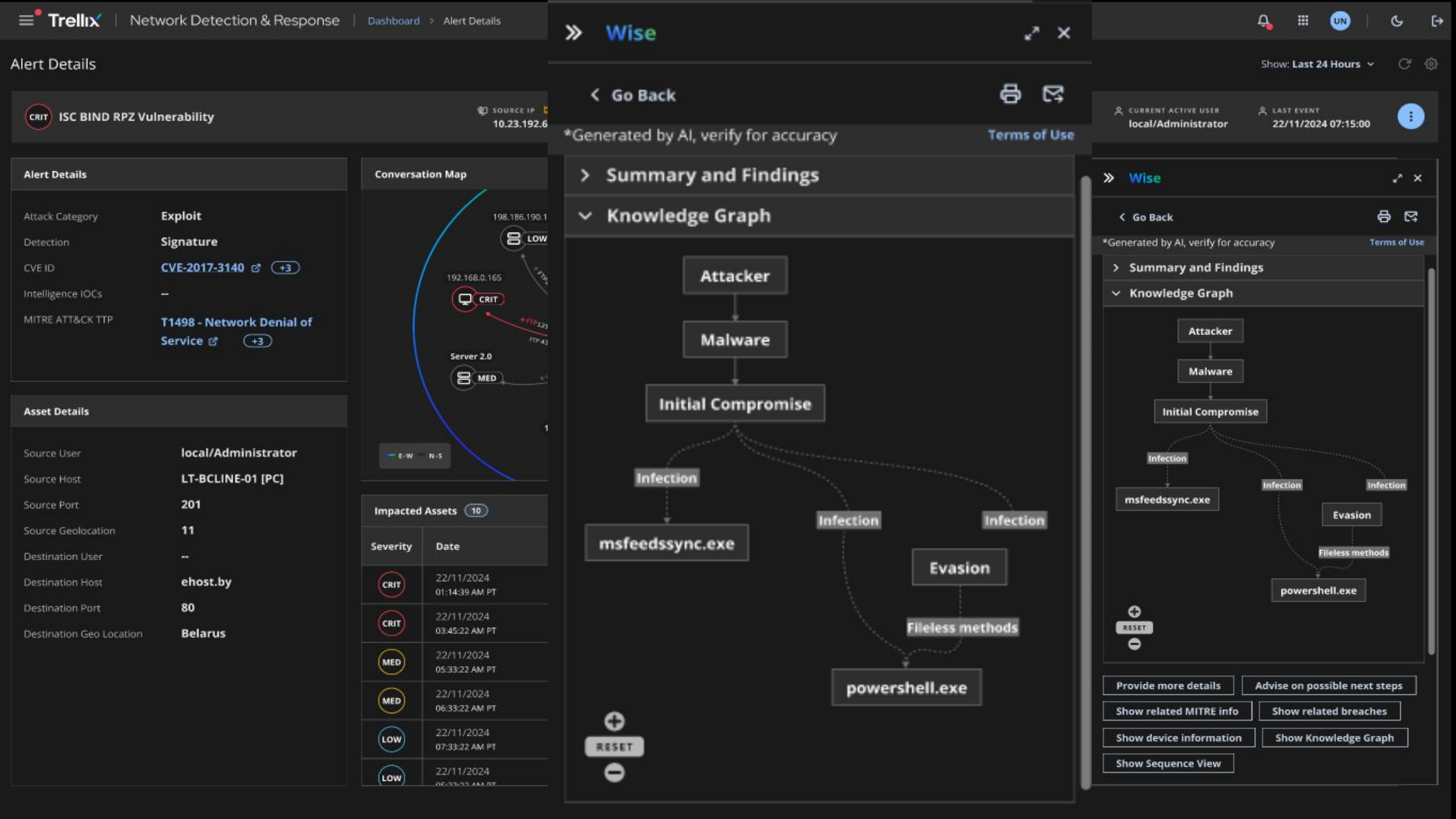
| DATE | SOURCE IP | DESTINATION IP | PROTOCOL |
|---|---|---|---|
| 2020/12/12 03:45 PM | 10.23.192.68 | 192.168.0.165 | HTTP |

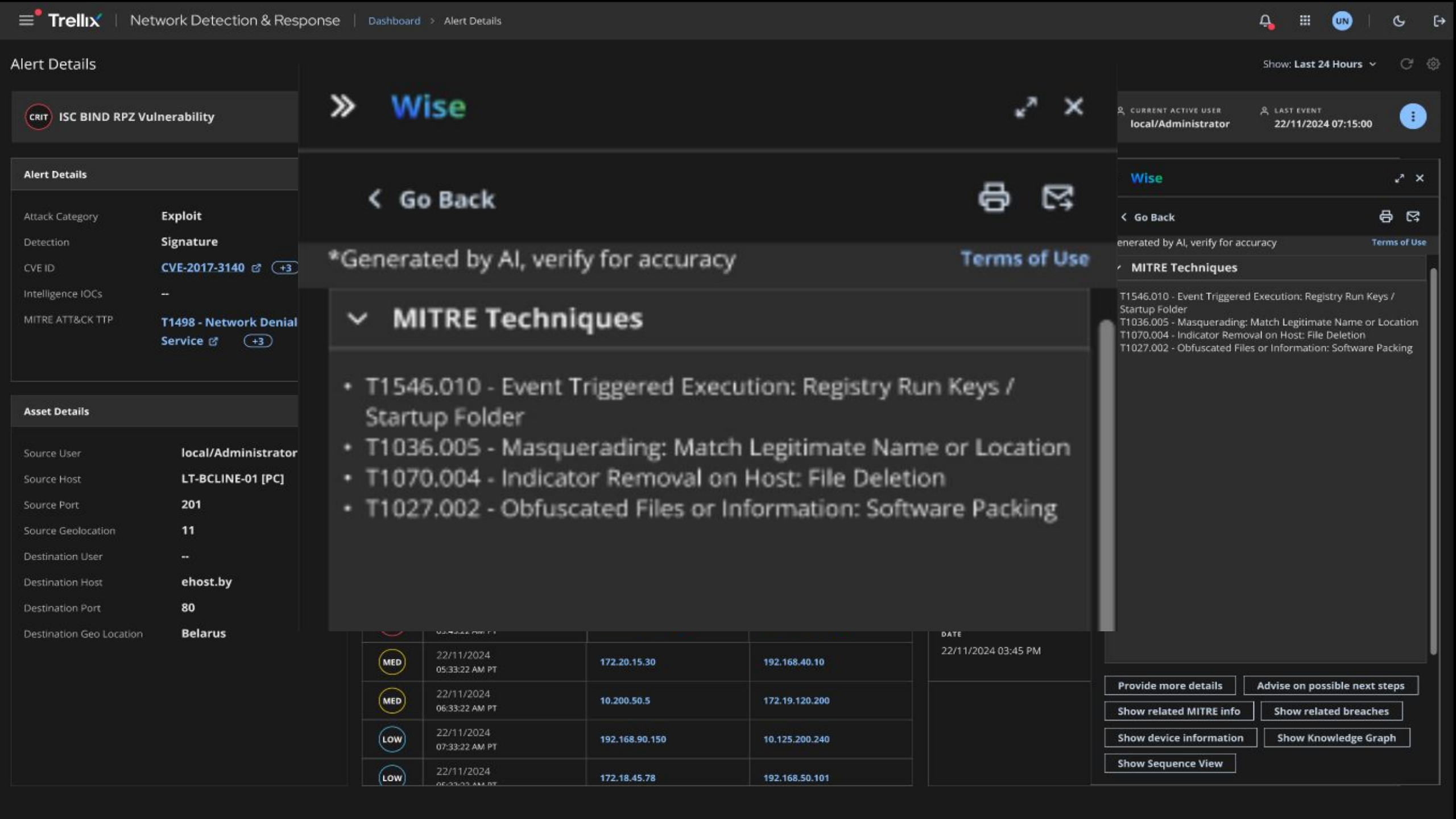
### Network Activity: Process:x733cd url:http...

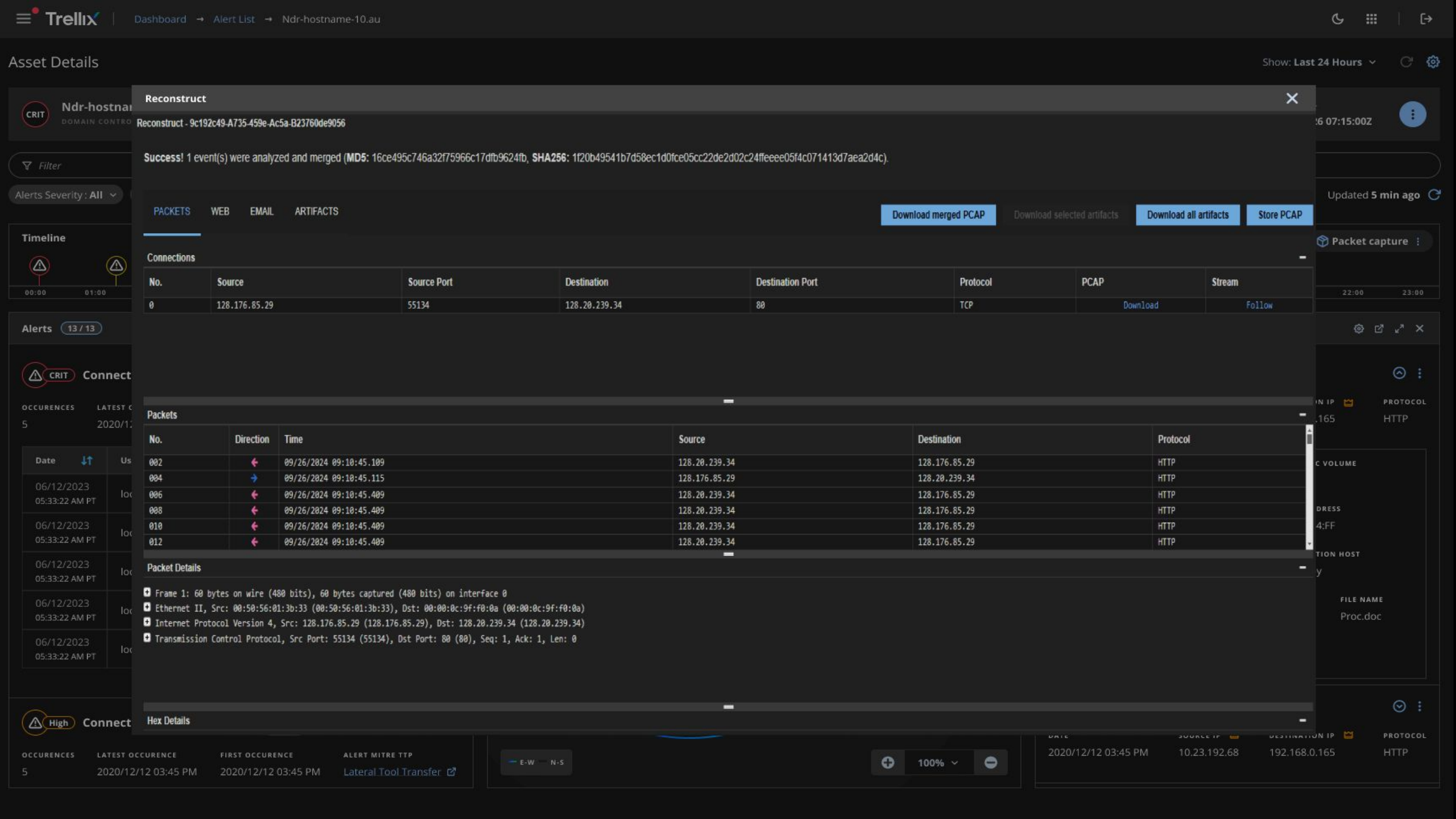
| DATE | SOURCE IP | DESTINATION IP | PROTOCOL |
|---|---|---|---|
| 22/11/2024 03:45 PM | 10.23.192.68 | 192.168.0.165 | HTTP |

Wise | OS Change | JSON


Trellix | Network Detection & Response | Dashboard
Alert Details
CRIT ISC BIND RPZ Vulnerability
Alert Details
Attack Category Exploit
Detection Signature
CVE ID CVE-2017-3140 +3
Intelligence IOCs --
MITRE ATT&CK TTP T1498 - Network Denial of Service +3
Asset Details
Source User local/Administrator
Source Host LT-BCLINE-01 [PC]
Source Port 201
Source Geolocation 11
Destination User --
Destination Host ehost.by
Destination Port 80
Destination Geo Location Belarus
Conversati
Impacted A
Severity
CRIT
CRIT
MED
MED
LOW
LOW
Wise
Go Back
*Generated by AI, verify for accuracy
Terms of Use
Summary and Findings
1. Summary:
The events show suspicious PowerShell activity indicative of an attempt to disable security software logging and evade detection. A PowerShell command was executed to modify the Image File Execution Options debug settings for the McAfee Endpoint Security software. An exclusion was added to disable logging. The except_db.txt file containing exclusions was then deleted to cover tracks.
2. Event 1:
2.1. The PowerShell command is base64 encoded. Decoding it reveals:New-Item 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options' -erroraction 'silentlycontinue';Set-ItemProperty -Path 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options' -Name 'DEBUGGER' -Value exclusion_test -Force;Start-Sleep -Seconds 2;Remove-ItemProperty -Path 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options' -Name 'DEBUGGER' -Force;
Show: Last 24 Hours
CURRENT ACTIVE USER local/Administrator
LAST EVENT 22/11/2024 07:15:00
Provide more details
Advise on possible next steps
Show related MITRE info
Show related breaches
Show device information
Show Knowledge Graph
Show Sequence View


Trellix | Network Detection & Response | Dashboard > Alert Details
Alert Details
Show: Last 24 Hours
CRIT ISC BIND RPZ Vulnerability
SOURCE IP 10.23.192.6
CURRENT ACTIVE USER local/Administrator
LAST EVENT 22/11/2024 07:15:00
Alert Details
Attack Category Exploit
Detection Signature
CVE ID CVE-2017-3140 +3
Intelligence IOCs --
MITRE ATT&CK TTP T1498 - Network Denial of Service +3
Asset Details
Source User local/Administrator
Source Host LT-BCLINE-01 [PC]
Source Port 201
Source Geolocation 11
Destination User --
Destination Host ehost.by
Destination Port 80
Destination Geo Location Belarus
Conversation Map
198.186.190.1
LOW
192.168.0.165
CRIT
Server 2.0
MED
E-W N-S
Impacted Assets 10
Severity Date
CRIT 22/11/2024 01:14:39 AM PT
CRIT 22/11/2024 03:45:22 AM PT
MED 22/11/2024 05:33:22 AM PT
MED 22/11/2024 06:33:22 AM PT
LOW 22/11/2024 07:33:22 AM PT
LOW 22/11/2024
Wise
Go Back
*Generated by AI, verify for accuracy
Terms of Use
Summary and Findings
Knowledge Graph
Attacker
Malware
Initial Compromise
Infection
Infection
Infection
msfeedssync.exe
Evasion
Fileless methods
powershell.exe
RESET
Wise
Go Back
*Generated by AI, verify for accuracy
Terms of Use
Summary and Findings
Knowledge Graph
Attacker
Malware
Initial Compromise
Infection
Infection
Infection
msfeedssync.exe
Evasion
Fileless methods
powershell.exe
RESET
Provide more details
Advise on possible next steps
Show related MITRE info
Show related breaches
Show device information
Show Knowledge Graph
Show Sequence View


Trellix | Network Detection & Response | Dashboard > Alert Details
Alert Details
Show: Last 24 Hours
CRIT ISC BIND RPZ Vulnerability
CURRENT ACTIVE USER local/Administrator
LAST EVENT 22/11/2024 07:15:00
Alert Details
Attack Category Exploit
Detection Signature
CVE ID CVE-2017-3140 +3
Intelligence IOCs --
MITRE ATT&CK TTP T1498 - Network Denial Service +3
Asset Details
Source User local/Administrator
Source Host LT-BCLINE-01 [PC]
Source Port 201
Source Geolocation 11
Destination User --
Destination Host ehost.by
Destination Port 80
Destination Geo Location Belarus
Wise
Go Back
*Generated by AI, verify for accuracy
Terms of Use
MITRE Techniques
• T1546.010 - Event Triggered Execution: Registry Run Keys / Startup Folder
• T1036.005 - Masquerading: Match Legitimate Name or Location
• T1070.004 - Indicator Removal on Host: File Deletion
• T1027.002 - Obfuscated Files or Information: Software Packing
MED 22/11/2024 05:33:22 AM PT 172.20.15.30 192.168.40.10
MED 22/11/2024 06:33:22 AM PT 10.200.50.5 172.19.120.200
LOW 22/11/2024 07:33:22 AM PT 192.168.90.150 10.125.200.240
LOW 22/11/2024 172.18.45.78 192.168.50.101
DATE
22/11/2024 03:45 PM
Provide more details
Advise on possible next steps
Show related MITRE info
Show related breaches
Show device information
Show Knowledge Graph
Show Sequence View


Trellix
Dashboard → Alert List → Ndr-hostname-10.au
Asset Details
Show: Last 24 Hours
Reconstruct
Reconstruct - 9c192c49-A735-459e-Ac5a-B23760de9056
Success! 1 event(s) were analyzed and merged (MD5: 16ce495c746a32f75966c17dfb9624fb, SHA256: 1f20b49541b7d58ec1d0fce05cc22de2d02c24ffeeee05f4c071413d7aea2d4c).
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
0 128.176.85.29 55134 128.20.239.34 80 TCP Download Follow
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
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
Hex Details
Timeline
Alerts 13 / 13
Updated 5 min ago
Packet capture
CRIT Connect
High Connect
OCCURENCES 5
LATEST OCCURENCE 2020/12/12 03:45 PM
FIRST OCCURENCE 2020/12/12 03:45 PM
ALERT MITRE TTP Lateral Tool Transfer
100%
2020/12/12 03:45 PM 10.23.192.68 192.168.0.165 HTTP

# 下一步 Next Steps

## Trellix Professional Services:

- Security Assessment 安全評估
- Incident Response 事件回應
- Health Check 健康檢查

## Trellix Solution Design Workshop:

- Endpoint
- Email
- XDR
- NDR - IPS,NX
- Data Lost prevention

## Proof of Value:

- Limited deployment of Trellix solutions to demonstrate results
- Measurable outcomes in your environment
- Clear business case for full implementation

## Contact:

dylan.wei@trellix.com

Trellix

# Thank You

Trellix