SOC Summary Report – October 2025

Executive Summary
This project demonstrates the design, deployment, and validation of a Splunk-based Security Information and Event Management (SIEM) environment. The goal was to build an end-to-end detection and monitoring capability using Windows Server 2022 and Sysmon telemetry, applying realistic threat simulation to confirm operational detection accuracy.

The implementation included installing Splunk Enterprise, ingesting Windows Event Logs and Sysmon telemetry, configuring detection logic for common attack behaviors, and verifying alert accuracy through controlled simulations. Hardening measures were also applied to the Windows host and Splunk environment to mirror real-world enterprise security baselines.

The result is a fully functional SIEM lab capable of detecting authentication abuse, encoded PowerShell activity, and suspicious outbound network connections — validated through practical, repeatable scenarios mapped to MITRE ATT&CK techniques.

Environment Overview
Component	Description
Platform	Windows Server 2022 VM
SIEM Tool	Splunk Enterprise 9.x
Telemetry Sources	Windows Security, System, Application Logs + Sysmon v15
Index	main
Retention	Default Splunk retention (7 days)
Data Inputs	Security, System, Application, Sysmon (Microsoft-Windows-Sysmon/Operational)

The environment was built entirely on a local Windows Server 2022 VM, with Splunk collecting telemetry directly through native inputs and Sysmon integration. Splunk Web access was secured via HTTPS, and the underlying host was hardened to reduce attack surface.

Detection Coverage

Detection	Purpose	MITRE Technique
Failed Logon Brute-Force → Success	Detect multiple failed authentication attempts followed by a successful logon	T1110 – Brute Force
Encoded PowerShell Execution	Identify obfuscated PowerShell commands leveraging the `-enc` flag	T1059 – Command & Scripting Interpreter
Outbound Connection Spike	Detect abnormal outbound network activity potentially indicating beaconing or data exfiltration	T1071 – Application Layer Protocol

Each detection was implemented as a scheduled Splunk alert running every 5 minutes over the last 10–15 minutes of data.

Threat Simulation and Validation

Scenario	Description	Outcome
Failed Logon Brute Force	Multiple incorrect logins followed by one successful attempt using `runas /user:SecAdmin cmd`	☑ Alert triggered; correlated 4625 + 4624 events
Encoded PowerShell Command	Execution of an encoded PowerShell string (`-enc`)	☑ Alert triggered; Sysmon Event ID 1 confirmed obfuscated execution
Outbound Connection Spike	Repeated outbound HTTPS connections via `Test-NetConnection`	☑ Alert triggered; Sysmon Event ID 3 reflected multiple external destinations

```markdown

All detections triggered correctly and aligned precisely with the simulated behaviors, validating both event ingestion and correlation logic.

---

## Hardening Summary

| Area | Action | Outcome |
|--------|----------|-----------|
| **Windows OS** | Applied password and lockout policy; enabled audit logging | ☑ Secured baseline |
| **Splunk Access** | Enabled HTTPS; created restricted “analyst” role | ☑ Role-based access enforced |
| **Firewall** | Restricted inbound rules to Splunk web interface | ☑ Controlled exposure |

---

## Observations & Recommendations

The SIEM successfully detected all test behaviors with no false positives. Alerts and dashboards provide actionable visibility for typical endpoint threats. Recommended next steps include:

- Expanding data ingestion to include Linux or firewall logs.
- Integrating email/webhook notifications for automated alerting.
- Adding detections for privilege escalation and lateral movement.
- Exploring threat enrichment with WHOIS or VirusTotal lookups for outbound IPs.

---

## Conclusion

This project demonstrates a complete SIEM deployment lifecycle — from installation and data ingestion to detection, alerting, validation, and reporting. The environment provides a realistic training and demonstration platform for SOC workflows, emphasizing practical detection engineering and operational readiness.

```