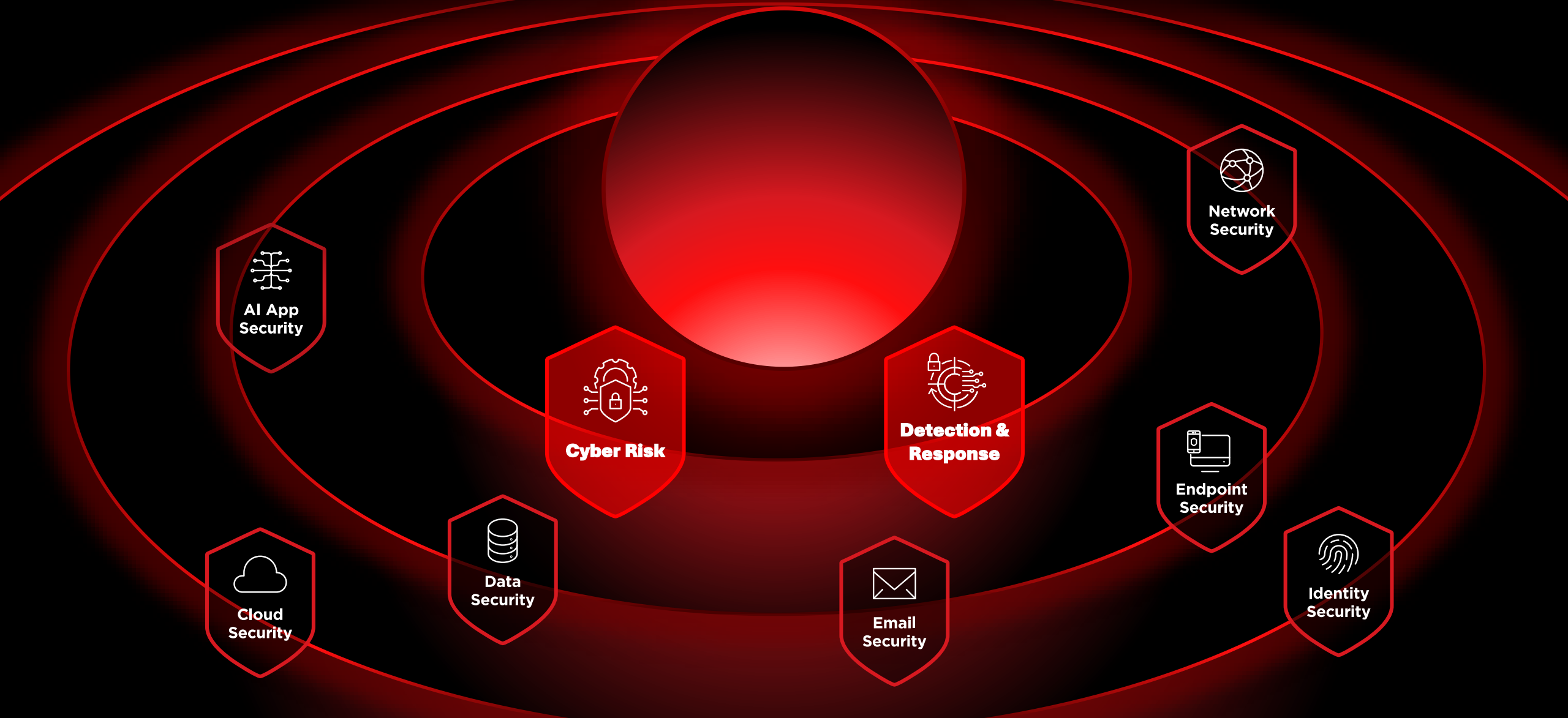




**Tři jednoduché kroky  
ke zvýšení bezpečnosti**

# Securing and governing every part of complex, dynamic environments



# Flexible platform

Customers can use  
**1 or all 11** solutions



Industry-Leading  
AI Security Platform





# Proaktivní analýza rizik

# Jak dnes provádíme hodnocení rizik?

## Risk Assessment Policy

January 2009

## Purpose

This policy is written in support of the Health & Safety Policy to help monitor and manage the Risk Assessments in place for Health and Safety. CMC (2015).

**Popillia (Stenocryptus)**

Healthwatch (Cambridgeshire) will comply with all legal requirements concerning the management of health and safety of their regulations 1998, which pose a legal requirement to make a written risk assessment for all HCA's, so as to determine what measures need to be taken to protect the health & safety of employees,<sup>1</sup> volunteers. These must be reviewed or regular if the risk, e.g. annually or immediately if circumstances change.

## 1. Introduction/Definition

- Under the Management of Health and Safety of Work Regulations 1999 (MHSW), the employer must make an assessment of risk to the health and safety of employees and others.
- The purpose of the assessment is to identify action necessary to comply with legal requirements, making suitable and sufficient assessments of risk, arrangements for the effective planning, organisation, control, monitoring and review of the preventive and protective measures.
  - Although the phrase 'risk assessment' may conjure up images of a complex process of judgement, based upon detailed technical knowledge, the assessment is in fact, nothing more than a careful examination of what the organisation does, and the way in which the organisation as a whole, its members, its staff, customers, its visitors and members of the public who may be harmed are offered by its activities.

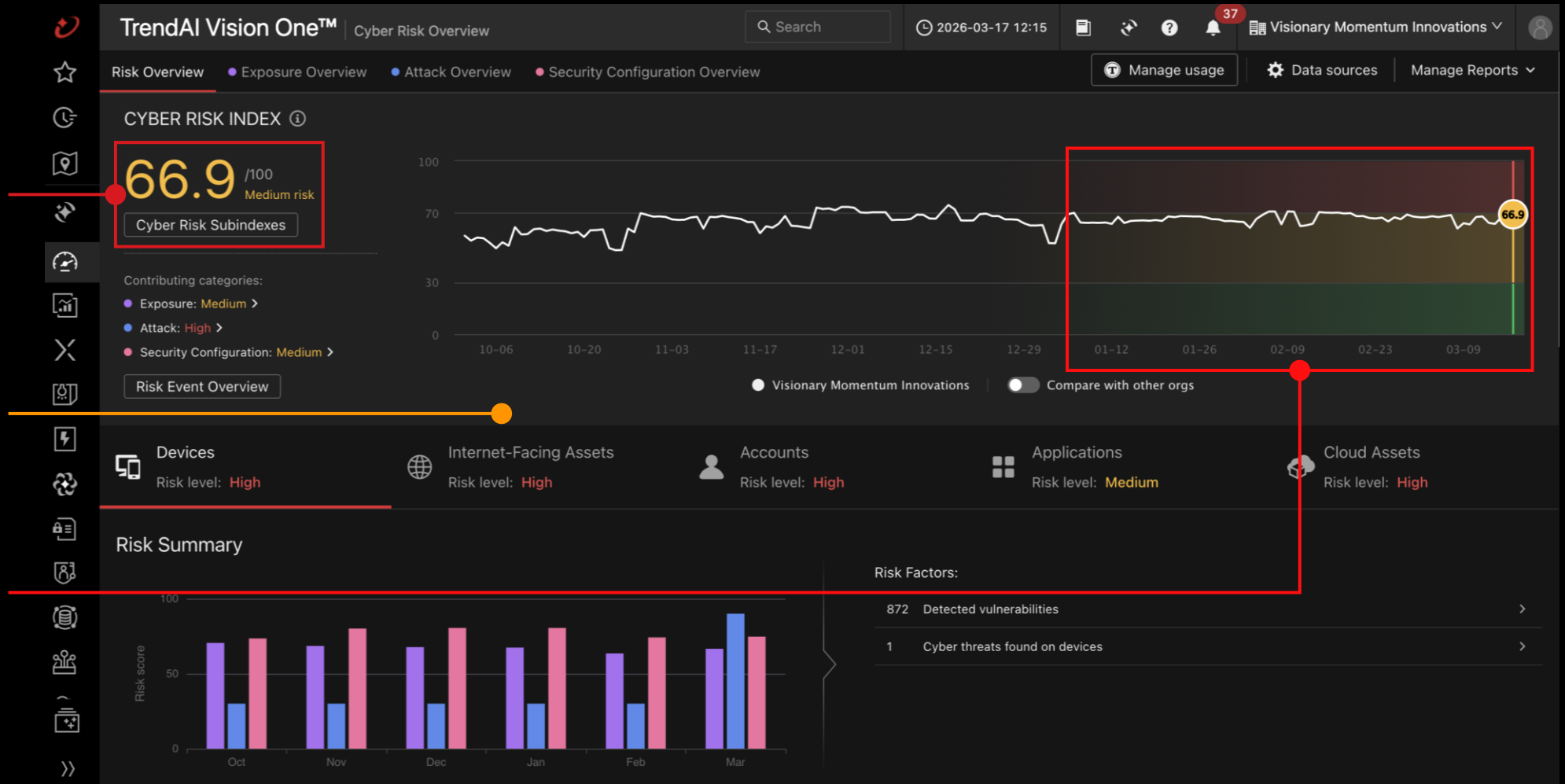
[illegible]

# One number. Nine risk factors. Real-time.

One score — built from 9 factors: vulnerabilities, identity risk, system configuration, active threats and more.

Updates in real time as your environment changes.

Trending view — the answer to “are we getting safer?”



# This Is What You Fix First — And Why.

Prioritized by actual risk in your environment — not generic CVE scores.

Factors in asset criticality, active threats, and exploitability.

Your team stops debating what to patch next.

TrendAI Vision One™ Threat and Exposure Management > Vulnerabilities

DETECTED VULNERABILITIES | Powered by Zero Day Initiative

Internal Assets | Internet-facing Assets | Containers | Cloud VMs *Preview* | Serverless Functions *Preview*

597 Total CVEs | 40 High impact CVEs (CVE impact score: 70-100) | 243 Medium impact CVEs (CVE impact score: 31-69) | 314 Low impact CVEs (CVE impact score: 0-30)

Group by: CVE event | Status: New | CVE ID | Add filter | Configure CVE Coverage | Import Third-Party Data | Export | Manage Reports

Vulnerability ID	CVE i...	Impact sco...	Prevention ...	Exploit a...	First seen time	Case
CVE-2023-27350	84	1	13	0	2024-03-22	0
CVE-2024-21412	84	1	12	0	2024-03-22	0
CVE-2024-38112	84	2	10	0	2024-07-12	0
CVE-2024-49138	84	2	0	0	2024-12-11	0
CVE-2025-33073	84	5	5	0	2025-06-14	0
CVE-2024-30088	83	2	0	0	2024-06-13	0
CVE-2024-49039	83	2	0	0	2024-11-19	1
CVE-2024-43451	81	2	4	0	2024-11-19	0
CVE-2024-29988	80	1	2	0	2024-04-12	0
CVE-2024-38193	80	2	0	0	2024-08-15	0
CVE-2026-3909	80	4	0	0	2026-03-15	0

Cyber Risk Exposure Management calculates impact scores for CVEs relative to the endpoints that they affect. The table displays the highest value among all the impact scores of a CVE for the specified impact scope. [Learn more.](#)

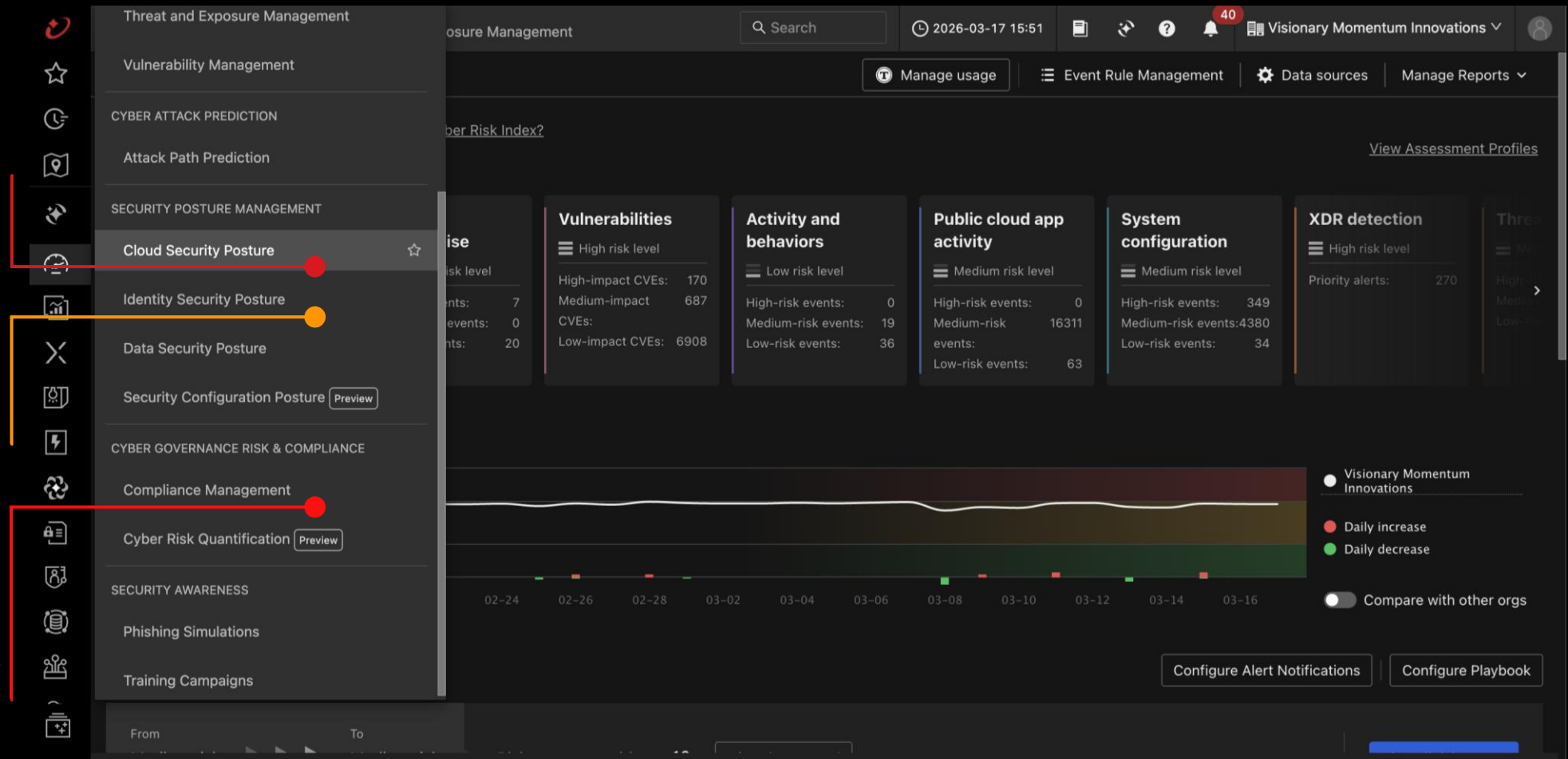


# Endpoints. Cloud. Identity. Compliance. One Platform.

Cloud Security Posture — misconfigurations and cloud risk, correlated with endpoint data.

Identity Security Posture — over-privileged accounts, stale credentials.

Compliance Management — NIS2, DORA, and 19+ frameworks. Already in your platform.





# Data

Regulations

Value

Sensitivity

Impact of disclosures

*Are you insured?*

# Your Business

Regulatory landscape

Financial state

Brand value

Private vs public

*Nature of business*

Attack History

Peers

Threat History

Attack Surface

# Risk Scoring

# CRQ

Cyber risk quantification

# CRQ

Cyber risk quantification

**Likelihood**  
**9-11%**

**Risk**  
**\$5.03M-6.14M**

The most probable outcome  
considering likelihood and impact

**Impact**  
**\$55.9M-97.3M**

Likeliest total monetary risk

**\$3.42M to \$41.46M** 0.34% to 4.15% of your annual revenue | Range: \$1.03M ~ \$67.08M

[Risk scenario settings](#)

High confidence Ransomware with data encryption

Likeliest total monetary risk

**\$3.42M**

0.34% of your annual revenue

Predicted event likelihood

**48%**

How likely your organization is to experience an event leading to loss

×

Predicted event impact

**\$7.65M**

Potential financial loss per event

High confidence Data exfiltration

Likeliest total monetary risk

**\$41.46M**

4.15% of your annual revenue

Predicted event likelihood

**64%**

How likely your organization is to experience an event leading to loss

×

Predicted event impact

**\$71.92M**

Potential financial loss per event

Quantified cyber risk over time



**Automatically Forecast Financial Impact**

- Spot high-risk areas at a glance
- Broken down by risk scenario
- Track risk reduction over time

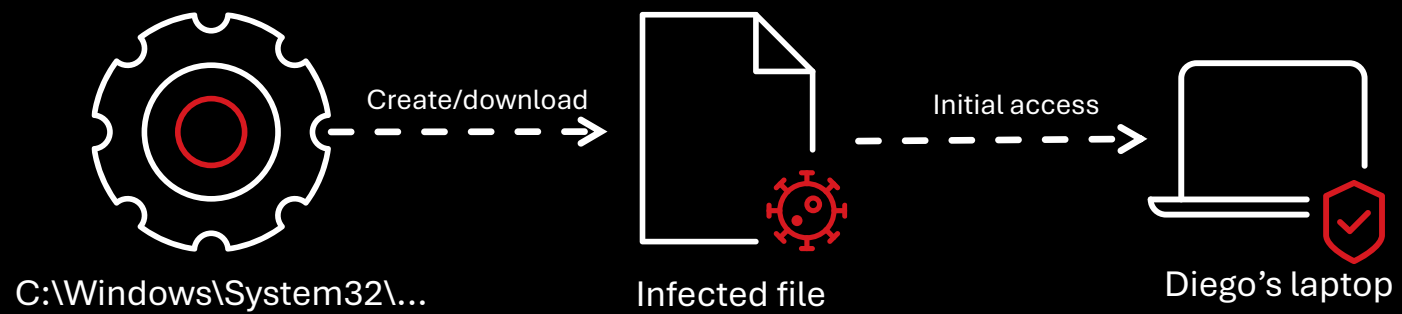
Control ID	Monetary risk reduction ↓	Reduction scope
<a href="#">Least Functionality (CM-07)</a> Disable unnecessary functions	\$5.67M 0.28% of annual revenue	Likelihood
<a href="#">Least Privilege (AC-06)</a> Grant minimal permissions	\$5.49M 0.27% of annual revenue	Likelihood
<a href="#">Account Management (AC-02)</a> Create and manage accounts	\$5.02M 0.25% of annual revenue	Likelihood
<a href="#">Information Fragmentation (SI-23)</a> Break up and distribute sensitive data	\$4.8M 0.24% of annual revenue	Impact
<a href="#">Distributed Processing and Storage (SC-36)</a> Spread workloads and data	\$4.4M 0.22%	
<a href="#">Software, Firmware, and Information Integrity (SI-07)</a> Verify integrity of software and data	\$4.31M 0.22%	
<a href="#">System Monitoring (SI-04)</a>	\$3.95M	Likelihood

#### Actionable Remediation Strategies

- See top recommended mitigation actions to strategically reduce your risk
- Tie each mitigation to reduced monetary risk



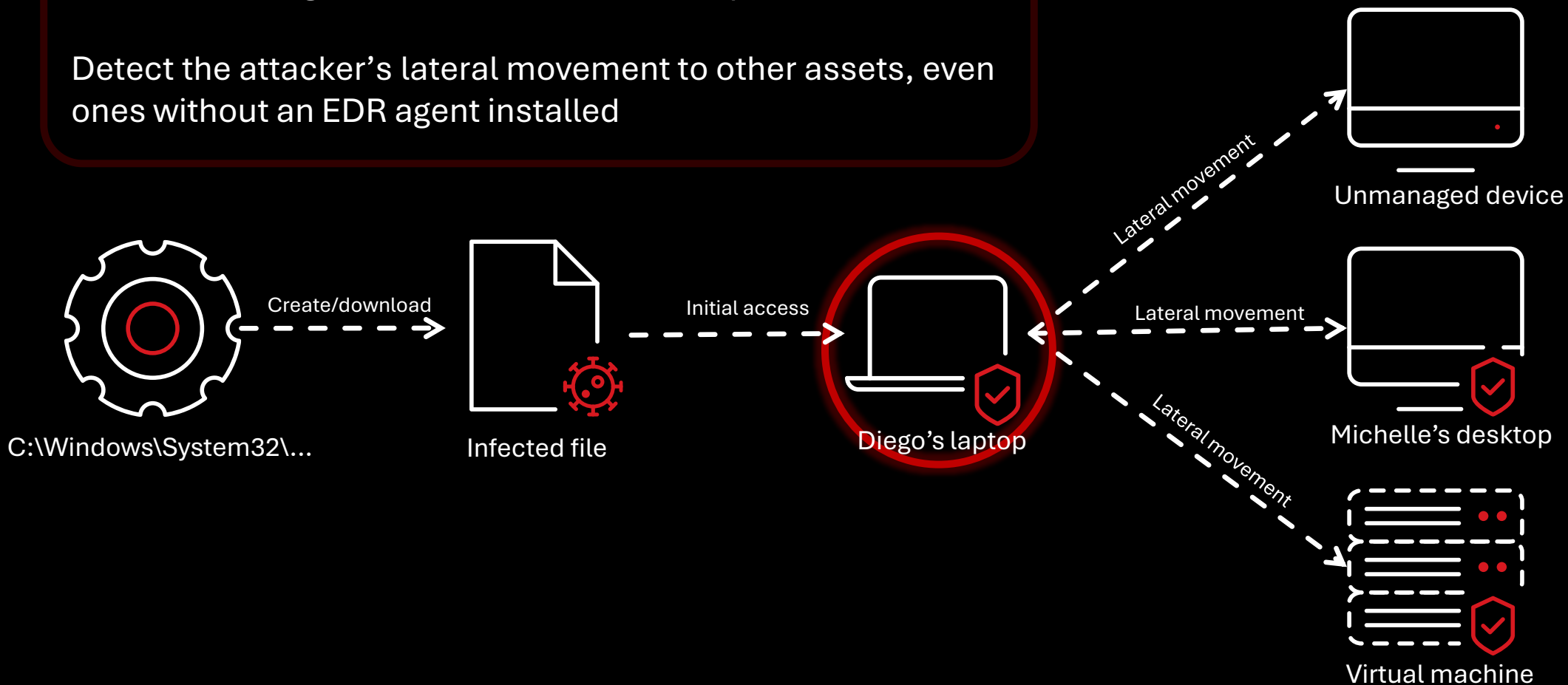
# Reakce na moderní hrozby



# Endpoint Detection and Response

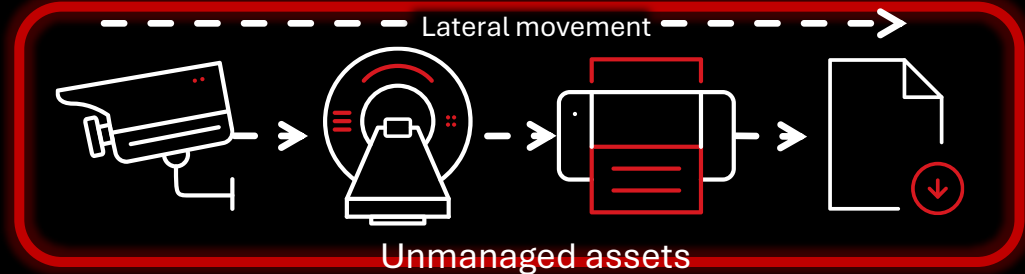
Detect that Diego's machine has been compromised

Detect the attacker's lateral movement to other assets, even ones without an EDR agent installed



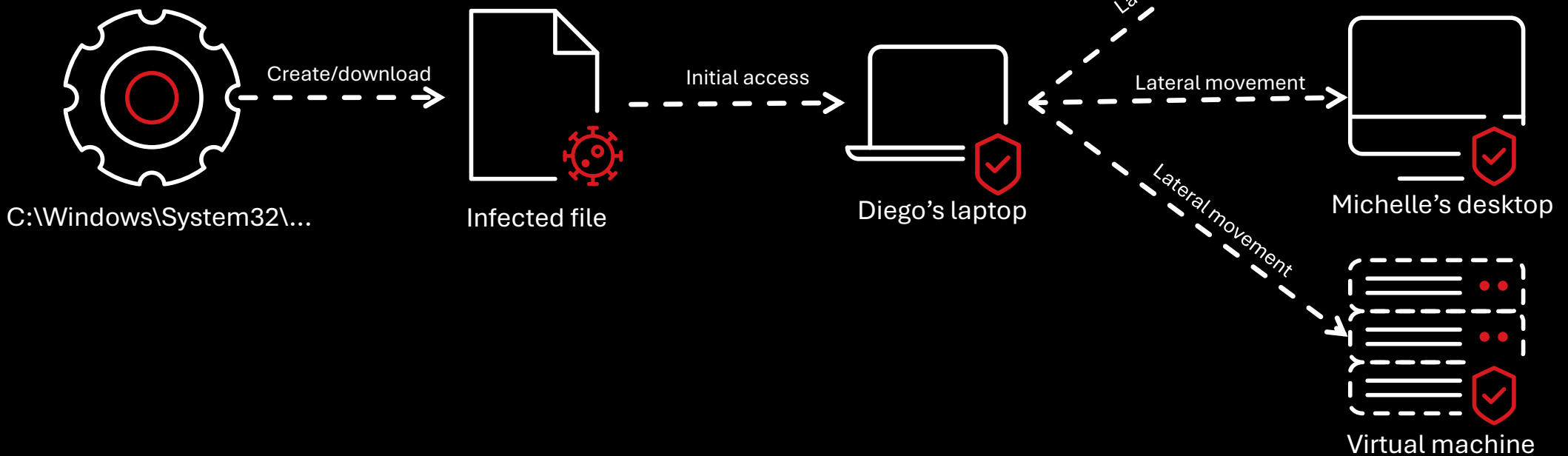


# Network Detection and Response

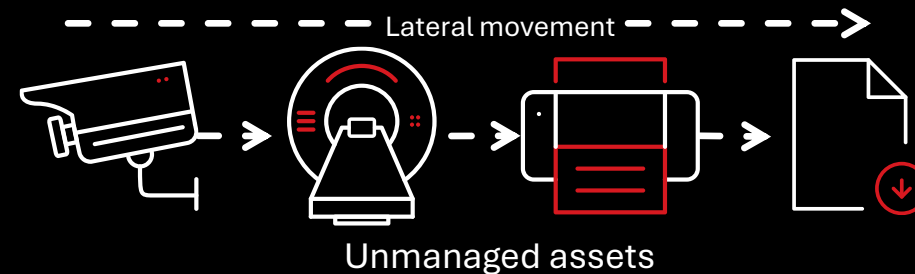


Not all assets have an agent installed

Detect the attacker's movements between unmanaged assets, and their C&C communication

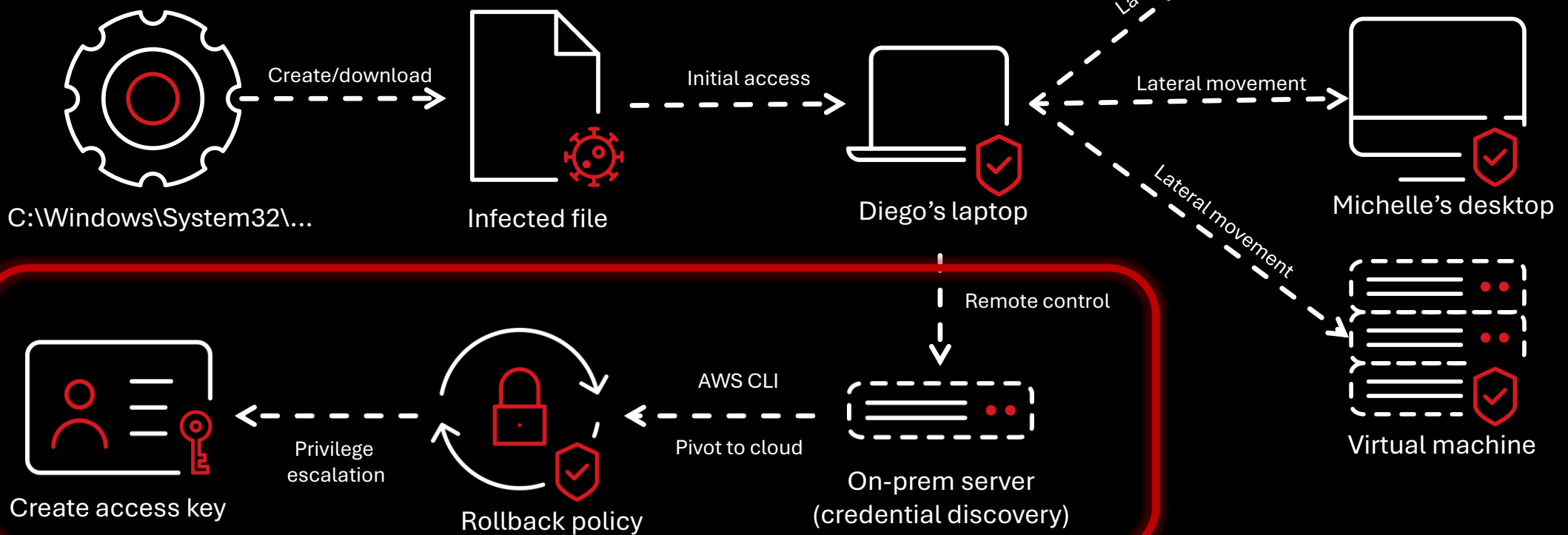


# Cloud Detection and Response



Attacker gets access to AWS credentials saved on the machine (AWS credential discovery)

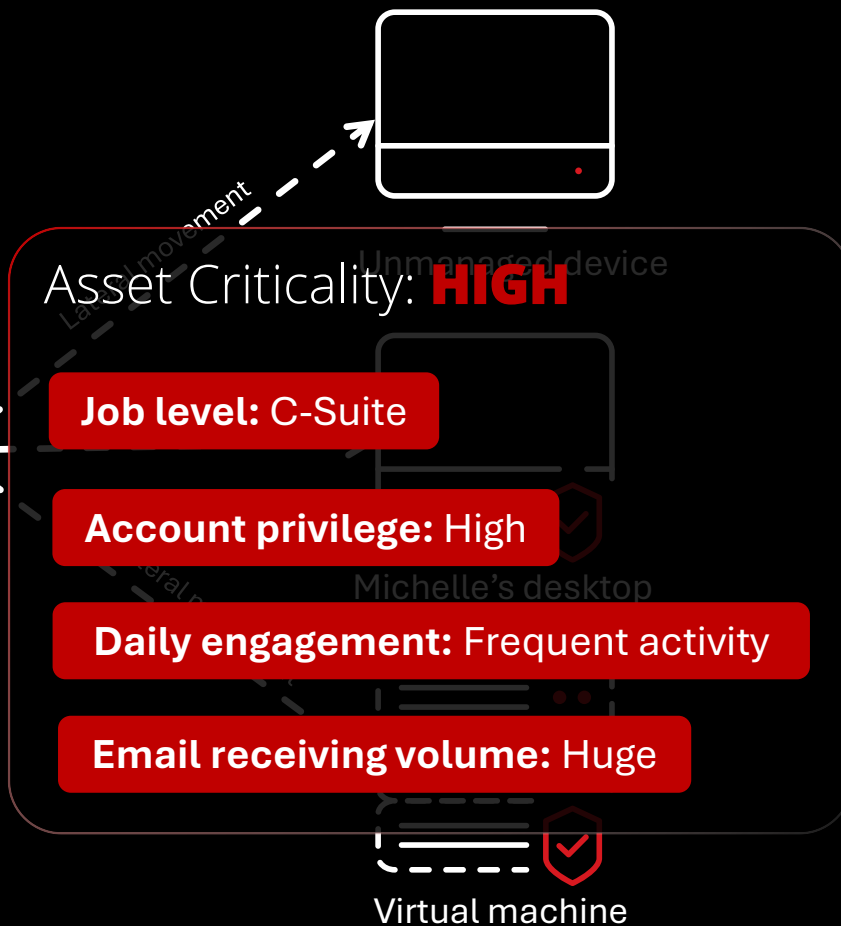
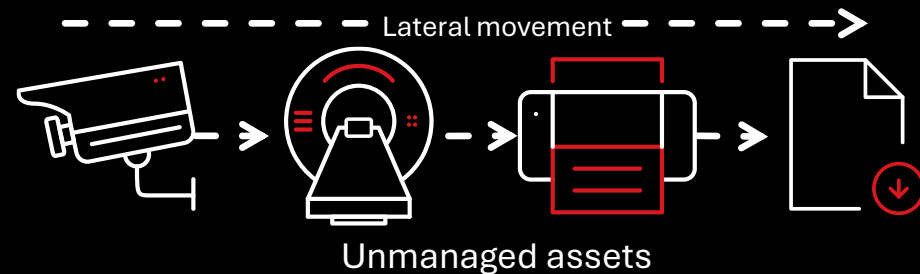
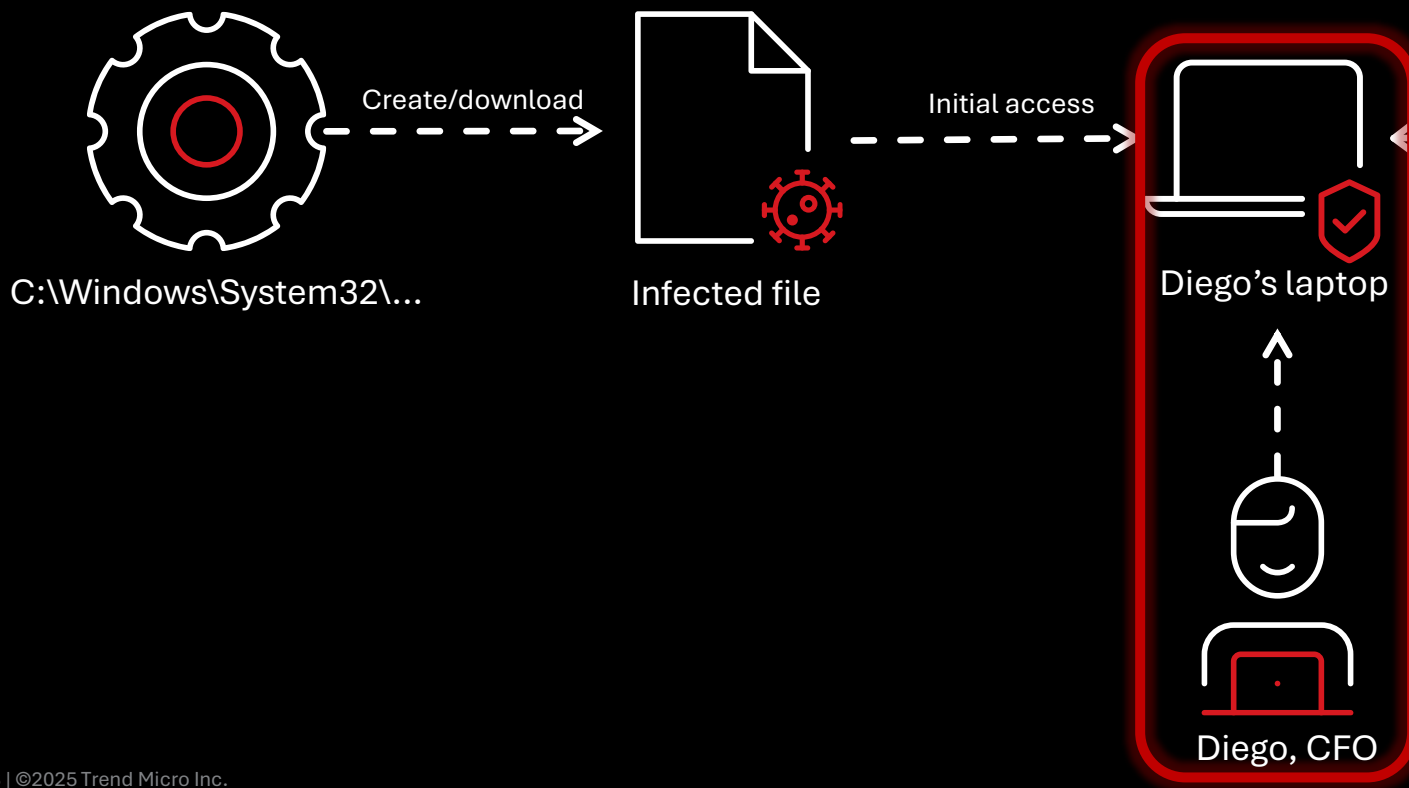
Attacker uses rolled back policy to generate access key



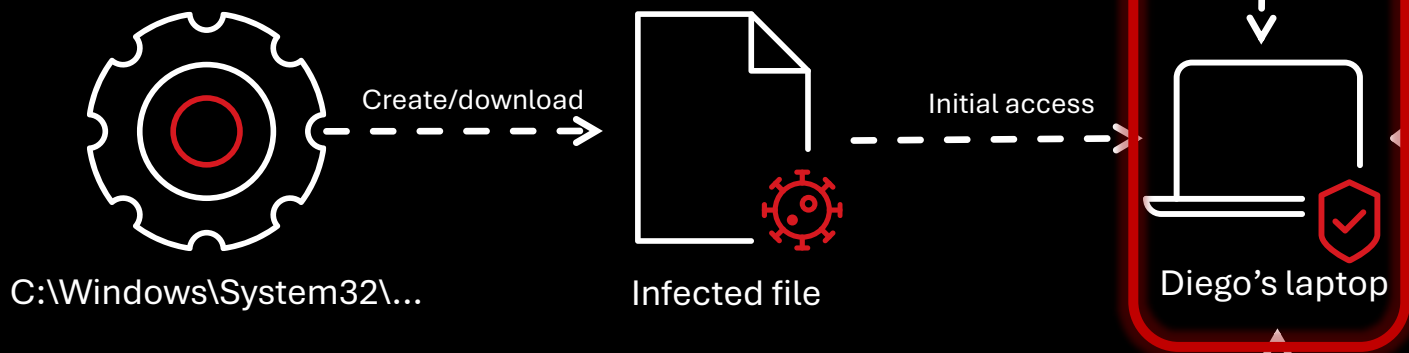
# Identity Threat Detection and Response

Detect whether a user has been compromised

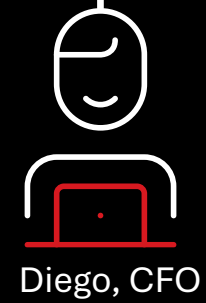
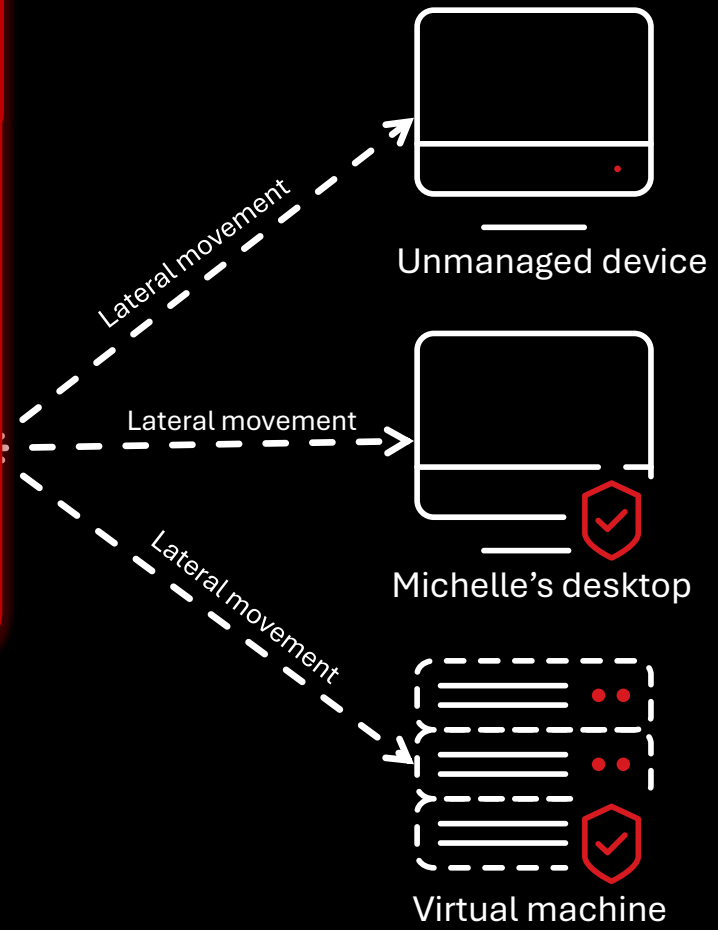
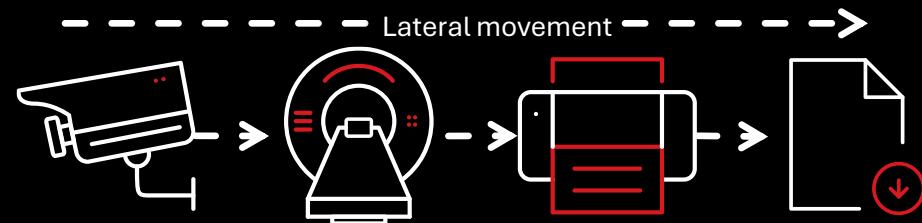
Without ITDR, we have no way of knowing that a high-profile user like Diego was compromised until it's too late...



# Email Detection and Response



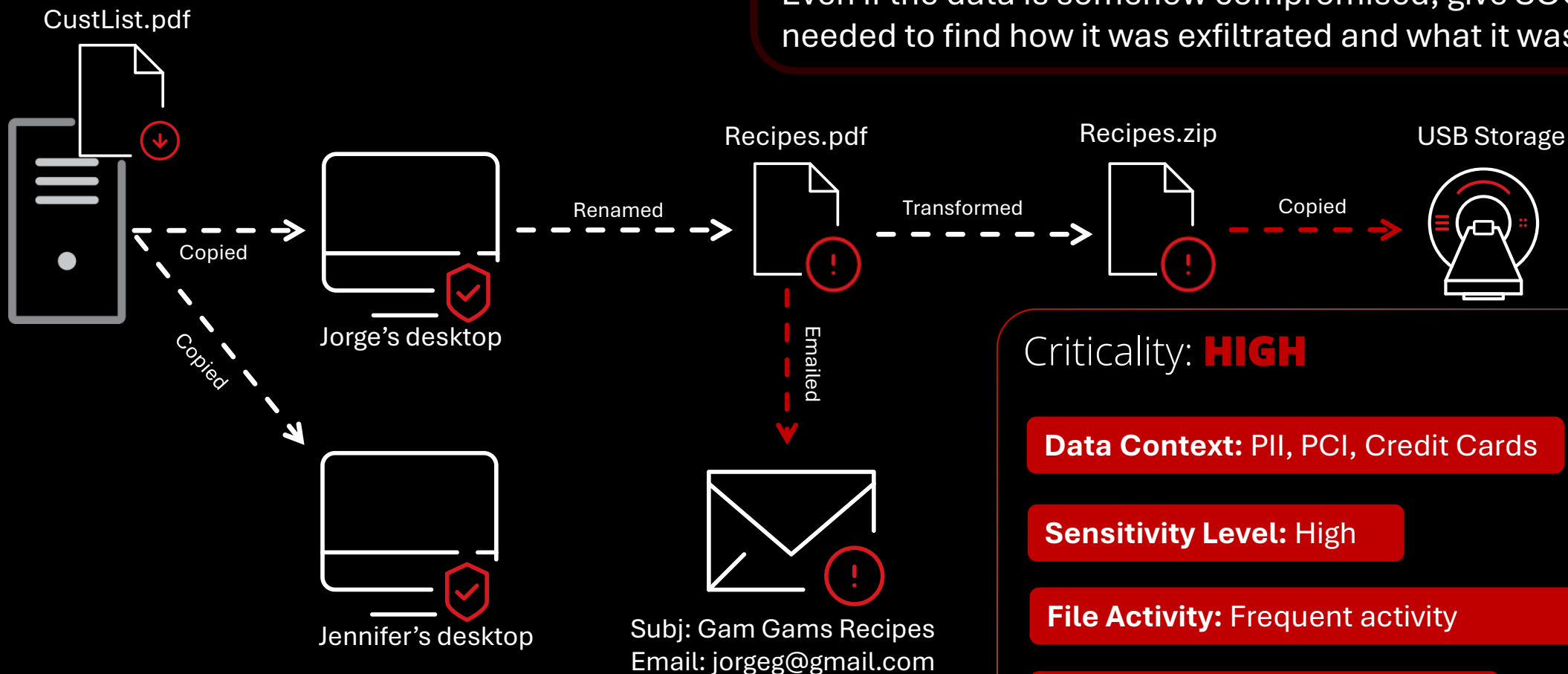
The initial infiltration was from a 3<sup>rd</sup> party webmail with a malicious payload attached



# Data Detection and Response

Gain visibility, context, and response to sensitive data as it moves throughout the environment

Even if the data is somehow compromised, give SOC the tools needed to find how it was exfiltrated and what it was before



Criticality: **HIGH**

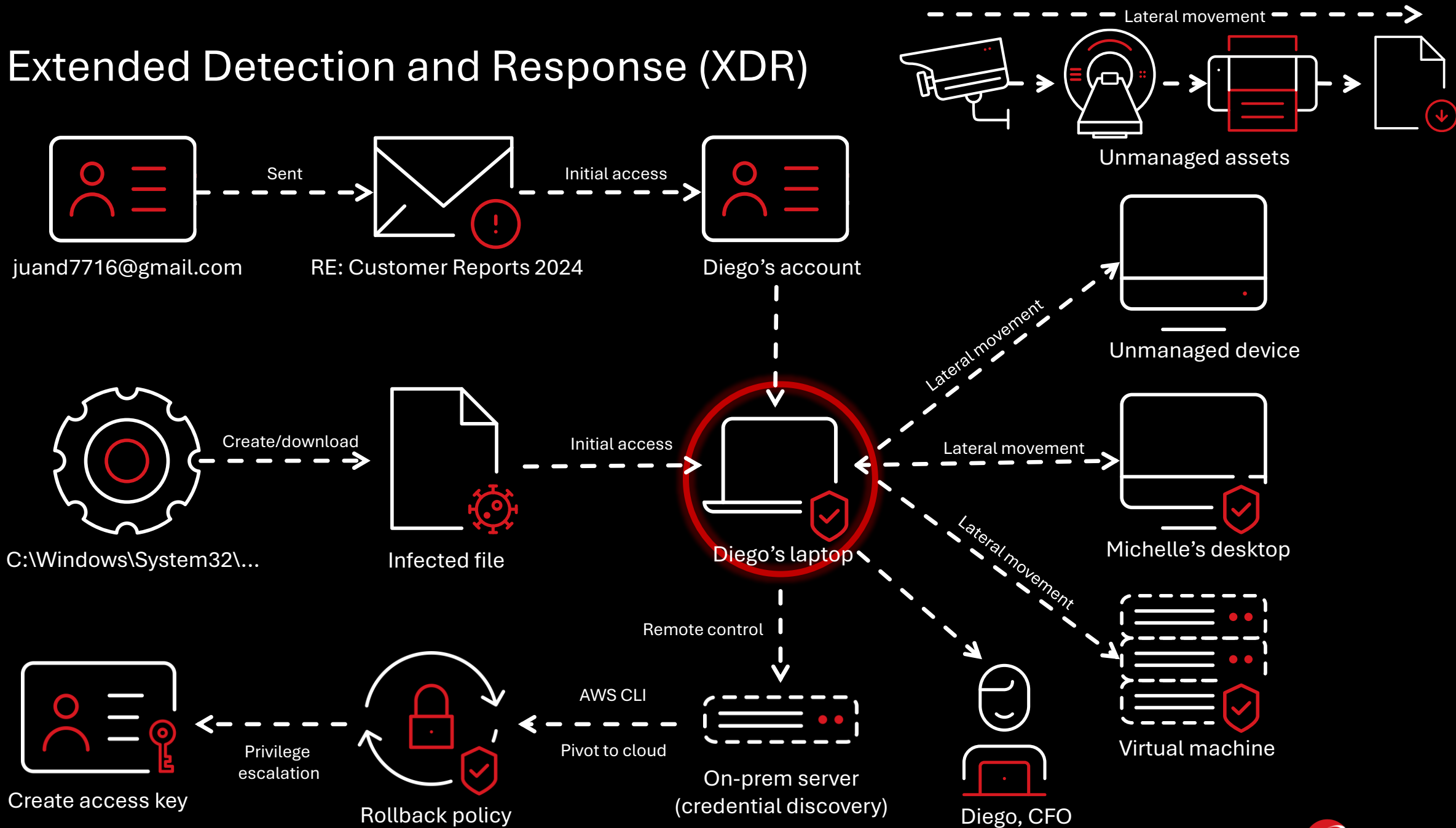
**Data Context:** PII, PCI, Credit Cards

**Sensitivity Level:** High

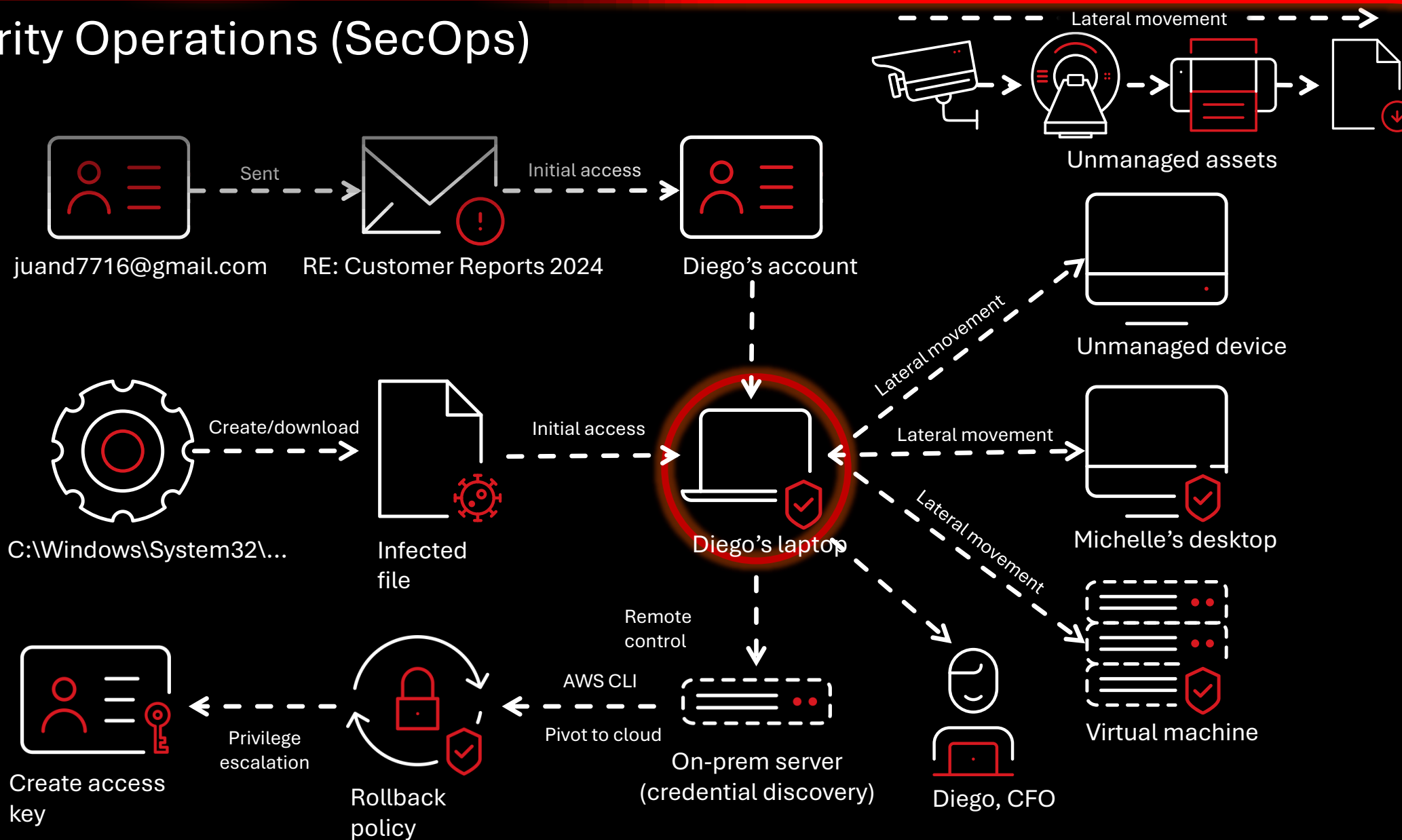
**File Activity:** Frequent activity

**Exfiltration Risk:** High

# Extended Detection and Response (XDR)



# Security Operations (SecOps)



+ Third-Party Telemetry



# Agentic SIEM: Two Data Types

## Analytic Data

**For detection and hunting**

**High security value**

**Analysis, correlation, and hunting**

**Can trigger XDR alerts, custom detections &  
Threat Intelligence sweeping**

## Archival Data

**For compliance and long-term retention**

**High volume logs**

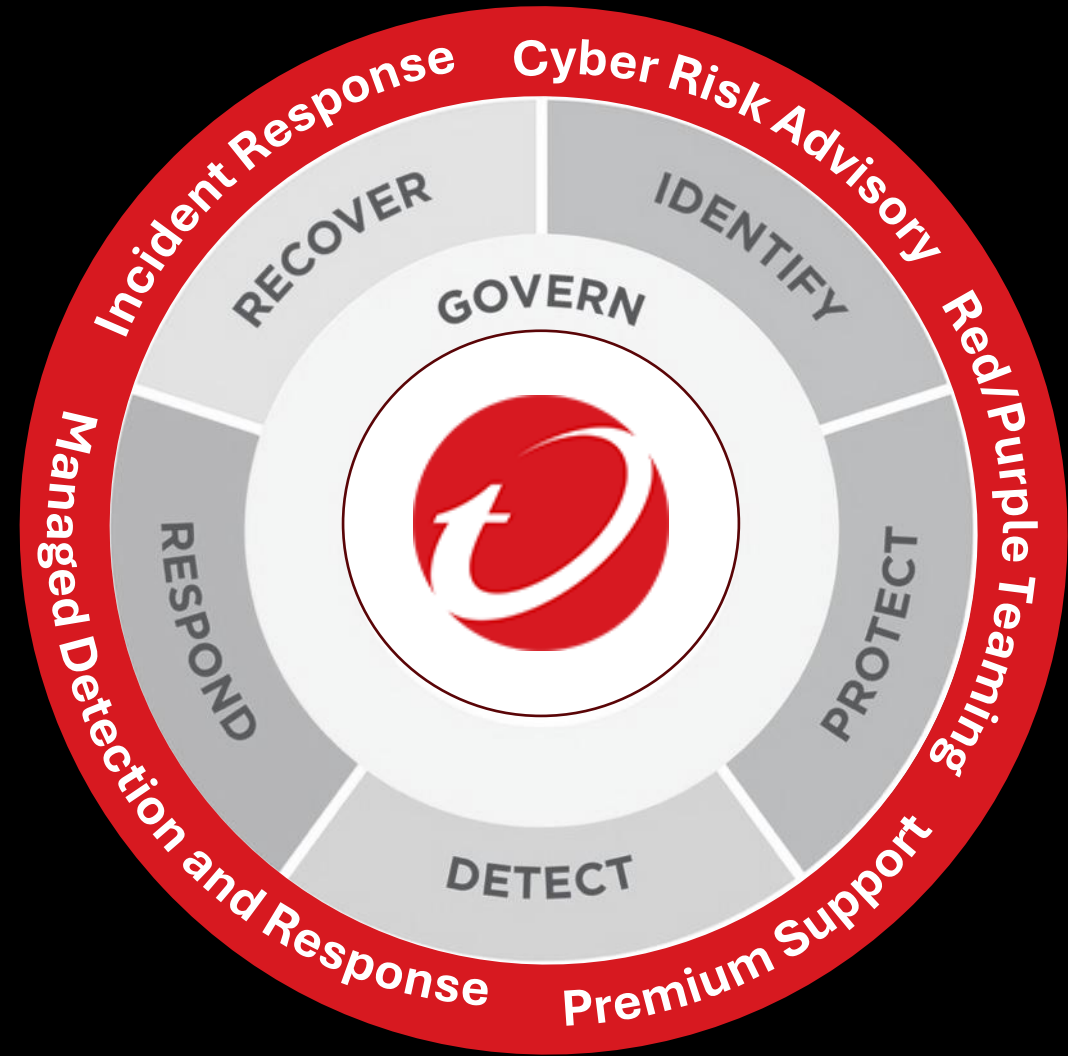
**Keyword search**

**No XDR alerts, custom detections, or Threat  
Intelligence sweeping**



**Bezpečnost jako  
služba**

# Trend Vision One™ Services



# Ukázka incidentu

- **13:56** Uživatel stáhl a nainstaloval „ChatGPT“ aplikaci
- **14:04** Na základě EDR dat a vytvořen první alert detekující sběr přihlašovacích údajů z prohlížeče (High Severity)
- **14:26** Provedena analýza podezřelých souborů analytikem (MDR)
- **14:33** Napadená stanice izolována na síti (response akce)
- **14:48** Zákazník dostává domluveným kanálem report o incidentu
- **14:53** Další sběr forenzních dat z napadené stanice pomocí skriptu

# Possible Credential Dumping from Web Browsers

Credentials stored in web browsers were accessed that could possibly be used to gain access to other systems. - WB-17 [REDACTED]

high Severity

## Investigation Notes

- Trend Micro Managed XDR observed a **NOTEWORTHY** Vision One alert with the model name Possible Credential Dumping from Web Browsers and Workbench ID WB-17 [REDACTED].
- Managed XDR investigated further by.
  - Checking Execution profile
    - It appears the user "[REDACTED]" executes the following C:\Users\[REDACTED]\AppData\Local\Temp\Temp1\_ChatGPT\_For\_Windows\_Setup\_1.0.0.zip\ChatGPT For Windows Setup 1.0.0.exe which leads to this chain of events
      - ChatGPT For Windows Setup 1.0.0.exe > drops C:\Users\[REDACTED]\AppData\Local\Programs\vbloks\resources\resource\ChatGPT Support.exe > steals credentials
        - Connects to the following IP address
          - 188.[REDACTED]:443
          - 157.[REDACTED]:443
          - 3.[REDACTED]:443
          - 157.[REDACTED]:443
          - 149.[REDACTED]:443









[Request List](#) [Reports](#) [Settings](#)

Status: All



Action: All



<input type="checkbox"/>	Status	Action	Target	Description	Request... ↓	Processed by	Processed
▼ 1	✅ Approved	Run Trend Micr...	 [Redacted]	MDR investigation o...	2023-03-06 ...	Auto approval	2023-03-06 ...
	Kit: Full Investigation						
▼ 1	✅ Approved	Run Custom Scr...	 [Redacted]	Check for persistenc...	2023-02-27 ...	Auto approval	2023-02-27 ...
	Script file: Collect-AutorunList.ps1 						
▶ 1	✅ Approved	Collect File	 ChatGPT_For_Windows_Setup_1.0....	Collected for further ...	2023-02-27 ...	Auto approval	2023-02-27 ...
▶ 1	✅ Approved	Collect File	 ChatGPTSupport.exe	Collected for further ...	2023-02-27 ...	Auto approval	2023-02-27 ...
	✅ Approved	Isolate Endpoint	 [Redacted]	Observed an executi...	2023-02-27 ...	Auto approval	2023-02-27 ...
▼ 1	✅ Approved	Collect File	 ChatGPT For Windows.exe	Collected for furthes ...	2023-02-27 ...	Auto approval	2023-02-27 ...
	Endpoint: [Redacted]			File path: C:\Users\[Redacted]\AppData\Local\Programs\vbloks\ChatGPT For			
▼ 1	✅ Approved	Collect File	 ChatGPTSupport.exe	Collected for further ...	2023-02-27 ...	Auto approval	2023-02-27 ...
	Endpoint: [Redacted]			File path: C:\Users\[Redacted]\AppData\Local\Programs\vbloks\resources\resource\C			

# Děkuji

Filip Marvan

[filip\\_marvan@trendmicro.com](mailto:filip_marvan@trendmicro.com)

