FOUNDATIONS AND ADVANCEMENTS IN CYBERSECURITY: LEVERAGING XDR FOR MONITORING AND INCIDENT RESPONSE

An Internship-Based Evaluation of Extended Detection and Response in Modern Security.

Trend Micro Internship

Paarth Pandey
paarthdxb@gmail.com

9th June 2025
Monday
Dubai, UAE.

Table of Contents

Abstract

This whitepaper outlines the hands-on cybersecurity training and lab experience undertaken during a short-term internship at Trend Micro (22nd May – 4th June 2025). The internship involved expert-led sessions on cybersecurity domains, guided labs using Trend Micro Vision One, and a final project simulating and detecting a credential dumping attack. This experience emphasized real-world applications of XDR platforms in detecting sophisticated adversarial techniques such as memory scraping and privilege escalation, leveraging MITRE ATT&CK and telemetry analysis.

Introduction

Credential dumping is a common technique in post-exploitation phases of cyberattacks, where adversaries extract sensitive account credentials from a system's memory.

Tools like Mimikatz allow attackers to retrieve passwords, hashes, and Kerberos tickets—enabling lateral movement and privilege escalation.

This whitepaper captures the practical implementation and detection of such an attack using Trend Micro Vision One, a cloud-native XDR platform.

Through a guided simulation, the platform's advanced telemetry, correlation engine, and integrated threat intelligence were leveraged to investigate and contain the attack.

Internship Activities Overview

The internship began with multiple instructor-led sessions (via Microsoft Teams) on key cybersecurity topics, including:

- Cloud Workload Security Threat Landscape Overview
- Introduction to Vision One (XDR)
- Endpoint, Server, Cloud & Network Security (including IDS/IPS, firewalls)
- Zero Trust Security Architecture
- Risk Analytics and Attack Surface Management
- AI in Cybersecurity
- Security for AI

Following this, interns were given access to the Trend Vision One XDR Lab Guide v2.5, a simulated environment delivered through the Trend Micro Product Cloud. The guide included structured labs such as endpoint sensor deployment, policy creation, incident detection, and security playbook automation.

Finally, a group project was presented on DNS Covert Communication (theoretical), followed by a credential dumping demo executed and detected in real-time using Vision One.

Lab Tools and Setup

- VirtualBox – Hypervisor for lab VM environment
- Windows 10 VM – Target for simulated attack Trend Micro
- Vision One Console – Used for detection, telemetry, and response
- PowerShell / CMD – Used for downloading and running Mimikatz
- Trend Micro Endpoint Sensor – Installed to monitor and forward telemetry from Windows client
- Trend Micro Server & Workload Protection Agent – Installed to monitor and forward telemetry from Ubuntu Server

Credential Dumping Simulation and Attack Timeline

A credential dumping attack was simulated using Mimikatz on a Windows 10 virtual machine (DESKTOP-C1M3ICF).

The attacker executed typical behaviors including:

- Downloading Mimikatz via PowerShell Disabling Windows Defender using Set-MpPreference
- Executing Mimikatz to access LSASS memory
- Loading potentially vulnerable drivers

All activities were continuously monitored by Trend Micro Vision One, which correlated them into a single attack incident with a high-risk score of 85.

Detailed Attack Chain and Detection (Vision One Workbench)

The attack was visualized via the Workbench feature of Vision One. It grouped all associated behaviors into one threat scenario with visual graph mapping.

Key highlights from the detection:

MITRE ATT&CK Techniques Detected

Technique ID	Description
T1003	OS Credential Dumping
T1003.001	LSASS Memory Dumping
T1059.003	Windows Command Shell
T1562.001	Disabling Windows Defender
T1543.003	Malicious Driver Creation (Persistence)
T1105	Ingress Tool Transfer
T1212	Exploitation for Credential Access

Detailed Attack Chain and Detection (Vision One Workbench)

Notable Indicators:

Tool used: Mimikatz

Mapped Threat Actor: Turla

High severity alerts from Endpoint Sensor telemetry

Command execution via PowerShell

Disabling of Windows Defender (detected multiple times) D

river loading and credential scraping attempts

Vision One linked all steps under a single correlated incident

Detection and Response in Trend Micro Vision One

Trend Micro Vision One’s XDR capabilities effectively:

- Mapped the full execution chain
- Detected credential access attempts and defense evasion
- Showed MITRE technique mapping
- Assigned a risk score of 85 (high priority)
- Enabled remote response actions:
- Isolate endpoint
- Start remote shell
- Submit malicious file for sandboxing
- Add file to blocklist
- Execute security playbooks

The graph-based Workbench view helped visualize affected processes, users, and systems, significantly speeding up investigation time.

Findings and Conclusion

This internship simulation proved that Trend Micro Vision One can effectively detect and respond to credential theft and post-exploitation activities.

It validated how telemetry, threat intelligence, and MITRE ATT&CK mapping together provide deep visibility into attacker behavior.

The experience strengthened practical understanding of both red teaming techniques and blue team detection strategies using modern security platforms.

Future Scope

Future projects and research can extend this work by:

- Simulating other MITRE techniques (e.g., lateral movement, persistence)
- Applying Vision One's AI-based anomaly detection.
- Comparing XDR detections with traditional SIEM platforms.
- Integrating cloud-based workloads, Linux systems, and mobile endpoints.
- Automating responses using playbooks and SOAR workflows.

Glossary of Key Cybersecurity Concepts Learned

During the internship, the following critical cybersecurity terms and tools were explored:

Threat & Defense Models:

- MITRE ATT&CK – Global open-source database of adversary techniques
- Cyber Kill Chain – 7-phase model of attack lifecycle
- Lateral Movement – Movement across network post-compromise
- Caldera – MITRE's red team simulation tool
- CVEs – Publicly disclosed software vulnerabilities

Platforms and Tools:

- Trend Micro Vision One – XDR platform
- Service Gateway (SG) – Proxy for agents; reduces Vision One bandwidth
- Endpoint Basecamp – Deploys sensors and risk telemetry
- SPN (Smart Protection Network) – Cloud-based content filtering
- Active Update – Automatic pattern and engine updates

Glossary of Key Cybersecurity Concepts Learned

Threat Intelligence:

- TAXII – Threat intelligence transport mechanism
- STIX – Structure for threat intelligence content
- MISP – Malware Information Sharing Platform
- SOs – Suspicious objects detected and shared

Monitoring and Detection:

- EDR, XDR, NDR, CDR – Detection platforms at various levels
- IPS/IDS, NGFWs – Network-level prevention and detection
- Web Sensors – Part of IDS/IPS ecosystem

Firewalls & Infrastructure:

- Firewall types: Network-based, Host-based, NGFW, WAF, Cloud Firewall
- Firewall placement: Internet edge, DMZ, internal segments

Systems & Environments:

- Active Directory & Azure AD – Identity management systems
- OpenLDAP – Open-source directory protocol
- Cloud Sandbox – Isolated analysis of suspicious files

- Containers – Lightweight virtual environments

Data & Analysis:

- Data Lake – Centralized repository for storing structured and unstructured data from multiple sources
- Telemetry – Real-time security data collected from endpoints and infrastructure
- Correlation Engine – Analyzes patterns and links indicators across data streams
- Risk Score – Numerical rating based on the severity and confidence of detection
- Indicators of Compromise (IOCs) – Data points like IPs, file hashes, domains used to detect threats
- Indicators of Attack (IOAs) – Behavioral signals pointing to intent or action, not just presence

Personal Reflection

This internship was a pivotal learning experience in my early cybersecurity journey. It bridged theoretical understanding with industry-grade practical exposure. Prior to this, concepts such as XDR, MITRE ATT&CK, or EDR solutions were largely academic to me. However, hands-on exposure to Vision One, credential dumping simulation, and incident investigation workflows brought real context to their application.

Collaborating with peers, attending expert-led sessions, and navigating through simulated threat environments gave me a deeper appreciation for both offensive and defensive sides of cybersecurity. The experience also helped reinforce the importance of threat intelligence, real-time detection, and automated response mechanisms in modern cybersecurity operations.

References

- MITRE ATT&CK Framework: https://attack.mitre.org
- Trend Micro Vision One Product Guide v2.5
- Trend Micro Official Blog: https://www.trendmicro.com/en_us/research.html
- Microsoft Docs – Mimikatz & Credential Dumping: https://learn.microsoft.com
- National Institute of Standards and Technology (NIST): https://www.nist.gov
- Cybersecurity & Infrastructure Security Agency (CISA): https://www.cisa.gov