Proactive Cyber Defence Strategy:

Insider Threat Detection and Monitoring System Evaluation for a UK-Based Client

Prepared by:

Yash Bhootra

Table Of Content

Assumptions

This section outlines the working assumptions that underpin the evaluation and recommendations provided in this report. These assumptions are based on the network architecture shown in Figure 1: Client Network and ensure consistency throughout the analysis. The assumptions reflect the client's operational posture, technical environment, and security requirements.

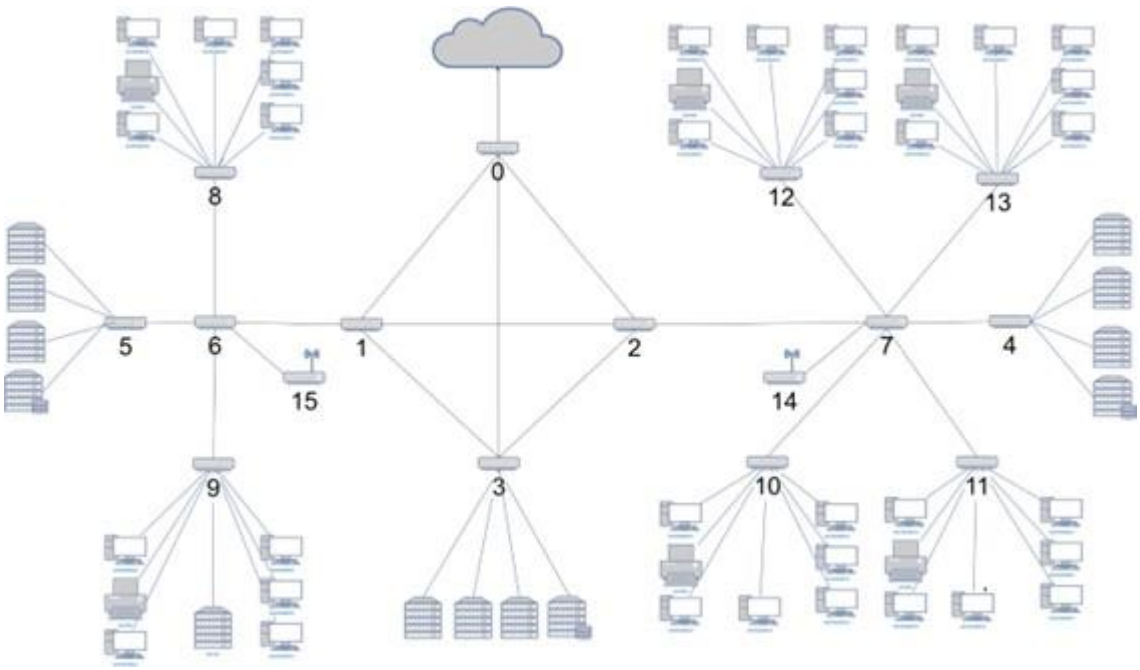

Figure 1: Client Network

1. **Organisational and Legal Context**

- The client is a UK-based defence-sector enterprise involved in product development, collaboration with foreign agencies, and innovation services.
- It is subject to UK GDPR, Computer Misuse Act 1990, and National Cyber Security Centre (NCSC) guidance.
- The client owns all data generated and transmitted on the network, including sensitive data and intellectual property.
- A Security Operations Centre (SOC) is in place, with internal analysts and selected partner teams.

2. Network Topology and Gateways

The network is segmented via gateway nodes 0 to 15, as illustrated in Figure 1. These nodes include external connections, internal routers, server access points, client network segments, and wireless infrastructure.

Gateway Node	Function
Node 0	Main internet gateway, handles all external web and cloud traffic.
Node 1	Internal core switch connecting Nodes 0, 2, and 6; used for routing.
Node 2	Core distribution switch, routes traffic to downstream server and client segments.
Node 3	Gateway to Server Farm 1 (likely database services and backend apps).
Node 4	Gateway to Server Farm 2, assumed to host email, application services.
Node 5	Gateway to Server Farm 3, likely file servers and internal collaboration platforms.
Node 6	Backbone router connecting Nodes 5, 8, and 15; handles east-west server traffic.
Node 7	Intermediate switch for client-side routing; connects Nodes 4, 10, 11, and 14.
Node 8	Connects a client subnet, possibly Finance or HR; monitored for sensitive access.
Node 9	Connects the File Server, accessed by multiple departments.
Node 10	Hosts workstations, including the compromised system involved in the SOC-detected incident.
Node 11	Represents partner development teams, accessing collaboration environments.
Node 12	General client access network (e.g., HR, Admin) with multiple workstations.
Node 13	External or third-party team access to internal systems.
Node 14	Wi-Fi access point node (e.g., for meeting rooms or mobile devices).
Node 15	Secondary Wi-Fi AP node (likely for the IT team or roaming users).

Figure 2: Gateway nodes and its function

3. Technical Infrastructure and Capabilities

- VLAN segmentation is implemented across all departments and servers.
- Active Directory is used for authentication and basic access control.
- Currently deployed tools include antivirus, firewall, and basic endpoint protection.
- The network lacks a centralised SIEM, SOAR, or behavioural analytics system.
- The infrastructure supports deployment of Wazuh, Suricata, Zeek, Elastic Stack, or Splunk.

4. Security and Monitoring Scope

- The organisation prioritises detection of insider threats, data exfiltration, and APT-style attacks.
- Sensor and log collection points are proposed at key junctions: Nodes 3, 5, 9, and 10.
- Monitoring extends to endpoint activity, network flow, USB usage, and authentication logs.
- The network is high-volume, especially during collaboration or product development cycles.
- Endpoint visibility is possible via agent-based logging and centralised syslog forwarding.

5. Ethical and Legal Considerations

- All security monitoring tools are assumed to be deployed with user notification, consent, and compliance with internal policy and legal standards.
- Evidence collection during incident response will be conducted following forensically sound procedures in line with UK legal frameworks.

Section 1: Detecting Reconnaissance

1.1 Introduction

In this section, I will examine how insiders typically conduct reconnaissance, what specific data I would collect to detect this activity, where I would deploy monitoring across the network, and which tools and configurations would support effective detection. I also consider how to handle the high data volume typical of enterprise networks.

1.2 Understanding Insider Reconnaissance

Insiders usually begin by attempting to build a map of the internal network. They might use tools such as nmap, PowerView, BloodHound, or even PowerShell scripts to probe devices, enumerate services, and identify active hosts. A user could scan subnets for machines exposing ports like TCP/445 (SMB), TCP/3389 (RDP), or UDP/53 (DNS), attempting to uncover shares, remote desktop access points, or domain controllers.

These actions may appear benign in isolation but become suspicious when analysed in context. For example, a non-IT employee performing an aggressive scan across multiple VLANs, or using enumeration tools on file servers, may be testing defences or preparing for further malicious activity. Such reconnaissance often precedes lateral movement, privilege escalation, or data exfiltration (MITRE, 2023).

1.3 What Data I Would Collect and Where

Detecting reconnaissance requires visibility into both network and endpoint activity. I would adopt a layered approach to data collection, focusing on the most valuable detection points. Below is a breakdown of the data I would collect and where it should be monitored:

- NetFlow/IPFIX at Gateways 3, 5, and 10 - This provides metadata on communication patterns. I would use it to spot unusual traffic volumes, frequent connection attempts, and port scanning behaviours.
- DNS Logs from internal DNS servers and Gateway 3 - These can reveal abnormal patterns like domain enumeration, reverse lookups, or DNS tunnelling attempts.
- Full Packet Capture using Zeek at Gateway 5 - This is critical for deep inspection of traffic directed at the client's internal servers. It allows for precise protocol-level analysis (e.g., SMB enumeration, HTTP probing).
- Authentication Logs at Gateway 10 and Domain Controllers - These would help identify brute-force attempts, logins from unusual IPs, and failed credential usage.
- Endpoint Telemetry from Wazuh agents installed on privileged user devices - I would monitor command-line activity, PowerShell execution, registry changes, and usage of tools like netstat, nltest, or whoami.

This combination ensures coverage across the perimeter, internal gateways, and host systems where reconnaissance might originate.

1.4 Tools to Use and Its Configuration

To collect and analyse this data effectively, I would recommend the following toolset:

Zeek (Network Traffic Monitor):

It allows for in-depth analysis of protocols such as DNS, HTTP, SMB, and FTP. I would configure it to:

- Detect multiple SYN packets from a single internal IP without follow-up ACKs (indicating a port sweep).
- Log unusual SMB share access or file browsing patterns.
- Monitor DNS for high-frequency subdomain queries.

Suricata (IDS/IPS):

It is excellent for detecting known scanning techniques. I would:

- Enable signature rules for FIN, NULL, and Xmas scans.
- Detect DNS tunnelling or encoded payloads.
- Monitor for malformed packets often used during service fuzzing.

Wazuh (Endpoint Monitoring Agent):

It would provide insight into user behaviour and endpoint-level activity. I'd configure it to:

- Alert when PowerShell is launched with suspicious flags (e.g., -enc, -nop)
- Track file access and modifications on sensitive directories
- Detect installation or execution of reconnaissance tools from user space

SIEM (e.g., Splunk or Elastic Stack):

Logs from all tools would feed into a central SIEM. I would configure:

- Correlation rules (e.g., scan → failed logins → file access)
- Behaviour-based alerts triggered by anomalous sequences
- Dashboards highlighting top talkers, scan heatmaps, and internal pivot paths

Beyond standard alerts, I would implement composite correlation rules. For instance, if a host triggers a scan alert, then attempts RDP access to multiple machines, and executes an unknown binary, this would be prioritised as a high-confidence threat. I would also measure

and regularly tune these rules to optimise Mean Time to Detect (MTTD), aiming for less than 20 minutes per confirmed alert.

1.5 Managing Scale on a High-Traffic Network

One of the most practical concerns is how to monitor efficiently without overwhelming the infrastructure. Here's how I would address this:

1. Packet Filtering (BPF): I would apply filters to Zeek to capture only specific protocols (e.g., DNS, SMB) or traffic from suspicious IPs.
2. NetFlow Sampling: I'd use 1:1000 packet sampling to detect abnormal behaviour trends without collecting full data.
3. Event-Triggered Capture: When Suricata detects a scan, it could trigger short-term full packet capture around the incident window.
4. Lightweight Edge Sensors: In remote offices or partner networks, I'd deploy trimmed-down sensors that forward only significant alerts.
5. Tiered Log Retention: Detailed logs (e.g., packet captures, endpoint events) would be retained for 7-14 days, while summarised metrics would be archived for longer durations.

This ensures a balance between detection fidelity and system performance.

1.6 Data Protection Considerations

Monitoring employee activity raises ethical and legal responsibilities. All data collection must comply with the UK General Data Protection Regulation (GDPR). I would recommend that the client:

- Conducts a Data Protection Impact Assessment (DPIA)
- Implements an Acceptable Use Policy (AUP) outlining that employee activity may be monitored
- Restricts access to logs based on least-privilege principles
- Maintains detailed audit logs of who accessed what data and when

In addition, I'd suggest regular employee training and transparency about monitoring policies to encourage responsible system use and mitigate privacy concerns (ICO, 2018).

1.7 Visual Support

To support this strategy, I have developed two key diagrams:

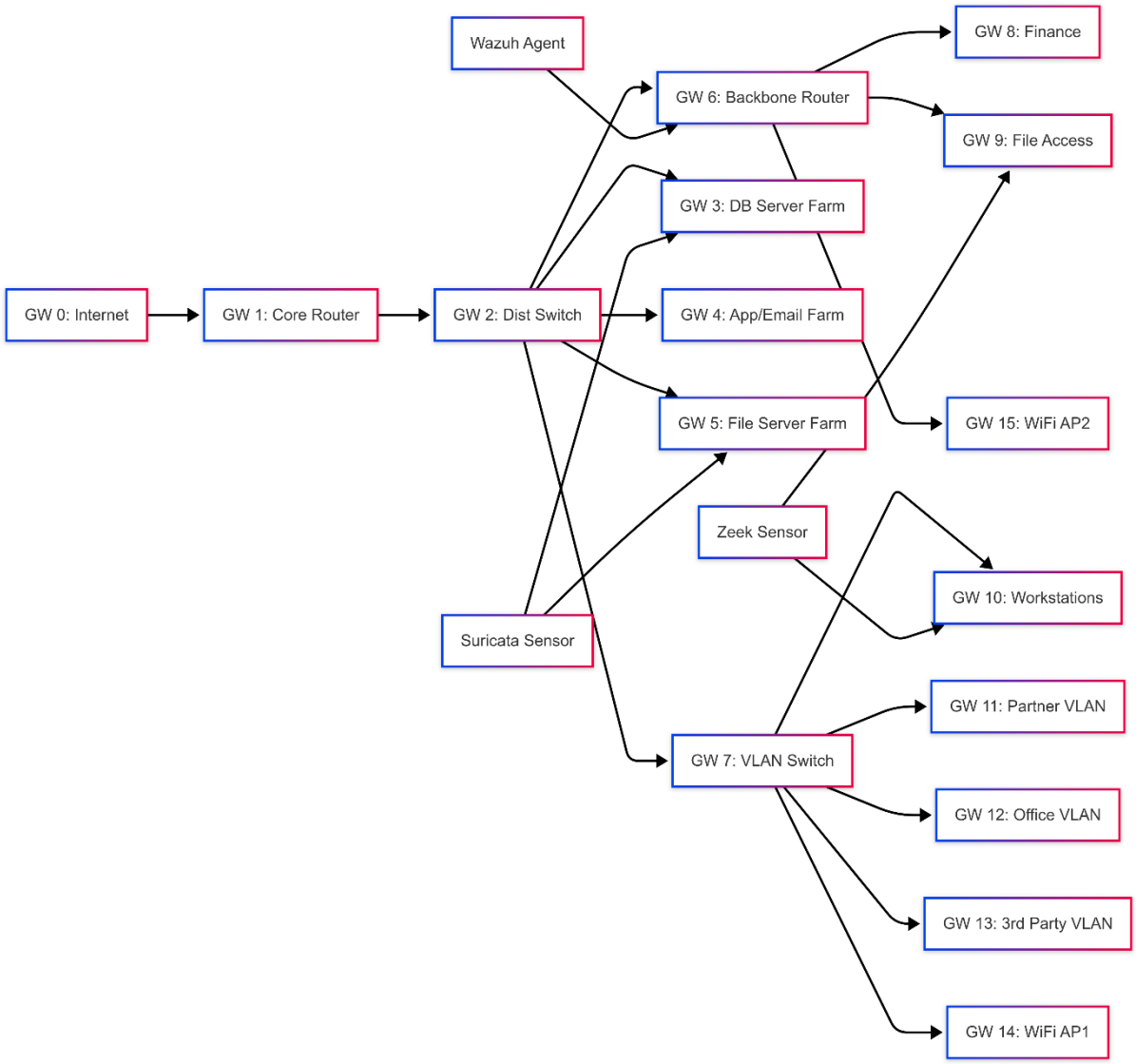

Figure 1: Sensor Placement Diagram - Illustrates monitoring sensors deployed at Gateways 3, 5, and 10, feeding into a centralised SIEM via the core switch.

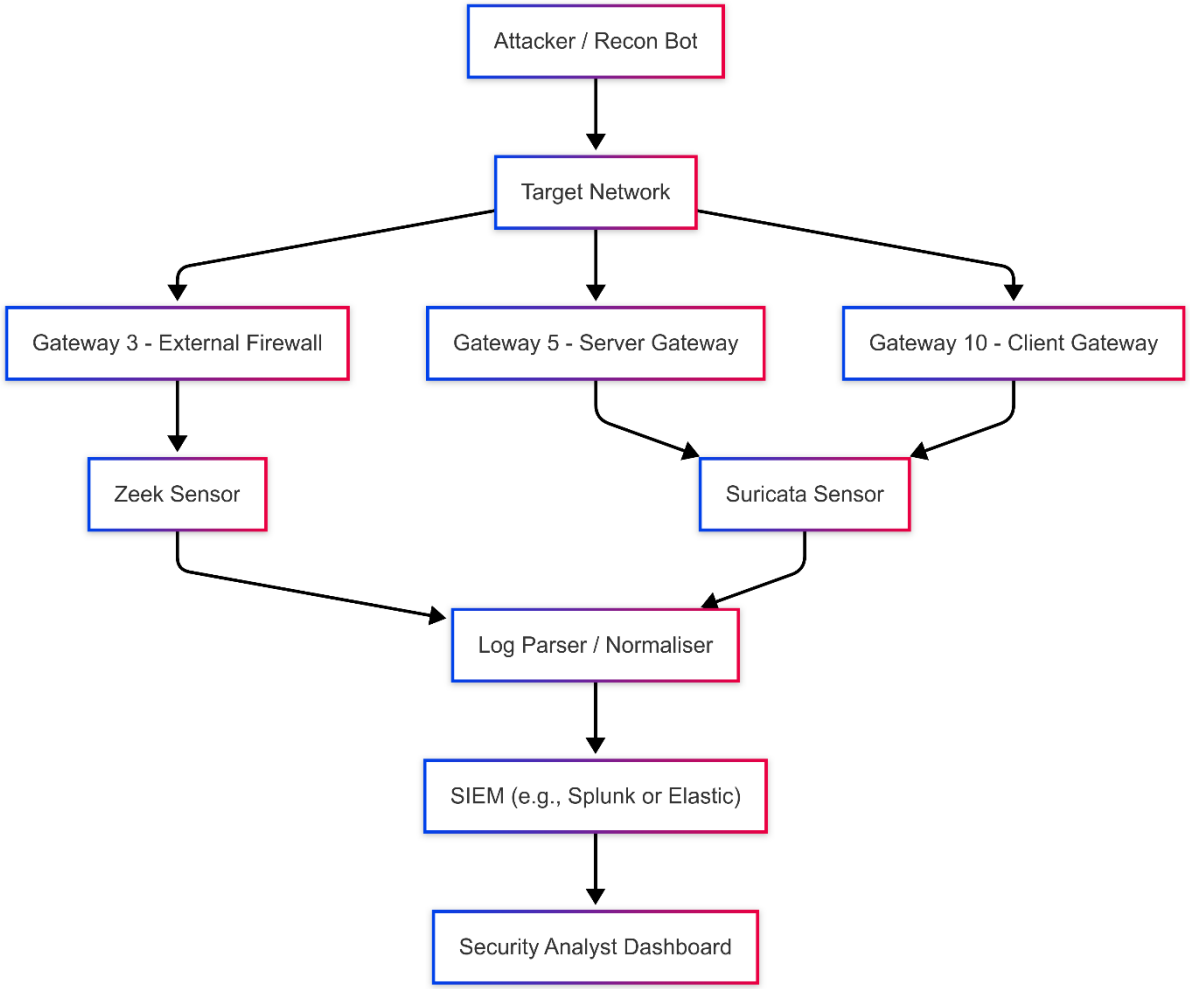

Figure 2: Reconnaissance Data Flow - Outlines the progression from attacker activity to alert generation

These diagrams ensure clarity in understanding how the detection architecture fits within the client's existing network.

1.8 Final Thoughts

Detecting internal reconnaissance is essential to stopping insider threats before they escalate into major breaches. Through a structured data collection plan, targeted sensor deployment, and intelligent correlation within a SIEM, I believe the client can significantly improve its early warning capabilities. Scalability is addressed through filtering, sampling, and decentralised processing. Most importantly, this approach respects user privacy while giving the security team the visibility they need to act decisively and compliantly.

Section 2: Statistical Data Collection

2.1 Understanding Statistical and Alert Data

Statistical data refers to numerical summaries of network activity, such as bandwidth usage, connection counts, protocol distributions, packet sizes, and session durations. This data is typically collected continuously and in bulk, enabling to establish baseline behaviours across network segments. For example, I might observe that normal SMB traffic from Gateway 5 to internal file servers averages 20 MB/min during working hours. Any significant deviation - such as a sudden spike or drop - may indicate abnormal or malicious activity.

Alert data is generated by predefined or behaviour-based rules that flag potentially suspicious events. This includes detections of port scans, failed login attempts, privilege escalation attempts, and known malware signatures. Alert data is highly focused and time-sensitive, drawing attention to specific incidents that may require immediate analysis or containment.

Both data types are crucial. Statistical data allows me to detect slow and stealthy attacks, like low-rate scanning or data exfiltration over time, which may not trigger alerts. Alert data, meanwhile, helps in identifying fast, aggressive behaviours that demand real-time response. When used together - particularly when visualised and correlated in a SIEM - they form the backbone of effective anomaly and threat detection.

2.2 Strategic Locations for Statistical Data Collection

Based on my analysis of Figure 1 in the client network, I have identified three strategic locations where statistical data collection will provide the highest value for early threat detection and long-term behavioural analysis:

1. Gateway Node 3 (External-Facing Server Farm)

This node handles traffic between the client's internal systems and external users. Monitoring here enables me to profile inbound and outbound flows, helping detect unusual volume or patterns in requests to public-facing services. For instance, a spike in HTTP POST requests might signal data exfiltration via web services.

2. Gateway Node 5 (Internal Server Access Point)

This gateway connects to sensitive internal application and database servers. By collecting flow data and protocol usage statistics here, I can baseline typical server interactions (e.g., volume of database queries, SMB transfers). Deviations from this norm - especially out-of-hours - could signal insider reconnaissance or unauthorised access attempts.

3. Gateway Node 10 (Client Workstations)

As the interface between user endpoints and the rest of the network, this location provides visibility into user behaviour. Collecting session statistics, such as file access frequency or

DNS request counts, enables me to detect compromised hosts engaging in beaconing or lateral movement.

2.3 Tools and Configuration

For effective data collection and processing, I recommend the following tools and setup:

- sFlow/NetFlow: I would enable sFlow exports on the selected gateways. Sampling at a 1:1000 ratio strikes a balance between visibility and performance overhead. These exports would include Layer 3/4 metadata and be directed to a flow collector such as ntopng or ElastiFlow (if using Elastic Stack).
- Zeek: For deeper protocol analysis, Zeek sensors deployed at Gateway 5 and Gateway 10 would allow me to generate structured statistical logs (e.g., conn.log, dns.log, http.log) which can feed into time-series dashboards.
- Filebeat and Metricbeat: These lightweight agents would ship statistical data (CPU, memory, connection count, etc.) from both network devices and endpoints to the SIEM. They can be centrally configured and tuned for efficiency.

All collected data would be ingested into a SIEM platform - either Splunk or Elastic Stack - with dashboards configured to show traffic baselines, time-series anomalies, and protocol-specific deviations. Correlation rules can then combine statistical trends with alert data (e.g., spikes in traffic followed by login failures), increasing confidence in detecting real threats.

Section 3: Splunk or Elastic Stack?

3.1 Introduction

Both Splunk and Elastic are reputable platforms with proven capabilities in SIEM, XDR, and SOAR use cases. In this section, I will compare their detection and response capabilities, discuss their popularity in the security community, and recommend the best fit for the client's specific context.

3.2 Detection Capabilities

Splunk:

Splunk's detection capabilities are mature and highly customisable. It offers a wide array of features through Splunk Enterprise Security (ES), which comes with prebuilt correlation searches, threat intelligence integration, and anomaly detection models. I've used Splunk to detect lateral movement, privilege abuse, and exfiltration using indicators like unusual login times, privilege escalations, and DNS tunnelling.

Splunk's User Behaviour Analytics (UBA) module provides machine learning-based detection, which is particularly effective in identifying insider threats. For example, I can use UBA to

flag deviations from a user's typical login time or detect rare command-line activity on a workstation.

Elastic Stack:

Elastic Stack, when used with Elastic Security, also delivers strong detection capabilities. I have configured it to monitor endpoint activity (via Elastic Agent) and ingest network and application logs in near real-time. It includes prebuilt detection rules mapped to the MITRE ATT&CK framework, enabling immediate value post-deployment.

Where Elastic shines is in its custom query-based detection using KQL (Kibana Query Language) and EQL (Event Query Language). This allows to create precise rules tailored to the client's environment. For example, detecting when a non-admin user attempts to access RDP or uses net.exe for enumeration.

3.3 Automated Response (SOAR/XDR)

Splunk:

Splunk integrates natively with SOAR (previously Phantom), which is one of the most widely adopted SOAR platforms on the market. I have built automated playbooks in Splunk SOAR that can isolate infected endpoints, disable user accounts in Active Directory, and trigger MFA resets when suspicious behaviour is detected.

For example, a typical insider threat response might involve:

- Detecting abnormal PowerShell use via UBA
- Querying user session logs via Splunk ES
- Automatically disabling the user account and generating a ticket in the helpdesk system

These responses happen within seconds and are fully auditable within the SOAR interface.

Elastic Stack:

Elastic Security also offers automated response capabilities, but it is less mature compared to Splunk's SOAR. Its response features are primarily limited to:

- Killing malicious processes
- Isolating compromised hosts (when Elastic Agent is installed)
- Alert forwarding and ticket generation

While these are sufficient for many scenarios, they are not yet as comprehensive or user-friendly as Splunk's orchestration engine.

3.4 Community, Support, and Usability

Splunk benefits from longstanding enterprise adoption and a well-documented community knowledge base. It also offers premium support tiers, which can be critical during high-severity incidents. However, it is often criticised for licensing costs, especially in high-ingest environments.

Elastic Stack, by contrast, is open source at its core and more cost-effective to deploy initially. It allows for horizontal scaling, making it ideal for environments with unpredictable data volumes. However, it may require more engineering effort to fine-tune and integrate, particularly when configuring detection rules or custom dashboards.

Both platforms are respected in the security community for their flexibility, search power, and extensibility - but Splunk tends to be preferred in highly regulated or mature SOC environments due to its full-spectrum integration and automation maturity (Gartner, 2023).

3.5 Recommendation

After evaluating both platforms, I confidently recommend that the client adopt Splunk as the preferred solution for insider threat detection and automated response. The reasons are clear:

- Splunk offers mature, integrated User Behaviour Analytics (UBA), which is essential for detecting nuanced insider activity such as privilege abuse, anomalous logins, and lateral movement.
- Its native SOAR platform allows me to design and implement robust response playbooks - automating containment, user lockdown, and escalation within seconds.
- The platform's proven track record in high-security environments and its alignment with regulatory standards make it an ideal choice for a business that prioritises both security and operational continuity.

The client seeks rapid deployment, reliable automation, and minimal manual overhead, Splunk provides the clearest and most effective path forward.

Section 4: Incident Response

4.1 Context and Relevance of Previously Collected Data

As part of the security monitoring strategy, I established in Sections 1 and 2, the client has already deployed a layered visibility architecture across Gateways 5, 9, and 10. This incident, involving off-hours workstation activity, high-volume file access, and substantial data transfer to a database server, indicates a probable case of internal data exfiltration or preparation for sabotage.

The following data previously configured is directly relevant to the case:

- Endpoint telemetry (via Wazuh agents) from the workstation on Gateway 10 will allow me to inspect USB connection logs, PowerShell command history, file access trails, and executed processes. I expect to find timestamps indicating unauthorised external device attachment, coupled with scripts or tools used to collect data from internal resources.
- Authentication logs collected at the domain controller and correlated through the SIEM will provide insight into whether the account was active during legitimate hours, if it was compromised, or if it bypassed multi-factor authentication (MFA).
- Zeek logs at Gateway 5 (where the database server resides) will include detailed session metadata. I expect to find unusual query behaviour or a spike in outbound data volume, indicating a possible data extraction from the database.
- NetFlow data from Gateways 5, 9, and 10 will allow me to trace traffic volume, session duration, and endpoint communication paths - establishing a pattern of activity consistent with reconnaissance and staged data theft.

Together, this evidence builds a timeline of malicious internal activity and supports early-stage attribution and containment.

4.2 Additional Data Collection Required

Given that the incident is ongoing, I recommend expanding the scope of data collection to strengthen visibility and support a forensically sound investigation. My goal here is to capture volatile data, preserve artefacts, and ensure legal admissibility.

4.2.1 Endpoint Data

I recommend deploying additional endpoint collection techniques on both the affected workstation and user account context, including:

- Memory dump (RAM): This will capture active processes, encryption keys, clipboard data, and potential malware in memory. This should be performed using tools such as FTK Imager or Magnet RAM Capture, ensuring hash verification before and after imaging.
- Windows Event Logs: Particularly Security, System, and PowerShell logs, to establish file access events, command execution chains, and anomalous login activity.
- Prefetch and Shimcache analysis: These will help identify applications that were executed, even if later deleted, reinforcing timeline reconstruction.
- Removable media history: Via registry keys (USBSTOR, MountPoints2), I expect to confirm make/model of the connected USB device, which supports physical traceability.

All collection should be performed using write-blockers or in forensic imaging mode to preserve integrity.

4.2.2 Network-Based Data

- Full packet capture on Gateway 5 and Gateway 10 for a defined time window around the incident. This will enable detailed inspection of potential command-and-control signals, database queries, and file transfer mechanisms. Tools such as tcpdump or Wireshark should be used with precise time filters to reduce noise.
- DNS log enrichment: To detect whether the host attempted communication with external domains—possibly indicating staging of data for exfiltration.
- SSL inspection logs: These are critical in determining whether encrypted channels were used to transfer data out, especially via HTTPS or cloud storage platforms.
- SIEM correlation enhancement: Temporary correlation rules can be added to identify repeat behaviour across other user accounts or hosts, e.g., large SMB read operations outside working hours.

4.3 Forensic Soundness and Legal Considerations

All incident response actions must be carried out in a forensically sound manner to preserve chain-of-custody and admissibility in legal proceedings. I would ensure:

- Imaging tools support hashing (e.g., SHA256), and hash values are logged pre- and post-acquisition.
- All activities are logged in an investigation chain-of-custody form, signed by personnel involved.
- Access to evidence is restricted and managed through role-based controls.
- Data retention policies are suspended temporarily for affected logs and endpoints to preserve historical evidence.

Additionally, I would advise involving the organisation’s legal counsel and Data Protection Officer (DPO) if there is a potential personal data breach, to ensure compliance with the UK GDPR and regulatory breach notification requirements.

Section 5: Advanced Persistent Threats (APTs)

5.1 Testing the Monitoring Solution

To determine whether the monitoring solution I've designed is effective, I recommend conducting a structured and continuous security testing programme that evaluates the system against its defined specifications and objectives. This includes a combination of the following:

- Red Team Engagements: These simulated adversarial exercises are invaluable in testing the full breadth of our monitoring solution. A red team mimics APT behaviour conducting stealthy reconnaissance, lateral movement, and data exfiltration to evaluate if our detection and response workflows are triggered as expected.
- Purple Team Collaboration: Involving both red and blue teams simultaneously allows for real-time tuning of rules, correlation logic, and playbooks. This feedback loop ensures that indicators of compromise (IOCs) and behaviour-based detections are refined.
- Tabletop Exercises and Incident Simulations: These are lower cost but highly effective for evaluating operational readiness, especially from a SOC coordination and escalation perspective.

Testing should occur on a quarterly basis or following any major infrastructure or rule-set changes. A controlled test environment replicating production should be used to avoid operational disruptions while still providing realistic results.

To assess the system's ongoing effectiveness, we will monitor key metrics:

- False Positive Rate (FPR): Targeting an FPR of less than 5% to avoid alert fatigue.
- Mean Time to Detect (MTTD): Aim for an MTTD of less than 30 minutes for lateral movement or data staging events.

5.2 Qualifications of Testers

The credibility and effectiveness of the tests hinge on the expertise of the individuals conducting them. For red team members and penetration testers, I would expect qualifications such as:

- Offensive Security Certified Professional (OSCP): Demonstrates hands-on ability to exploit and bypass defensive mechanisms.
- Certified Red Teamer (CRT) or CREST Registered Penetration Tester: Validates experience with real-world simulation of APT tactics.
- GIAC Penetration Tester (GPEN) or Certified Ethical Hacker (CEH): Beneficial for broader engagements and initial testing phases.

Equally important is their toolset experience. I would look for familiarity with tools such as Cobalt Strike, Metasploit, Empire, and MITRE Caldera - all of which can replicate advanced adversary behaviour. On the defensive side, testers should understand platforms like Splunk, Elastic Stack, Zeek, and Wazuh, since the goal is to verify the detection and response coverage of these tools.

Testers should also possess working knowledge of MITRE ATT&CK, which acts as a common taxonomy for mapping threat behaviours, making detection gaps more visible and actionable.

5.3 Monitoring for APT Threats

Advanced Persistent Threats are sophisticated, stealthy, and often operate over extended durations. In the monitoring architecture, I have implemented multiple mechanisms to address such threats:

- User Behaviour Analytics (UBA) in Splunk: Detects deviations from normal patterns, such as unusual login times, impossible travel, or atypical file access sequences.
- Zeek + Suricata combination: Identifies low-and-slow scanning, DNS tunnelling, protocol misuse, and lateral movement attempts. For instance, a host issuing numerous DNS queries to sequential subdomains could indicate a tunnelling attempt (a known APT tactic).
- Elastic SIEM or Splunk correlation rules: These are configured to map directly to ATT&CK techniques such as T1059 (command-line execution), T1021 (remote services), or T1003 (credential dumping).
- Endpoint Telemetry via Wazuh: Alerts when binaries such as Mimikatz or rundll32.exe behave outside typical usage patterns, suggesting credential access or code injection.

For example, if an APT actor gains access via a phishing payload, UBA will flag abnormal working hours or device usage. Zeek would log unusual port activity, and Suricata might detect malformed packets consistent with exploitation. These indicators, when correlated in the SIEM, would elevate the alert for analyst review.

Section 6: Cost Effectiveness

Implementing a security monitoring architecture, as recommended across Sections 1 to 5, inevitably involves cost. However, I view this not as an expense, but as a strategic investment in the client's long-term operational resilience. The costs can be divided into three areas: equipment and licensing, human resources, and operational inconvenience.

a) Equipment and Software Costs

While core tools such as Wazuh, Zeek, and Suricata are open source, deployment and integration require dedicated hardware and commercial solutions for optimal performance. For example:

- Splunk Enterprise Security licences for moderate log ingestion (20-50 GB/day) may cost £15,000-£25,000 per year (Splunk, 2023).
- Hardware sensors, log storage servers, and backup infrastructure may cost £8,000-£12,000 in initial investment.
- Optional add-ons like UBA and SOAR modules can add £3,000-£7,000 annually.

These costs deliver centralised visibility, high-fidelity alerting, and automated response capabilities. More importantly, they reduce the Mean Time to Detect (MTTD), helping to prevent breaches that, on average, cost UK organisations £3.4 million (IBM, 2023).

b) Human Resource Costs

Security operations are human-intensive. My design relies on trained analysts, engineers, and testers to configure, interpret, and tune the monitoring tools. Cost estimates include:

- £60,000-£90,000 annually per SOC analyst or detection engineer.
- £2,500-£5,000 per individual for certifications such as OSCP, GPEN, or Splunk Core Certified Power User.
- £20,000-£30,000 annually for periodic red/purple team simulations and consultant engagements.

This investment ensures resilience, adaptability, and proactive defence - enabling the client to stay ahead of evolving threats while maintaining compliance and audit readiness.

c) Operational Inconvenience

Some inconvenience is expected during deployment: USB monitoring may affect user habits, endpoint policies could introduce temporary friction, and initial tuning may generate alert noise. These are short-lived challenges. In contrast, an undetected APT or insider attack could result in £150,000-£250,000 per day in operational losses and recovery delays (ENISA, 2023).

References

- MITRE Corporation. (2023). MITRE ATT&CK Framework. Available at: https://attack.mitre.org/
- Open Information Security Foundation. (2023). Suricata Documentation. Available at: https://suricata.io/
- Paxson, V. (1999). Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, 31(23–24), pp.2435–2463.
- Wazuh Inc. (2023). Wazuh Documentation. Available at: https://documentation.wazuh.com/
- Elastic N.V. (2023). Elastic Security Overview. Available at: https://www.elastic.co/security
- Splunk Inc. (2023). Splunk SOAR Playbook Library. Available at: https://www.splunk.com
- Information Commissioner's Office (ICO). (2018). Guide to the GDPR. Available at: https://ico.org.uk
- Cisco Systems. (2023). NetFlow Configuration Guide. Available at: https://www.cisco.com
- The Zeek Project. (2023). Zeek Documentation. Available at: https://docs.zeek.org
- Gartner Research. (2023). Magic Quadrant for SIEM. Available at: https://www.gartner.com
- Magnet Forensics. (2023). RAM Capture Guide. Available at: https://www.magnetforensics.com
- ICO. (2018). Guide to the General Data Protection Regulation (GDPR). Available at: https://ico.org.uk
- SANS Institute. (2022). Incident Response & Digital Forensics. Available at: https://www.sans.org
- SANS Institute. (2023). Purple Team Exercises. Available at: https://www.sans.org
- Offensive Security. (2023). OSCP Certification Overview. Available at: https://www.offensive-security.com
- IBM Security. (2023). Cost of a Data Breach Report 2023. https://www.ibm.com/reports/data-breach
- Splunk Inc. (2023). Pricing Overview. https://www.splunk.com/en_us/products/pricing.html

- ENISA. (2023). Threat Landscape Report 2023. https://www.enisa.europa.eu/publications