Cypher Bank Limited — SOC Architecture & Telemetry Flow

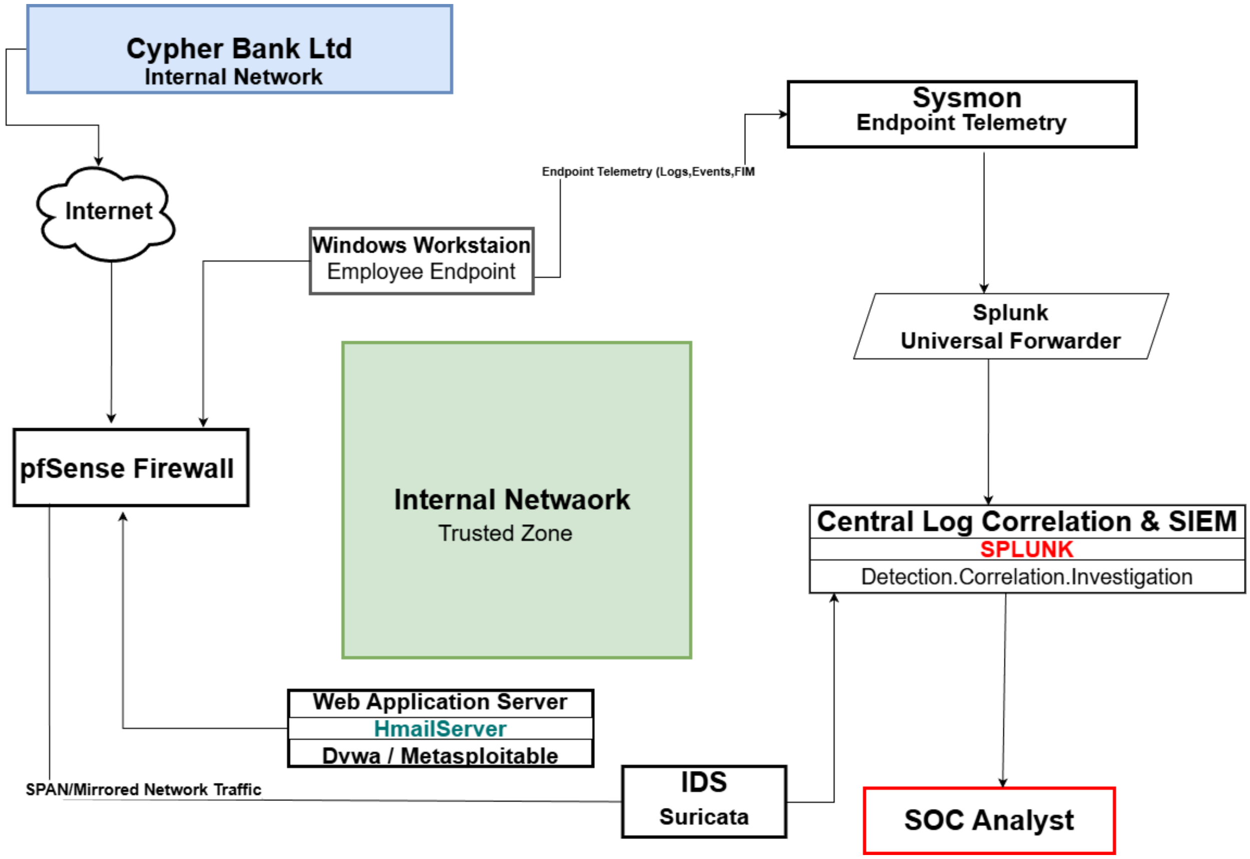
This diagram illustrates the **end-to-end security monitoring architecture** designed for the *Cypher Bank Limited* phishing-led attack simulation.

It shows how **endpoint, network, and email telemetry** are collected, normalised, and correlated within **Splunk SIEM** to support **real-world SOC investigations**.

Key highlights:

- Windows endpoint telemetry via **Sysmon**
- Network visibility through pfSense and Suricata IDS
- Email and web attack surface using **hMailServer**, **DVWA**, and **Metasploitable**
- Centralised detection, correlation, and investigation in **Splunk**
- Analyst-driven investigation workflow aligned **SOC Level 2 practices**

This architecture mirrors how enterprise environments enable **phishing detection, lateral movement analysis, and incident response** in regulated financial institutions.



Cypher Bank Ltd
Internal Network
Internet
Windows Workstaion
Employee Endpoint
Endpoint Telemetry (Logs,Events,FIM
Sysmon
Endpoint Telemetry
Splunk
Universal Forwarder
pfSense Firewall
Internal Netwaork
Trusted Zone
Central Log Correlation & SIEM
SPLUNK
Detection.Correlation.Investigation
Web Application Server
HmailServer
Dvwa / Metasploitable
SPAN/Mirrored Network Traffic
IDS
Suricata
SOC Analyst