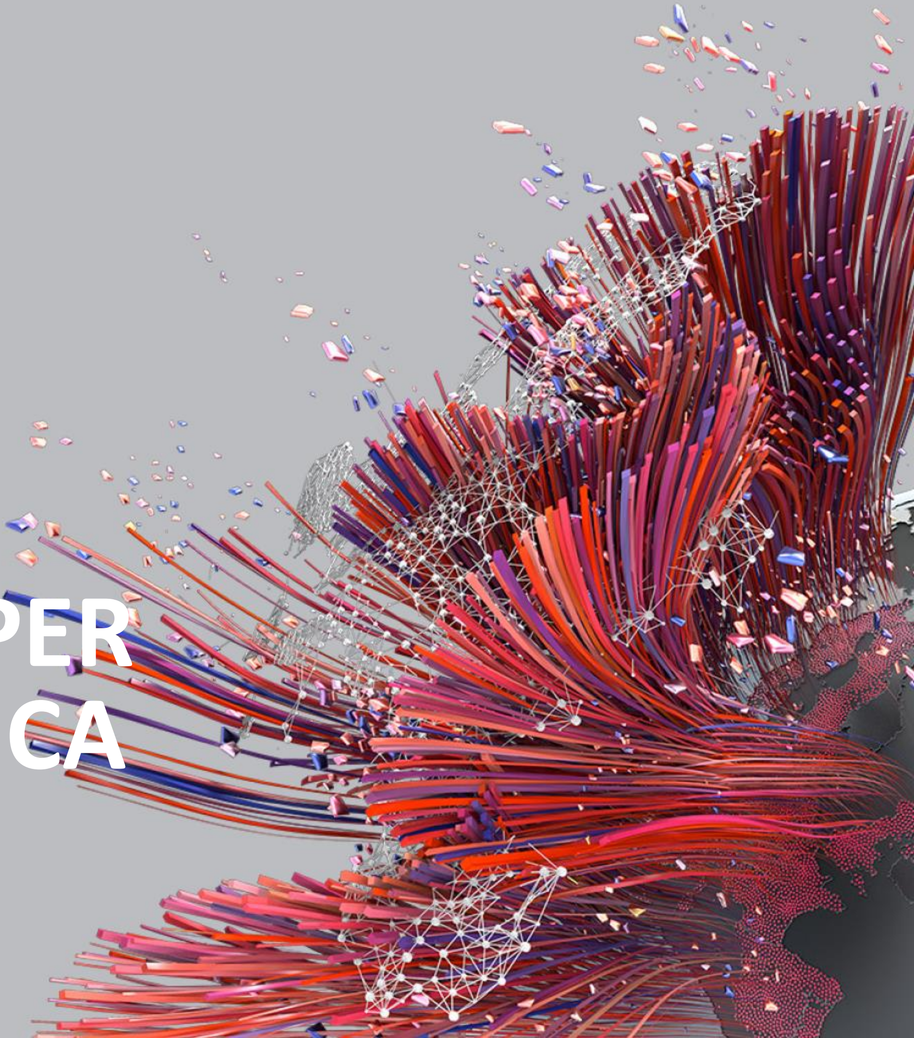
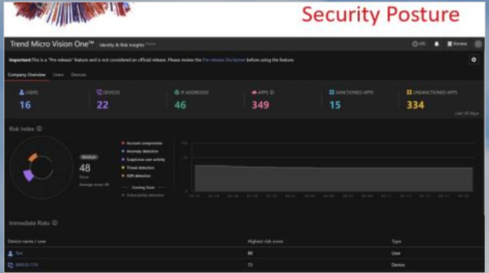
# IL VALORE DI UNA PIATTAFORMA XDR PER LA SICUREZZA OLISTICA

‘Non hai veramente capito qualcosa fino a quando non sei in grado di spiegarlo a tua nonna’ (A.Einstein)





Security Posture

Trend Micro Vision One™ Identity & Risk Insights Preview

Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

| USERS | DEVICES | IP ADDRESSES | APPS | SANCTIONED APPS | UNSANCTIONED APPS |
|---|---|---|---|---|---|
| 16 | 22 | 46 | 349 | 15 | 334 |

Last 30 days

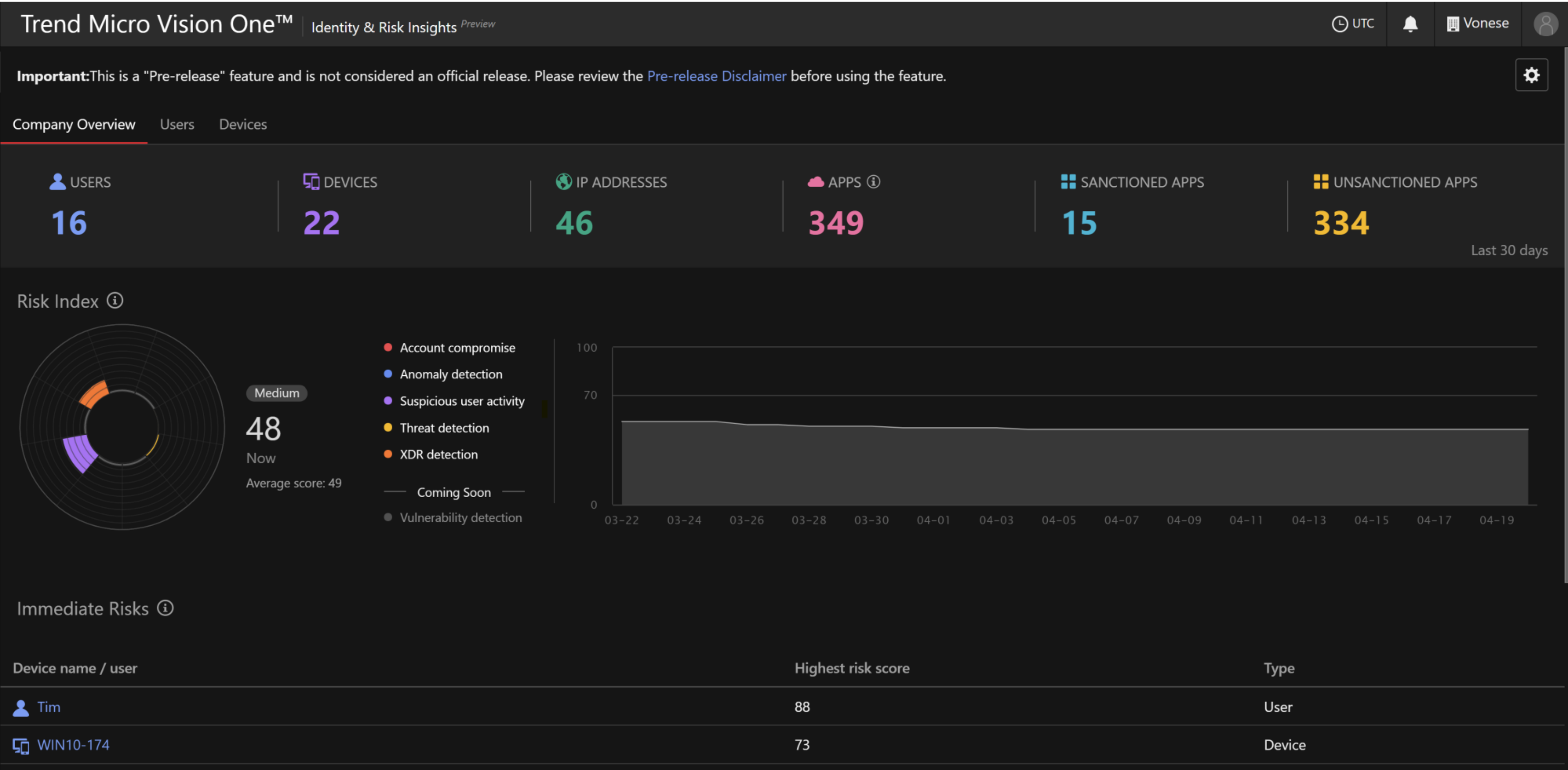
Risk Index

Immediate Risks

| Device name / user | Highest risk score | Type |
|---|---|---|
| [illegible] | 88 | User |
| [illegible] | 73 | Device |

# COME SIAMO MESSI?

# Security Posture



Trend Micro Vision One™ | Identity & Risk Insights *Preview*

UTC | Vonese

**Important:**This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

Company Overview | Users | Devices

| USERS | DEVICES | IP ADDRESSES | APPS ⓘ | SANCTIONED APPS | UNSANCTIONED APPS |
|---|---|---|---|---|---|
| 16 | 22 | 46 | 349 | 15 | 334 |

Last 30 days

Risk Index ⓘ

Medium

48

Now

Average score: 49

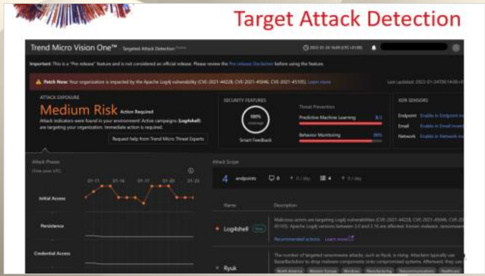
- ● Account compromise
- ● Anomaly detection
- ● Suspicious user activity
- ● Threat detection
- ● XDR detection

Coming Soon

- ● Vulnerability detection

Immediate Risks ⓘ

| Device name / user | Highest risk score | Type |
|---|---|---|
| Tim | 88 | User |
| WIN10-174 | 73 | Device |



## Target Attack Detection

Trend Micro Vision One™ Targeted Attack Detection Preview

2022-01-24 16:09 (UTC+01:00) [redacted]

Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

⚠ Patch Now: Your organization is impacted by the Apache Log4j vulnerability (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105). Learn more

Last updated: 2022-01-24T00:14:06+0

ATTACK EXPOSURE

Medium Risk Action Required

Attack indicators were found in your environment! Active campaigns (Log4shell) are targeting your organization. Immediate action is required.

Request help from Trend Micro Threat Experts

SECURITY FEATURES

100% Coverage

Smart Feedback

Threat Prevention

Predictive Machine Learning 3/3

Behavior Monitoring 90%

XDR SENSORS

Endpoint Enable in Endpoint in

Email Enable in Email inven

Network Enable in Network inv

Attack Phases

(Time zone: UTC)

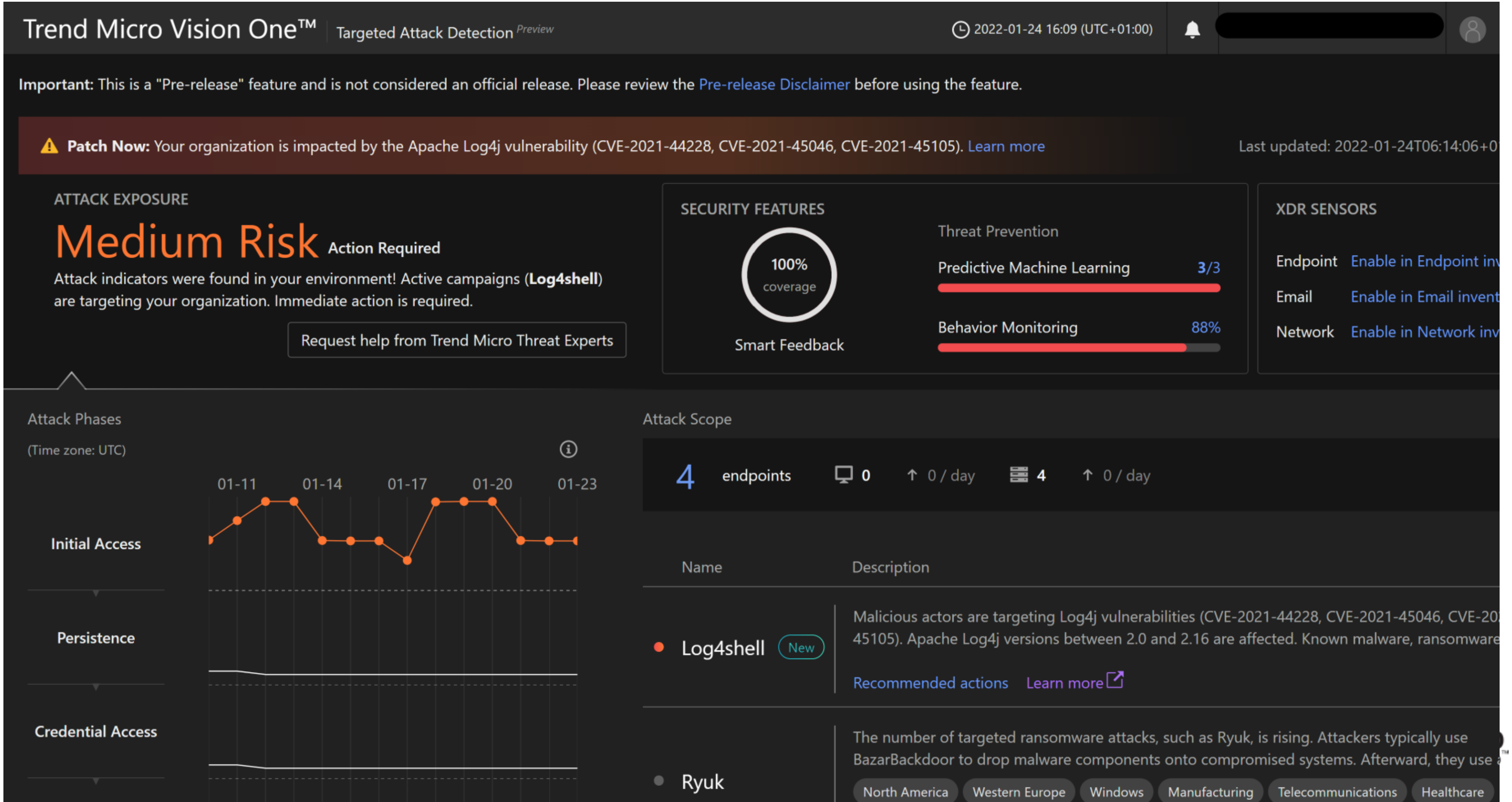
Attack Scope

4 endpoints 0 ↑ 0 / day 4 ↑ 0 / day

| Name | Description |
|---|---|
| Log4shell New | Malicious actors are targeting Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-20 45105). Apache Log4j versions between 2.0 and 2.16 are affected. Known malware: ransomware<br>Recommended actions Learn more |
| Ryuk | The number of targeted ransomware attacks, such as Ryuk, is rising. Attackers typically use BazarBackdoor to drop malware components onto compromised systems. Afterward, they use<br>North America Western Europe Windows Manufacturing Telecommunications Healthcare |

# SAPERLO PRIMA

# Target Attack Detection



Trend Micro Vision One™ Targeted Attack Detection *Preview*

2022-01-24 16:09 (UTC+01:00) [redacted]

**Important:** This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

⚠ **Patch Now:** Your organization is impacted by the Apache Log4j vulnerability (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105). Learn more

Last updated: 2022-01-24T06:14:06+0

ATTACK EXPOSURE

Medium Risk Action Required

Attack indicators were found in your environment! Active campaigns (**Log4shell**) are targeting your organization. Immediate action is required.

Request help from Trend Micro Threat Experts

SECURITY FEATURES

100% coverage

Smart Feedback

Threat Prevention

| | |
|---|---|
| Predictive Machine Learning | 3/3 |
| Behavior Monitoring | 88% |

XDR SENSORS

| | |
|---|---|
| Endpoint | Enable in Endpoint inv |
| Email | Enable in Email invent |
| Network | Enable in Network inv |

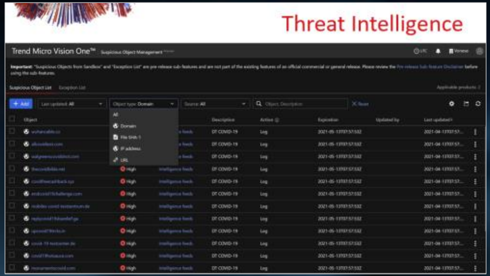
Attack Phases

(Time zone: UTC)

Attack Scope

4 endpoints 0 ↑ 0 / day 4 ↑ 0 / day

| Name | Description |
|---|---|
| ● Log4shell New | Malicious actors are targeting Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-20 45105). Apache Log4j versions between 2.0 and 2.16 are affected. Known malware, ransomware<br>Recommended actions Learn more |
| ● Ryuk | The number of targeted ransomware attacks, such as Ryuk, is rising. Attackers typically use BazarBackdoor to drop malware components onto compromised systems. Afterward, they use<br>North America Western Europe Windows Manufacturing Telecommunications Healthcare |



Threat Intelligence

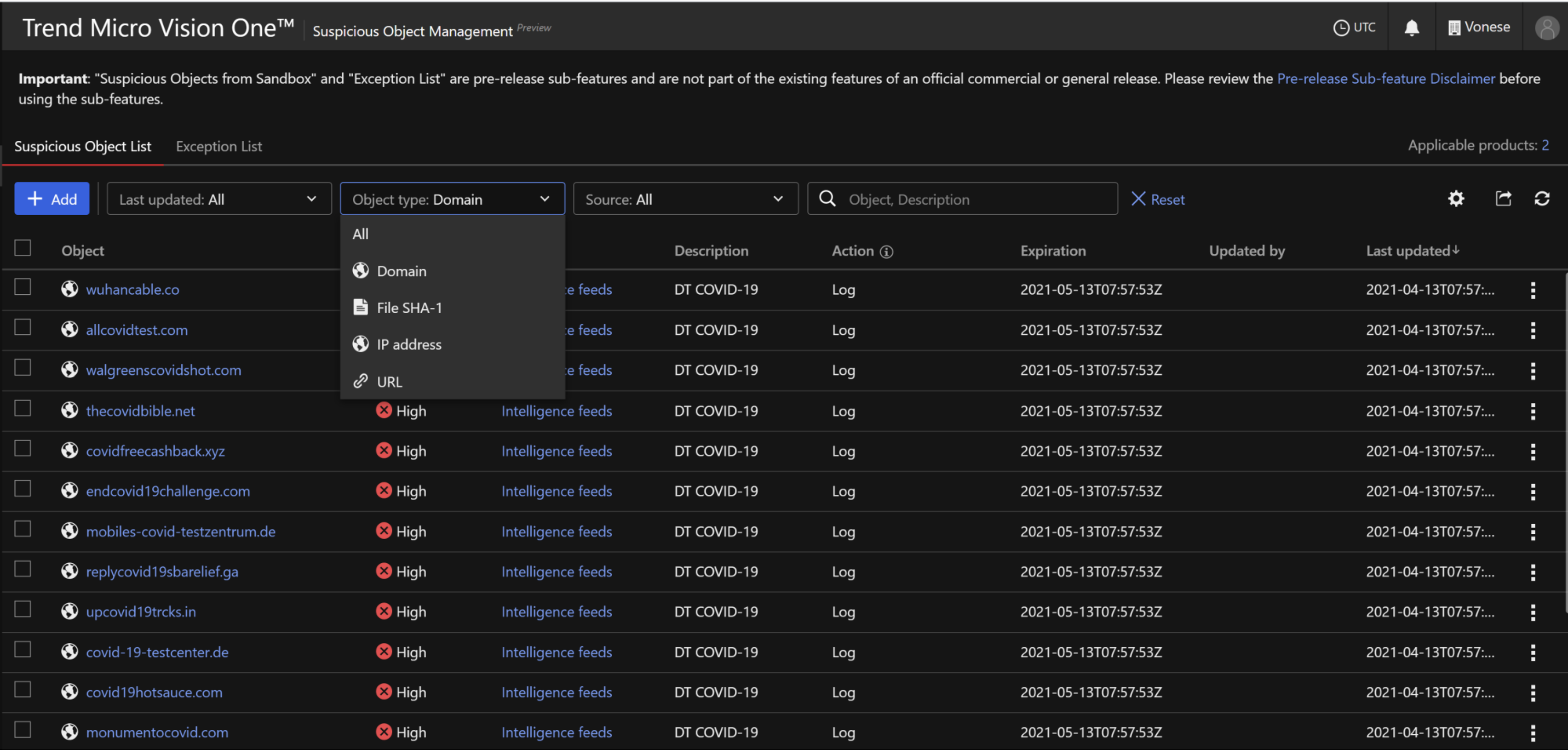
Trend Micro Vision One™ Suspicious Object Management

**Important:** "Suspicious Objects from Sandbox" and "Exception List" are pre-release sub-features and are not part of the existing features of an official commercial or general release. Please review the Pre-release Sub-feature Disclaimer before using the sub-features.

| Object | | | Description | Action | Expiration | Updated by | Last updated↑ |
|---|---|---|---|---|---|---|---|
| [illegible] | | [illegible] feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| allcovidtest.com | | [illegible] feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| walgreenscovidtest.com | | [illegible] feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| thecovidkids.net | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| covidfreecashback.xyz | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| endcovid19challenge.com | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| mobiles-covid-testzentrum.de | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| [illegible] | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| [illegible] | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| covid-19-testcenter.de | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| [illegible] | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |
| [illegible] | High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57... |

# USARE LE INFORMAZIONI

# Threat Intelligence



**Important**: "Suspicious Objects from Sandbox" and "Exception List" are pre-release sub-features and are not part of the existing features of an official commercial or general release. Please review the Pre-release Sub-feature Disclaimer before using the sub-features.

Last updated: All

Object type: Domain

Source: All

| Object | | | Description | Action ⓘ | Expiration | Updated by | Last updated↓ |
|---|---|---|---|---|---|---|---|
| wuhancable.co | | e feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| allcovidtest.com | | e feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| walgreenscovidshot.com | | e feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| thecovidbible.net | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| covidfreecashback.xyz | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| endcovid19challenge.com | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| mobiles-covid-testzentrum.de | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| replycovid19sbarelief.ga | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| upcovid19trcks.in | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| covid-19-testcenter.de | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| covid19hotsauce.com | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |
| monumentocovid.com | ☒ High | Intelligence feeds | DT COVID-19 | Log | 2021-05-13T07:57:53Z | | 2021-04-13T07:57:... |

XDR

Trend Micro Vision One™ Workbench > WB-10253-20210105-0006

Summary

[Threat Hunting] Suspicious WMI Executing Local Or Remote Process

Suspicious WMI Executing Local Or Remote Process

Created 2021-01-05T15:45:57Z

Highlights

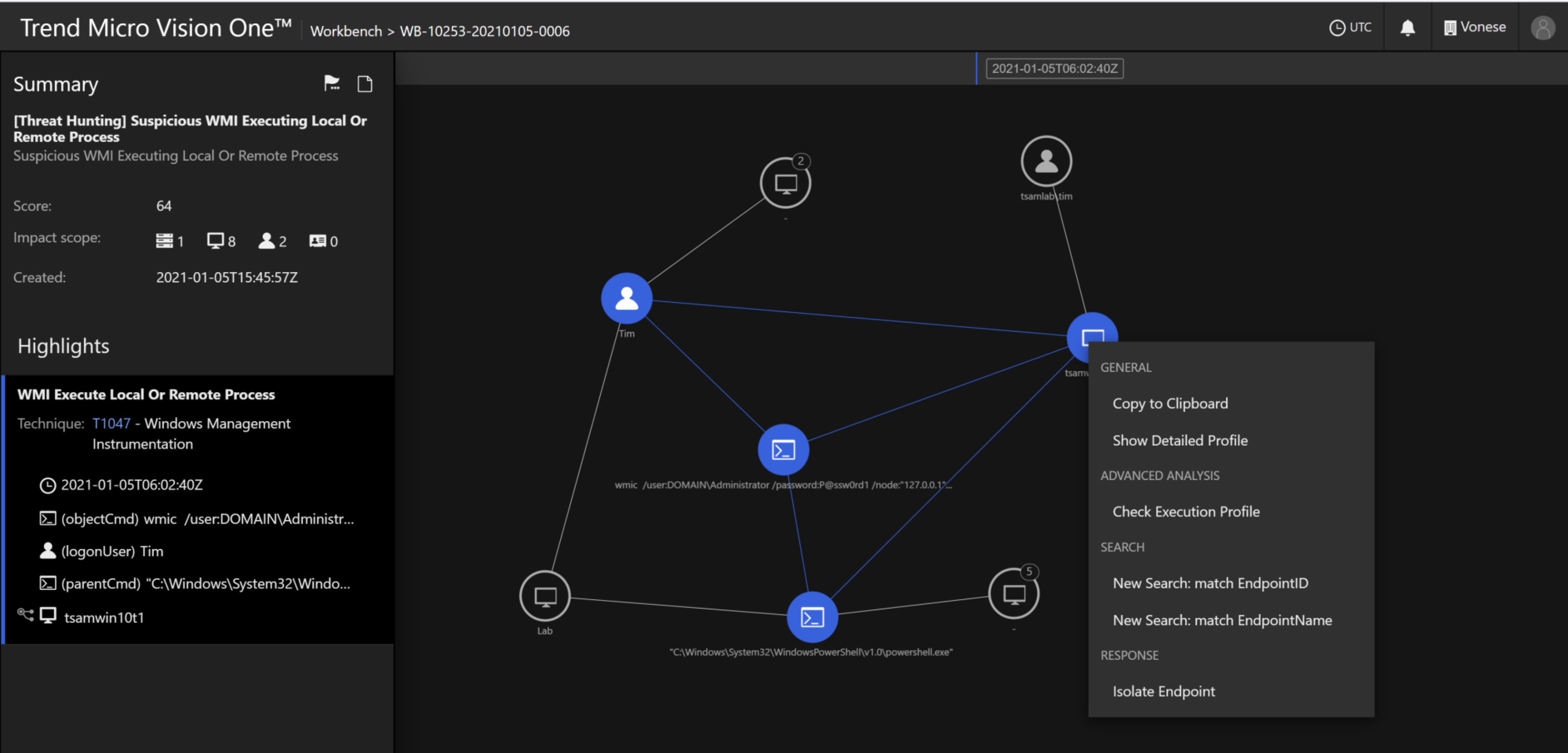
WMI Execute Local Or Remote Process

Technique T1047 - Windows Management Instrumentation

2021-01-05T06:02:40Z

# CAPIRE PER AGIRE

# XDR



Trend Micro Vision One™ | Workbench > WB-10253-20210105-0006

UTC | Vonese

## Summary

**[Threat Hunting] Suspicious WMI Executing Local Or Remote Process**
Suspicious WMI Executing Local Or Remote Process

Score: 64

Impact scope: 1 8 2 0

Created: 2021-01-05T15:45:57Z

## Highlights

**WMI Execute Local Or Remote Process**

Technique: T1047 - Windows Management Instrumentation

2021-01-05T06:02:40Z

(objectCmd) wmic /user:DOMAIN\Administr...

(logonUser) Tim

(parentCmd) "C:\Windows\System32\Windo...

tsamwin10t1

2021-01-05T06:02:40Z

wmic /user:DOMAIN\Administrator /password:P@ssw0rd1 /node:"127.0.0.1"...

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

# Trend Micro Vision One aiuta a …

- Percepire il reale livello di rischio
- Conoscere prima e meglio, per agire sicuri
- Integrare intelligenza per sapere di più
- Vedere oltre l’ovvio
- Essere pronti all’imprevisto (resilienza)

# THE ART OF CYBERSECURITY

The global shift of Trend Micro customers from on-premises to SaaS-based security. **Created with real data by artist Brendan Dawes.**