Staffordshire & Shropshire Health Informatics Service

Security Operations Centre Executive Summary

[Subject]

Distribution:	All
Document Owner:	Richard McCue (YDDAF) SSHIS

Certificate Number 13963
ISO 27001

Certified customer-led service desk

Gamma Accredited Partner

Microsoft Partner

Document Control

Title:	Security Operations Centre Executive Summary
Reference:	N/A
Status:	Release
Version:	V1.0
Date Issued:	12/05/2025
Last Review Date:	N/A
Next Review Date:	N/A
Document Owner:	Author
Approved by:	N/A

Change History

Date	Version	Author	Comments
09/05/2025	0.1	Rich McCue	Initial Draft
12/05/2025	1.0	Rich McCue	Release

Table of Contents

1 EXECUTIVE SUMMARY

During the reporting period, the Security Operations Centre (SOC) maintained robust surveillance and proactive incident response, successfully monitoring an average of **3.6 billion security events per month**. This comprehensive visibility allowed the SOC to detect and manage threats efficiently across the partnership's digital estate.

Out of these events:

- **63 security alerts** were generated on average per month.
- **37 alerts** were escalated to actionable **security incidents**, each requiring **manual investigation and remediation**.

In addition, all alerts generated by the NHS Central Security Operations Centre (CSOC) were detected and remediated ahead of the receipt of the notifications from the CSOC team.

This performance reflects the SOC's continuous commitment to threat detection, response accuracy, and operational resilience. It also demonstrates the value of local security teams working in collaboration with the CSOC team.

2 KEY METRICS

Metric	Monthly Average
Total Events Monitored	3.6 Billion
Security Alerts Generated	63
Incidents Requiring Intervention	37

The ratio of alerts to events (approx. 0.00000175%) underscores the precision of our filtering mechanisms and correlation engines, ensuring only credible threats reach the analyst.

3 MIGRATION TO SOAR CAPABILITIES

As part of our SOC modernisation roadmap, we have initiated the **migration to Security Orchestration, Automation, and Response (SOAR)** capabilities. This transition is pivotal to enhancing efficiency, scalability, and effectiveness in threat management and response.

3.1 MIGRATION OBJECTIVES:

- **Automate repetitive tasks** such as triage, threat enrichment, and incident categorisation.

- **Standardise response playbooks** for consistent, auditable actions.
- **Reduce mean time to detect (MTTD) and mean time to respond (MTTR)**.
- **Integrate threat intelligence platforms**, ticketing systems, and endpoint protection solutions.
- **Alleviate analyst fatigue** by minimising manual workload on low-complexity incidents.

3.2 SOAR BENEFITS:

Benefit	Description
Efficiency Gains	Routine tasks are automated, freeing analysts to focus on high-impact investigations.
Faster Response Times	Real-time orchestration enables quicker containment and remediation.
Improved Accuracy	Automated threat enrichment reduces human error and ensures consistent incident handling, while ensuring analysts have access to the information they need to make rapid decisions.
Scalability	The SOC can handle increasing alert volumes without a negative effect on response time.
Knowledge Retention	Playbooks codify expert knowledge, reducing dependency on individual expertise.
Compliance & Reporting	Detailed logs and action trails support audit and compliance requirements.

4 CONCLUSION AND OUTLOOK

The SOC continues to operate with a high degree of effectiveness, managing massive volumes of data with precision and diligence. The transition to SOAR marks a significant evolution in our security posture, laying the groundwork for a more agile, intelligent, and responsive cybersecurity operation.

For further information email contactus@sshis.nhs.uk