Samuel Gresty
Worksop, Nottinghamshire | Email: samgresty1@icloud.com | Phone: 07546 839 545
Website: https://sgcs.uk | GitHub: https://github.com/Github-SGCS

Target Roles:

Cyber Security Analyst • Threat Detection Engineer • GRC Analyst • Cloud Security Analyst • Risk Analyst

Summary:

Cybersecurity Analyst with solid experience in Incident Response, Vulnerability Management, Risk Management, PIM, and SIEM engineering. Skilled in leading incidents, collaborating with third-party SOC teams, and enhancing detection logic.
Hands on with Microsoft Sentinel, Defender, Mimecast, Nessus, and Cisco Umbrella. Experienced in audits, access reviews, and remediation projects. Proactive, composed under pressure, and dedicated to ongoing development (currently working towards OSCP certification).

Technical Skills:

Detection & Response:
SIEM (Microsoft Sentinel, Arctic Wolf), KQL queries, alert creation/tuning, Incident triage, phishing investigations.

Vulnerability & Risk Management:
Nessus, Defender, 4Risk Risk management tool

Identity & Access Security:
Active Directory, Azure AD, Conditional Access, User account reviews.

Systems & Infrastructure:
Windows Server, endpoint hardening, VPN, firewall basics, Cisco Umbrella.

Automation & Scripting:
PowerShell (intermediate), Python (foundational), KQL Scripting, Command Prompt.

Frameworks & Methodologies:
MITRE ATT&CK, CIS Benchmarks, ISO27001 awareness.

Tech Tools:

Microsoft Sentinel • Arctic Wolf • Intune • Defender for Endpoint • Nessus • Cisco Umbrella • Mimecast • Exchange • On-Prem AD• Azure AD • Microsoft 365 Security • PowerShell • Windows Server • Linux (Basic)

Professional Experience:

Cybersecurity Analyst | Sciensus | March 2023 – Present

Hybrid Azure / on-prem environment • 500+ users • 1500+ endpoints • Internal Security Team with third-party SOC

Core Responsibilities:

Incident Response & SOC Operations

- Led and chaired multiple high-severity incidents, coordinating with IT, HR, vendors, and third-party SOC.
- Investigated phishing, malware, and sign-in anomalies, preventing compromise of 500+ user accounts.
- Contained incidents by quarantining emails, blocking IOCs, and rebuilding compromised endpoints.

SIEM & Threat Detection

- Built custom KQL queries in Microsoft Sentinel to improve threat hunting and tune detections.
- Reduced false positives by 48%, streamlining analyst workload.
- Developed Sentinel dashboards to report SOC KPIs and incident metrics.

Vulnerability & PIM Management

- Conducted Nessus vulnerability scans and supported remediation.
- Performed privileged access reviews, remediating mailbox, device, and Active Directory permissions.
- Supported patch cycles (building reports and leading patch/vulnerability meetings) and mentored colleagues on Patch My PC, reduced vulnerabilities by 35%

Risk Management

- Experience being the point of contact for the IT team risk management (AI, Patient App, Business Intelligence, Cybersecurity, D365, IT Opps, Enterprise Architecture)
- Built a risk template that was used in our new risk management software (4Risk)

Audit & Compliance

- Contributed to ISO 27001 audit preparation and internal CIS Benchmark reviews.
- Supported external penetration testing engagements by providing evidence and remediation input.

Collaboration & Vendor Liaison

- Partnered with third-party SOC providers for escalations and tuning recommendations.
- Liaised with vendors and internal teams to remediate vulnerabilities and improve detection tooling.

Process & Documentation

- Authored SOPs, knowledge base entries, and workflow guides.
- Delivered incident reports and chaired stakeholder review sessions.

Previous Roles:

Service Desk Engineer	Littlefish, Nottingham	Nov 2022 – Mar 2023
Technical Support Engineer	Opus / Everything Tech	Jan 2022 – Aug 2022
1st Line Support Technician	EMCS	Aug 2021 – Jan 2022
1st Line Support Engineer	Ergo Computing	Nov 2020 – Jul 2021
Kitchen Assistant	Notcutts Garden Centre	Aug 2018 – Nov 2020

Projects & Portfolio (Full details at [https://sgcs.uk]):

Vulnerability Reporting Using KQL

Produced a detailed vulnerability report using Kusto Query Language to highlight and prioritise security weaknesses across the business.

Incident Response Plan (IRP)

Developed a comprehensive incident response plan that outlines detection, containment, eradication, and recovery procedures in case of a security incident.

Certifications & Training:

- OSCP (Offensive Security Certified Professional) – In progress)
- (ISC)² Certified in Cybersecurity (CC) – Scheduled, expected completion: December 2025
- Microsoft SC-900 (Achieved)
- Continuous learning via Self-Study, Webinars and Personal Projects.

Additional Strengths:

- Strong investigative and analytical mindset.
- Ability to improve processes.
- Excellent documentation and communication skills.
- Experience across both IT Service Desk (MSP & Customer facing) and Security Operations.
- Proactive approach to Risk and Vulnerability Management.

Key Achievements:

- Reduced open vulnerabilities by 35% through targeted patching
- Reduced Sentinel false positives by 48% through custom KQL and rule tuning.
- Using Mimecast to prevent phishing attempts to 500+ users, done this by improving rules and policies