1. Executive Summary

This project demonstrates how a Security Operations Center as a Service (SOCaaS) can be tailored to meet Vanguard's security needs. The goal was to design and simulate a managed solution that delivers continuous monitoring, rapid detection, and automated response without the overhead of building an in-house SOC.

The SOCaaS package integrates Wazuh SIEM, OpenEDR with Sysmon, Shuffle SOAR, and Suricata IDS, designed under a combined Zero Trust and Defense-in-Depth security model. This layered approach ensures that every access request is continuously verified while multiple defensive layers work together to reduce risk. The result is full visibility of endpoint and network activity, advanced detection rules mapped to the MITRE ATT&CK framework, and response playbooks.

Through simulated incidents such as brute-force logins, unauthorized privilege escalation, and ransomware precursors, the solution demonstrated Vanguard's ability to:

- Detect and investigate threats in real time
- Escalate and triage using standardized playbooks
- Enrich alerts with external threat intelligence for better decision-making

The outcome highlights SOCaaS as a scalable and cost-effective approach for Vanguard to strengthen its defenses against modern cyber threats while ensuring enterprise-grade security operations.

2. Customer Profile & Security Model

Customer Overview – Vanguard Law Firm

Vanguard is a mid-sized legal services provider with 50+ employees and two national offices (Beirut HQ and Saida branch). The firm specializes in corporate and intellectual property law, serving high-profile clients with highly confidential case data. Due to budget constraints, the initial SOCaaS deployment is scoped to 5 core endpoints and 1 Domain Controller, representing the most critical assets.

- Endpoints: 5 Windows workstations onboarded in phase one (out of 50+ total)

- Server Infrastructure: 1 Windows Server acting as a Domain Controller, hosted on Google Cloud
- Remote Access: Tailscale VPN connections for secure staff access
- Security Priority: Protecting client records, maintaining service uptime, and meeting confidentiality obligations under local bar association and privacy regulations

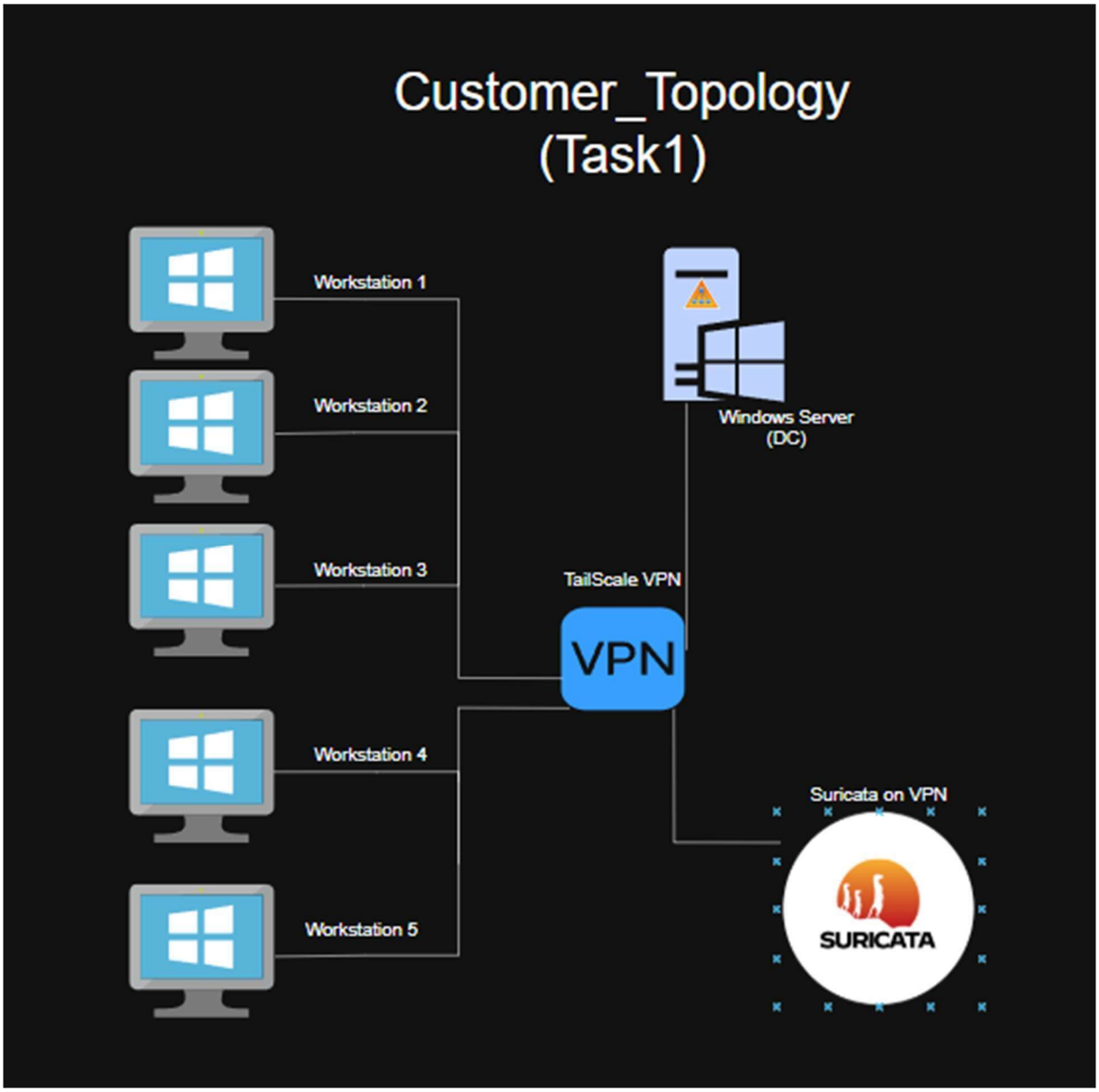

Figure 1: Customer Topology

Threat Landscape

As a law firm, Vanguard faces a diverse set of threats including:

- Credential-based attacks (brute force, password spraying, stolen credentials)
- Privilege escalation within Active Directory
- Ransomware campaigns targeting legal case files
- Phishing and legal document fraud aimed at attorneys handling sensitive correspondence
- Insider risks amplified by economic instability, where employees may be bribed or coerced into misuse

Chosen Security Model

To address these risks, the SOCaaS design follows a combined Zero Trust and Defense-in-Depth strategy:

- Zero Trust: Continuous authentication, least-privilege enforcement, micro-segmentation, and device compliance validation.
- Defense-in-Depth: Layered security with endpoint monitoring (OpenEDR, Sysmon), network traffic inspection (Suricata IDS), centralized log correlation (Wazuh SIEM), and SOAR-based workflows (Shuffle).

Why this approach?

This hybrid model was selected because Vanguard's environment is resource-constrained yet highly sensitive. Zero Trust enforces strict identity and access controls, while Defense-in-Depth ensures resilience through redundancy, meaning even if one control fails, others remain active to protect case data. Together, they provide a strong foundation for SOC-as-a-Service delivery, balancing practical budget limits with robust protection against advanced threats.

3. SOCaaS Architecture

Overview

The SOC-as-a-Service (SOCaaS) architecture for Vanguard is designed to provide full visibility, detection, and triage capabilities across its critical IT assets while remaining cost-efficient. The

architecture integrates endpoint, server, and network telemetry into a centralized SIEM, with SOAR providing playbooks for triage and escalation.

Core Components

- Endpoints (Windows Workstations): Deployed with Sysmon, OpenEDR, and Wazuh Agents to generate detailed telemetry on process activity, malware behavior, and security events.
- Server Infrastructure (Domain Controller): Windows Server logs (Security Events + Sysmon) are collected and forwarded through Wazuh for monitoring authentication, group policy changes, and privilege escalations.
- Suricata IDS: Deployed as a VPN and LAN traffic sensor, inspecting packets for exploit attempts, command-and-control (C2) traffic, and anomalous behavior. JSON alerts are forwarded via Wazuh Agents.
- Wazuh SIEM (Manager): Serves as the central collection and correlation engine, normalizing logs from endpoints, DC, and IDS. Detection rules are mapped to MITRE ATT&CK and custom rules designed for Vanguard's threat landscape.
- Shuffle SOAR: Connected to Wazuh via Webhooks. Contains playbooks for enrichment (VirusTotal, AbuseIPDB), notifications (Discord), and escalation workflows.

Log Flow

- Endpoints & Server: Sysmon, OpenEDR, and Windows Security events → Wazuh Agent → Wazuh Manager.
- Suricata IDS: Tailscale VPN Network alerts → Wazuh Agent → Wazuh Manager.
- Wazuh Manager: Normalizes, correlates, and triggers detection rules.
- Shuffle SOAR: Receives alerts from Wazuh, contains playbooks for enrichment and escalation.

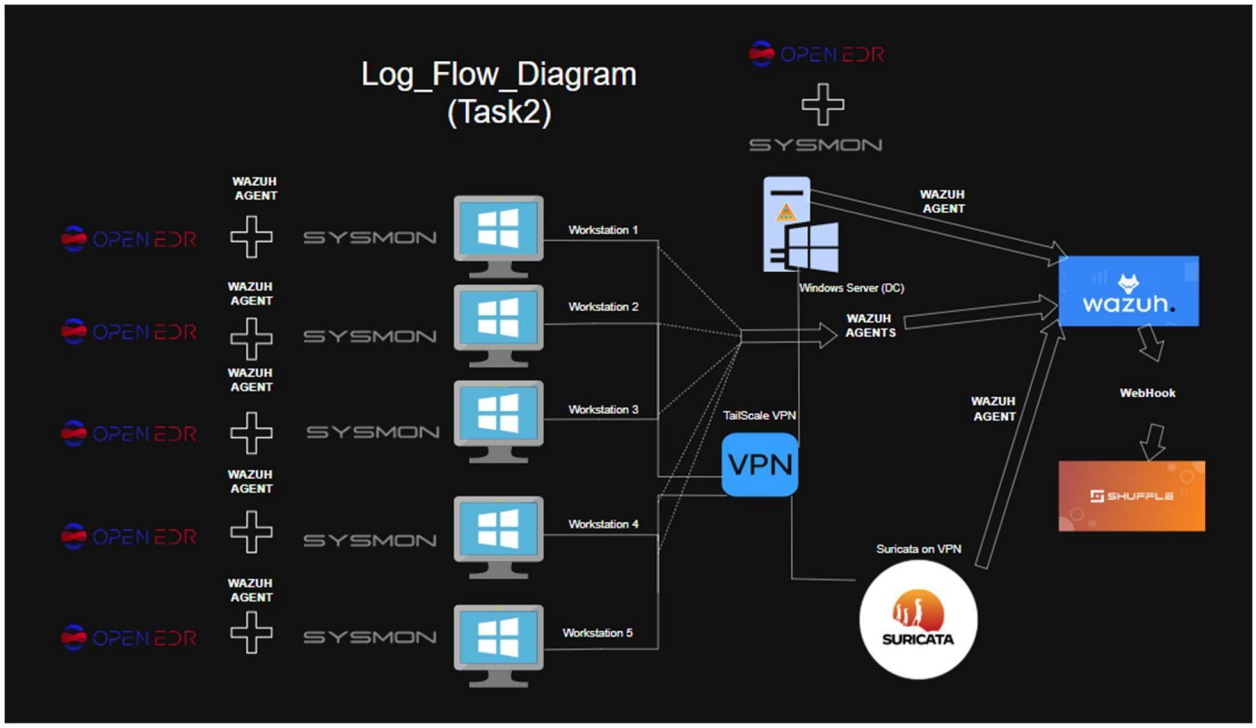

Figure 2: Log Flow Diagram

Outcome

This architecture ensures Vanguard benefits from multi-layered detection and response, combining endpoint, network, and server monitoring under one SOCaaS package. It validates the hybrid Zero Trust + Defense-in-Depth approach while keeping deployment scalable to the firm's budget and phased adoption strategy.

4. Detection Content

Overview

To protect Vanguard's most critical assets, several custom detection use cases were developed. Each rule was designed in Wazuh SIEM, mapped to relevant MITRE ATT&CK techniques, and validated against simulated events. These detections focus on common attack paths faced by law firms: credential abuse, privilege escalation, ransomware precursors, and suspicious process activity.

Detection Rules

a) Failed RDP Logon (Rule 100010)

- Log Source: Windows Security Events (Event ID 4625, Logon Type 10)
- Detection Logic: Flags repeated failed remote logons to identify brute force attempts.
- MITRE Technique: T1078 – Valid Accounts
- Priority: High
- False Positives: Occasional user password typos.
- Group By: Source IP and Target Username

b) Domain Admins Membership Change (Rule 100015)

- Log Source: Windows Security Events (Event ID 4728/4729)
- Detection Logic: Alerts when a user is added to or removed from the Domain Admins group.
- MITRE Technique: T1098 – Account Manipulation
- Priority: Critical
- False Positives: Authorized IT maintenance with change tickets.
- Group By: Actor User and Modified User

c) Group Policy Modification (Rule 100014)

- Log Source: Windows Security Events (Event ID 5136, ObjectClass = groupPolicyContainer)
- Detection Logic: Detects unauthorized or suspicious Group Policy changes.
- MITRE Technique: T1484.001 – Domain Policy Modification
- Priority: High
- False Positives: Approved GPO updates during scheduled changes.
- Group By: User making the change and Object name

d) LSASS Access Attempt (Rule 100100)

- Log Source: Sysmon (Event ID 10 – Process Access)

- Detection Logic: Triggers when a process attempts to access lsass.exe, a common target for credential dumping tools.

- MITRE Technique: T1003.001 – OS Credential Dumping: LSASS Memory
- Priority: Critical
- False Positives: Security tools (EDR/AV) performing memory scans.
- Group By: Source Process Image and host

e) Shadow Copy Deletion (Rule 100104)

- Log Source: Sysmon (Command Line Execution)
- Detection Logic: Detects commands using vssadmin delete shadows or wmic shadowcopy delete, techniques often linked to ransomware.
- MITRE Technique: T1490 – Inhibit System Recovery
- Priority: Critical
- False Positives: Legitimate IT maintenance during backup cleanup.
- Group By: Command Line and User

Outcome

These rules form the foundation of Vanguard's SOCaaS detection content. They ensure that high-impact attack behaviors are rapidly identified, triaged, and escalated for investigation. By aligning detection logic with MITRE ATT&CK and supplementing with visuals where useful, the SOCaaS platform provides Vanguard with structured visibility against the tactics most likely to target law firms.

5. Triage Playbooks

Overview

For each detection rule, a Level 1 triage playbook was designed. These playbooks provide analysts with standardized investigation steps, escalation criteria, and closure conditions, ensuring alerts are handled consistently and efficiently.

a) Failed RDP Logon (Rule 100010)

- Investigation Steps: Check source IP reputation, validate target username, review frequency of failed attempts.
- Escalation Criteria: Repeated attempts from foreign IP.

- Closure Conditions: Single failed attempt, user confirms mistyped password.

  Decision Flow: If repeated + external → Escalate. Otherwise → Close.

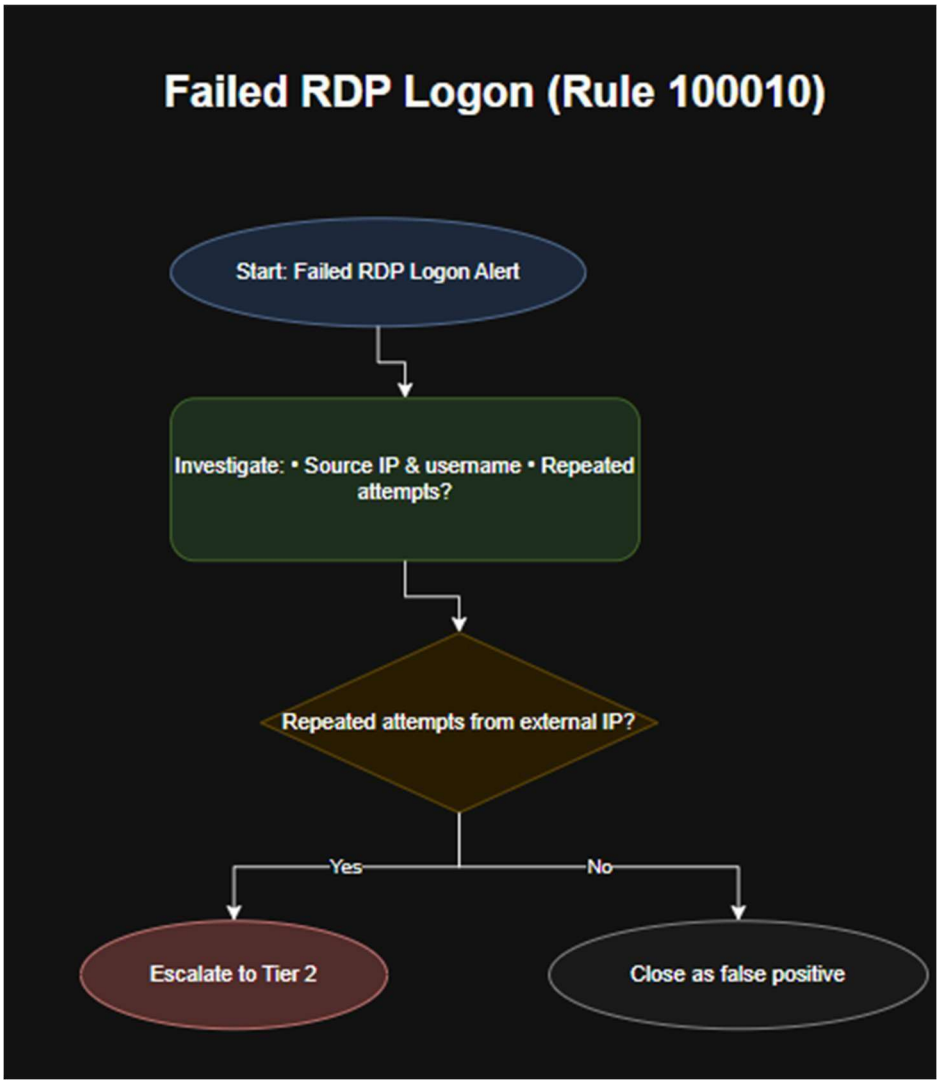

Figure 3: Failed Logon Triage

b) Domain Admins Membership Change (Rule 100015)

- Investigation Steps: Review command line (-enc string) and identify parent process launching PowerShell.
- Escalation Criteria: Suspicious parent process (e.g., Word, Excel) or non-IT user executing encoded commands.

- Closure Conditions: Known IT/admin script executed by an authorized IT user.

  Decision Flow: If suspicious parent or non-IT user → Escalate. Otherwise → Close as legitimate IT script.

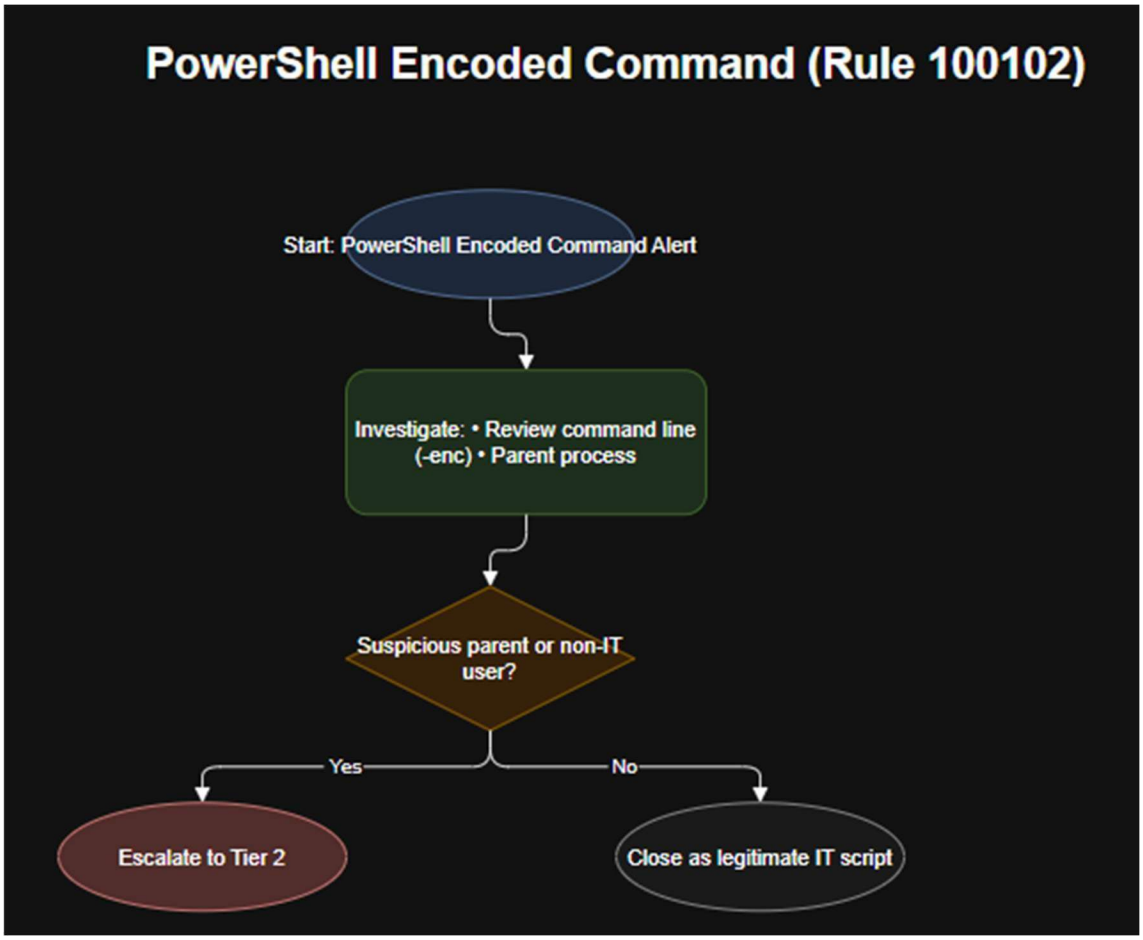

Figure 4: PowerShell ENC Triage

c) Group Policy Modification (Rule 100014)

- Investigation Steps: Identify which GPO was modified, validate actor user against AD admin list, check for change ticket.
- Escalation Criteria: Modification outside scheduled window, unauthorized actor.
- Closure Conditions: Approved update confirmed by IT.
- Decision Flow: Authorized change → Close. Unauthorized → Escalate.

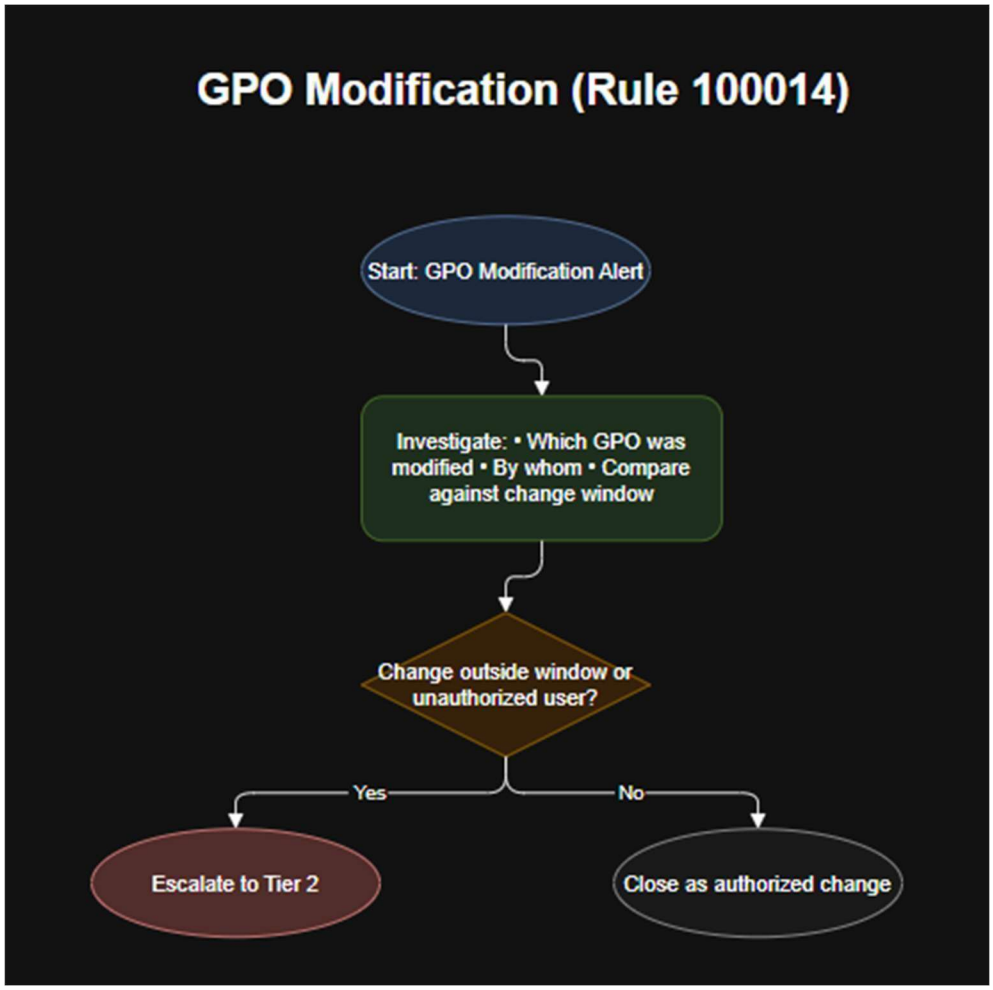

Figure 5 : GPO Modification Triage

d) LSASS Access Attempt (Rule 100100)

- Investigation Steps: Review source process image, check hash in VirusTotal, compare against baseline of legitimate tools.
- Escalation Criteria: Unknown or malicious tool (e.g., Mimikatz) accessing LSASS.
- Closure Conditions: Security tool performing expected memory scan.
- Decision Flow: Legitimate security tool → Close. Unknown/malicious process → Escalate.

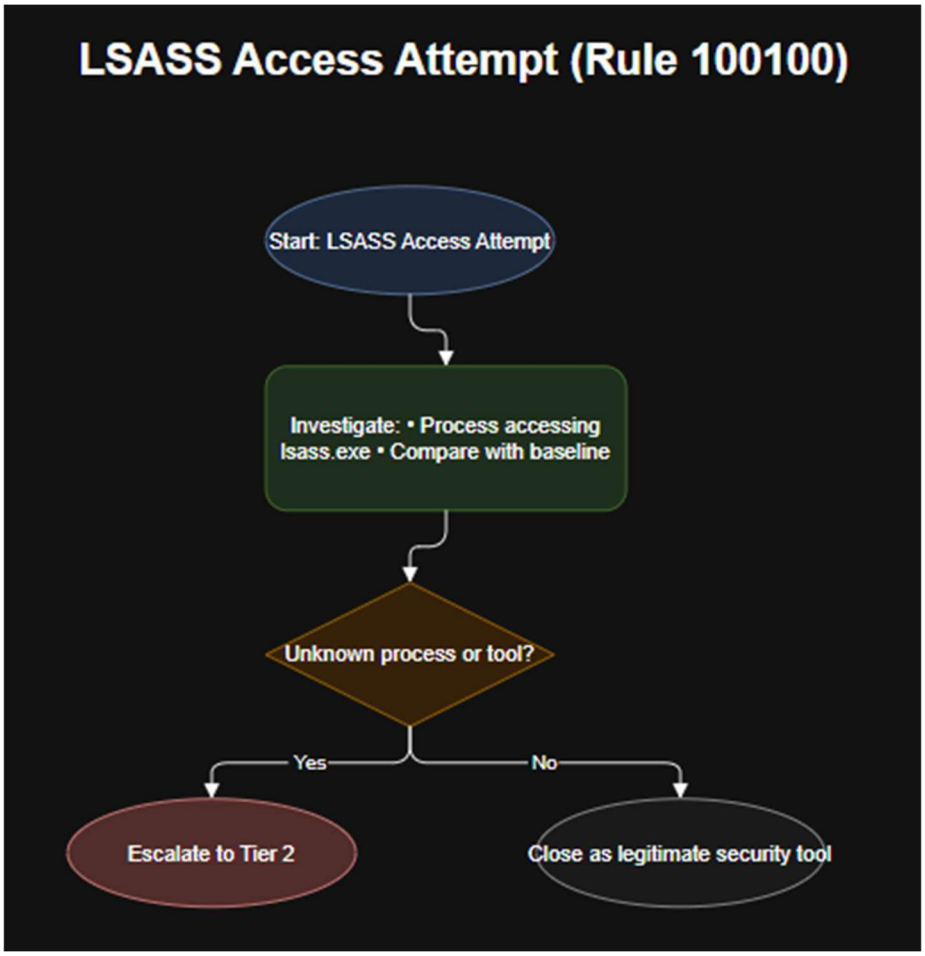

Figure 6: LSASS Access Triage

e) Shadow Copy Deletion (Rule 100104)

- Investigation Steps: Review command line for vssadmin/wmic shadow deletion, check actor user role, verify if cleanup task was scheduled.
- Escalation Criteria: User not backup admin, unexpected deletion during work hours, activity accompanied by file encryption.
- Closure Conditions: Scheduled backup cleanup or storage maintenance.
- Decision Flow: Approved maintenance → Close. Unexpected → Escalate.

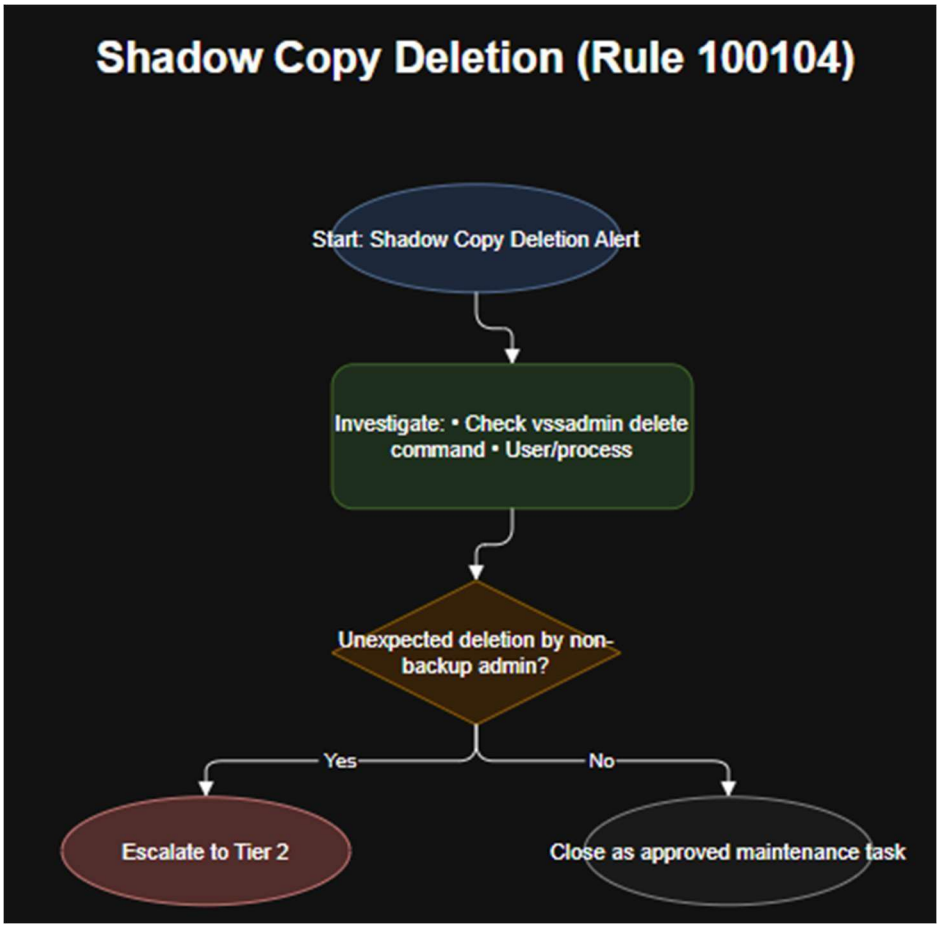

Figure 7: Shadow Copy Deletion Triage

Outcome

These playbooks provide Vanguard's SOCaaS with structured triage steps. They reduce analyst guesswork, shorten investigation times, and ensure consistent escalation when threats are confirmed. Even without full automation, the playbooks demonstrate how SOCaaS operations would function in practice.

6. SOAR Workflow

Overview

To complement detection rules and triage playbooks, five SOAR workflows were designed in Shuffle SOAR. These workflows focus on enriching alerts, notifying analysts, and streamlining escalation paths. While full automated containment was not achieved, the implemented workflows demonstrate how SOCaaS can accelerate response and reduce analyst workload in the next phase.

Automation Workflows

a) Login (Failed RDP / Suspicious Authentication – Rules 100010, 100012, 100013)

- Trigger: Wazuh alert for failed RDP logons or repeated suspicious authentication attempts.
- Automation: Extract source IP → Query AbuseIPDB → Post result to Discord.
- Outcome: Provides analysts immediate context on whether the source IP is malicious.

b) PowerShell Encoded Command (Rule 100102)

- Trigger: Wazuh alert for PowerShell execution with -enc.
- Automation: Extract command line → Decode Base64 content → Extract IOCs (URLs, IPs, hashes) → Check IPs in AbuseIPDB and hashes in VirusTotal.
- Outcome: Analysts receive enriched alerts showing whether the command or extracted indicators are malicious.

c) Group Policy Modification (Rule 100014)

- Trigger: Wazuh alert for GPO modification.
- Automation: Extract actor user → Check against authorized admin list → Post to Discord.
- Outcome: Immediate notification whether change was legitimate or requires escalation.

d) LSASS Access Attempt (Rule 100100)

- Trigger: Wazuh Sysmon alert for LSASS process access.

- Automation: Extract source process hash → Submit to VirusTotal → Return verdict to Discord.
- Outcome: Reduces time spent by analysts manually gathering process reputation.

e) Shadow Copy Deletion (Rule 100104)

- Trigger: Wazuh alert for vssadmin or wmic shadow copy deletion commands.
- Automation: Match patterns (vssadmin with delete + shadow, or wmic shadowcopy delete) → Capture full command line → Post immediate highseverity notification to Discord.
- Outcome: Ensures ransomware precursors are highlighted to analysts in real time.

Outcome

These SOAR automations validate how Vanguard's SOCaaS can integrate enrichment and escalation directly into alert handling. Even with limited containment actions, they demonstrate the value of automating repetitive tasks, speeding up triage, and giving analysts enriched, actionable alerts.

Conclusion & Next Steps

7. Conclusion

The SOCaaS project for Vanguard successfully demonstrated how open-source technologies can be combined into a managed security operations model. Through Wazuh SIEM, OpenEDR, Sysmon, Suricata IDS, and Shuffle SOAR, the environment gained multi-layered visibility across endpoints, servers, and network traffic. Custom detection rules and L1 triage playbooks provided the structure needed for analysts to investigate threats. The hybrid security model ensures that access is tightly controlled and multiple safeguards exist to contain threats even if one control fails.

Next Steps

- Scale Coverage: Expand SOCaaS onboarding from the initial 5 endpoints to all 50+ employee workstations.
- Cloud Integration: Extend detection to Microsoft 365, cloud storage, and SaaS applications commonly used by law firms.

- SOAR Automation: Full setup the defined SOAR playbooks to automatically execute automated tasks.
- Threat Intelligence: Integrate additional feeds beyond VirusTotal and AbuseIPDB for broader coverage.
- Continuous Tuning: Refine detection rules to reduce false positives and align with emerging attack techniques.

This phased approach allows Vanguard to build on the current foundation, evolving toward fullscale managed detection and response while maintaining cost efficiency and strong protection for sensitive legal data.