Threat Intelligence-Driven Endpoint Detection and Response for Security Operations Center Operations

Presenter: Prof. AUNG Htein Maw

Institution: University of Information Technology (UIT), Myanmar

Background and Motivation

Modern SOC Monitoring & Endpoint Detection:

- Security Operations Centers (SOCs) continuously monitor complex enterprise infrastructures and respond to evolving threats.
- Endpoint Detection and Response (EDR) agents identify suspicious host activity, process spawns, and abnormal behavioral telemetry across workstations and servers.

The Core Operational Challenge: Alert Fatigue & Context Gaps:

- Extreme alert volume creates severe analyst fatigue, leading to missed or delayed high-severity incident responses.
- Isolated endpoint alerts frequently lack surrounding threat context, leaving analysts to guess the attacker's broader campaign objective.

The Proposed Motivation: CTI-Driven Decision Support:

- Cyber Threat Intelligence (CTI) feeds deliver crucial indicators, known adversary tactics, and historical campaign context.
- Combining dynamic CTI enrichment with EDR telemetry offers significant potential to elevate individual alerts into prioritized, understandable incidents.

Problem Statement: From Individual Alerts to Actionable Security Incidents

1. Repetitive & Unfiltered Alert Volume

Duplicate, low-fidelity endpoint alerts can overwhelm tier-1 triage and obscure important activity.

2. Limited Threat Context

IPs, domains, files, and techniques may lack timely, integrated threat intelligence.

3. Difficult Event Correlation

Related activity across endpoints can be hard to connect when events sit in separate systems.

4. Manual Investigation & Unclear Prioritization

Cross-portal pivots consume analyst time; static severity labels may not reflect evidence-based risk.

Research challenge

Connect isolated endpoint alerts with threat intelligence to form evidence-weighted potential incidents.

Project Aim and Objectives

Primary Project Aim: To design and evaluate an integrated threat intelligence-driven framework that correlates endpoint telemetry with actionable threat intelligence to enhance SOC detection quality and analyst efficiency.

1. Telemetry & CTI Integration

- Integrate endpoint security information with CTI.
- Enrich suspicious events with relevant indicators and context.

2. Context-Aware SOC Dashboard

- Develop a conceptual, context-aware SOC dashboard.
- Present incident timelines and evidence summaries to support analyst triage.

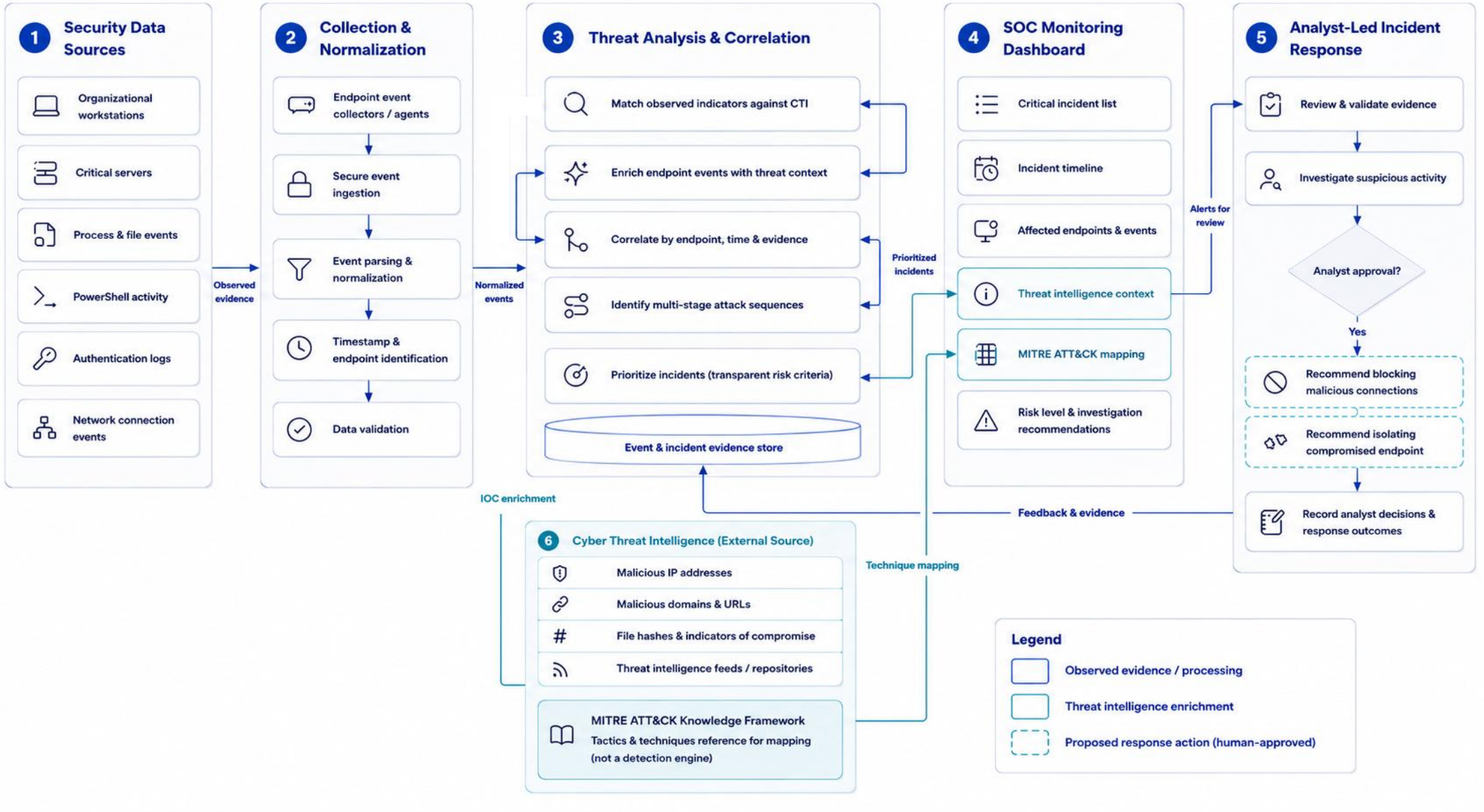
3. Correlation & Prioritization

- Correlate endpoint events into potential incidents.
- Prioritize incidents using available evidence to reduce unnecessary investigation effort.

4. Scenario-Based Evaluation

- Evaluate the proposed approach using cyberattack scenarios.
- Assess enrichment, correlation, prioritization, and analyst workflow.

Proposed System Overview: Architecture Workflow



Correlation, CTI and ATT&CK logic

Selected causal links

- Process-tree / process GUID
- File-write → execution
- Persistence
- Corroborated cross-host links

CTI enrichment

- Exact-value checks for SHA-256, IP, domain and URL
- Optional read-only MISP
- One-hour cache; errors remain unavailable

ATT&CK mapping

- Enterprise ATT&CK v19.2 pinned
- Technique hypotheses tied to evidence
- Source IDs, basis and status shown

- A shared user, nearby timestamp, logon ID or IOC alone does not establish incident membership.
- Inventory: 13 tactics and 43 techniques represented; 26 rows unverified and 17 not covered due to missing telemetry.

Explainable Risk Score & Promotion Gate

Base score B = clamp(round(S × C × I − A), 0, 100)

S — Severity

Event/rule severity plus bounded increments for suspicious event types and tactics.

C — Confidence

Base 0.45 plus bounded behavioral, CTI and Sigma contributions.

I — Asset impact

Analyst-configured impact from 1 to 10.

A — Adjustment

Allowlist and administrative PowerShell context can reduce score.

Promotion gate

At least 2 linked member events, score ≥ 20, and an independent qualifying signal.

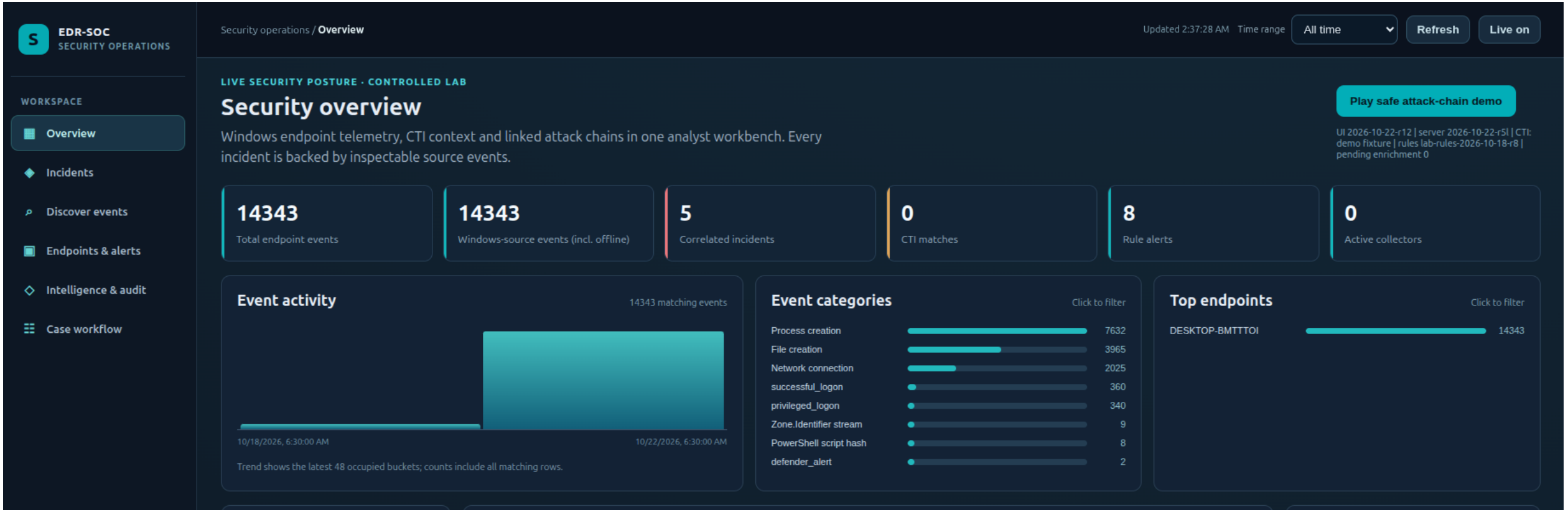
Priority bands

Low < 45 | Medium 45–74 | High ≥ 75

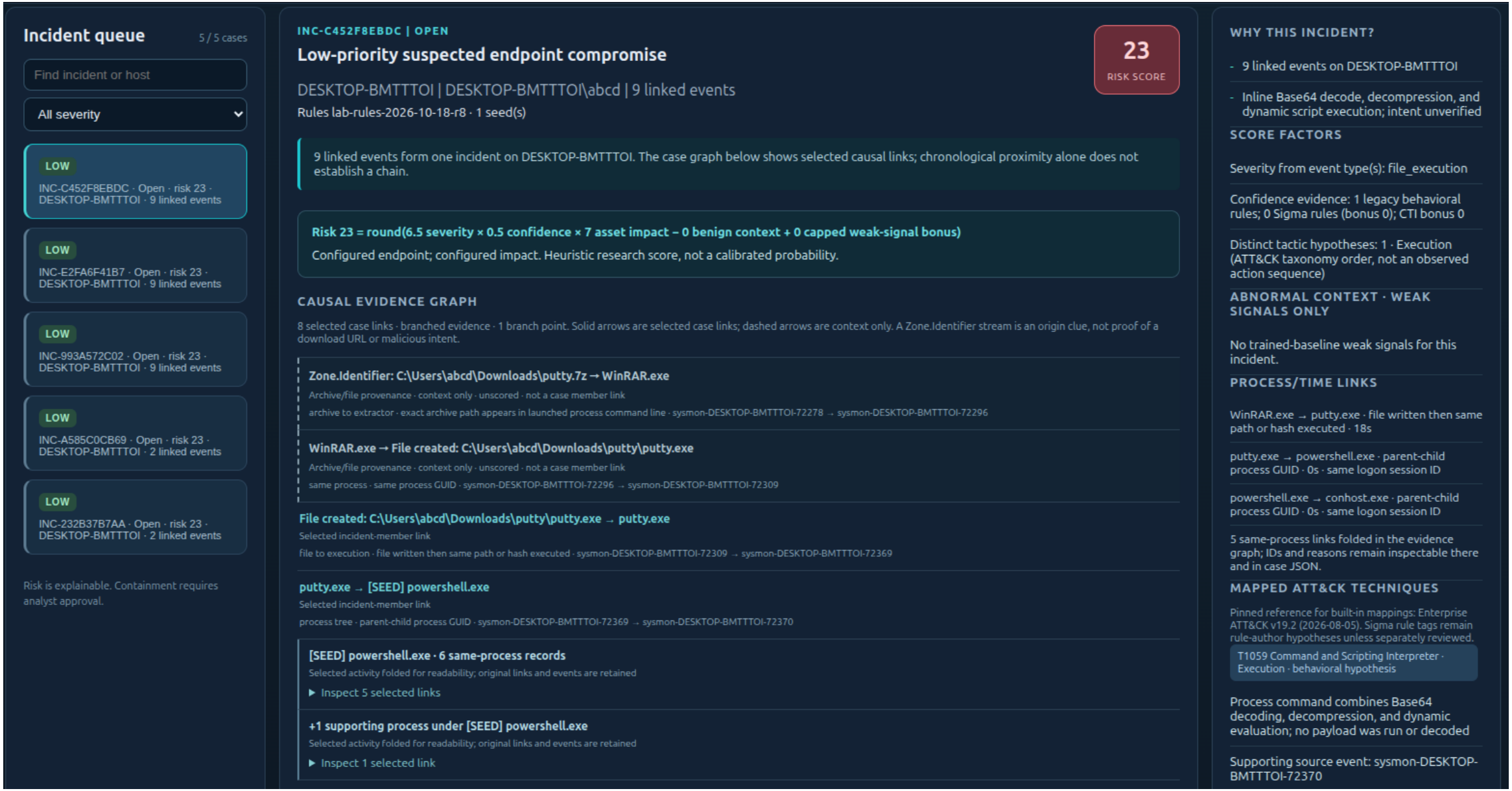
Implementation Technology Stack

Main Technology	Purpose
Windows Sysmon	Endpoint event collection
Python	Backend processing and event correlation
SQLite	Event and incident storage
MISP	Cyber Threat Intelligence (CTI) enrichment
Sigma	Detection rule integration
MITRE ATT&CK	Threat technique mapping
Custom SOC Dashboard UI R12	Incident visualization and risk prioritization

SOC Dashboard Overview



Selected Incident and Evidence



Cyberattack Scenarios and Evaluation Plan

Proposed Evaluation Scenarios

1. **Brute-Force Authentication:** Repeated failed logons followed by abnormal off-hours access.
2. **Suspicious Scripting:** Obfuscated PowerShell downloading payloads in memory.
3. **Malicious Binary Execution:** Unsigned binary execution attempting persistence via Scheduled Tasks.
4. **C2 Communication:** Host beaconing to known malicious IPs/domains.
5. **Multi-Stage Attack:** Phishing drop leading to discovery, privilege escalation, and lateral movement.

Planned Experimental Metrics

- **Ingestion & Normalization:** Lossless parsing rate across varied host event schemas.
- **CTI Enrichment Accuracy:** Precision of indicator matching against benchmark feeds.
- **Correlation Quality:** Accuracy in clustering multi-step attack traces without false grouping.
- **Prioritization Usefulness:** Alignment of risk scores with expert severity rankings.
- **Analyst Value:** Investigation time, false-positive and alert-reduction potential, and usefulness of recommendations.

Expected Outcomes and Practical Applications

Anticipated Operational Benefits

- **Enhanced Threat Visibility:** Continuous host-level telemetry unified with global threat intelligence.
- **Actionable Incident Context:** Rapidly links disparate host logs into coherent adversary narratives.
- **Objective Risk Prioritization:** Replaces arbitrary alert rankings with evidence-grounded scoring.
- **Investigative Acceleration:** Minimizes manual pivot queries across isolated threat intelligence platforms.

Potential Sector Beneficiaries

- **Academic & Higher Education:** Distributed university campus networks with decentralized workstations.
- **Government & Public Administration:** Critical civic digital public service delivery systems.
- **Banking & Financial Services:** High-compliance environments requiring auditable incident provenance.
- **Healthcare Systems:** Medical device management and hospital information systems.
- **Regional SMEs:** Cost-effective, prioritized SOC monitoring capabilities.

References

[1] Microsoft, “Sysmon,” Microsoft Learn: Sysinternals. [Online]. Available: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon. [Accessed: Oct. 25, 2026].
[2] MITRE, “Enterprise ATT&CK Tactics,” MITRE ATT&CK. [Online]. Available: https://attack.mitre.org/tactics/enterprise/. [Accessed: Oct. 25, 2026].
[3] MISP Project, “MISP Documentation and Support.” [Online]. Available: https://www.misp-project.org/documentation/. [Accessed: Oct. 25, 2026].
[4] SigmaHQ, “Sigma Specification.” [Online]. Available: https://sigmahq.io/sigma-specification/. [Accessed: Oct. 25, 2026].
[5] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, “Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile,” NIST Special Publication 800-61 Rev. 3, National Institute of Standards and Technology, Apr. 2025. [Online].

THANK YOU!!!!