Samuel Gresty

samgresty1@icloud.com 07546839545 S80 www.sgcs.uk LinkedIn

Professional Summary:

Cybersecurity Analyst with strong experience in SOC operations, incident response, vulnerability management, PIM, and SIEM engineering. Skilled at leading incidents, collaborating with third-party SOCs, and improving detection logic. Hands-on with Microsoft Sentinel, Defender, Mimecast, Nessus, Cisco Umbrella. Experienced in audits, access reviews, and remediation projects. Proactive, calm under pressure, and committed to professional growth (currently pursuing OSCP certification).

Core Competencies

- SOC Operations & Incident Response: Incident leadership, Investigations, Containment, Escalation
- SIEM & Threat Hunting: Microsoft Sentinel, KQL scripting, custom dashboards
- Threat Detection & Email Security: Phishing analysis, Mimecast tuning, Defender quarantine
- Vulnerability & Access Management: Nessus (Tenable), PIM reviews, Patch cycles
- Cloud & Endpoint Security: Microsoft 365 Defender, Intune, Azure, Cisco Umbrella
- Audit & Compliance: ISO 27001, CIS Benchmarks, External pen-testing exposure
- Infrastructure Security: Windows Server/Desktop, Firewall, DNS
- Collaboration & Vendor Liaison: Third-party SOC, Vendors, HR, IT teams
- Documentation & Process: SOPs, knowledge bases, workflow optimisation

Technical Tools

Security:	Microsoft 365 Defender, Mimecast, Cisco Umbrella, Nessus Scanning, Microsoft Entra Privileged Identity Management (PIM)
SIEM & Scripting:	Microsoft Sentinel, KQL, Basic PowerShell
Infrastructure:	Windows OS, Active Directory, Intune, Azure
Network Security:	Firewalls, DNS
Collaboration & Ticketing:	Microsoft Teams, Outlook, Ivanti

Notable Achievements

- Mail Delivery: Reduced the time it takes for users to receive emails, improving Mimecast policies and rules.
- Vulnerability Management: Scoped and remediated critical vulnerabilities using Nessus and Defender.
- Knowledge Sharing: Created SOC SOPs and mentored new members of the cybersecurity team to use Patch My PC
- Contained a credential phishing campaign with zero business impact.
- Proposed and implemented SOC triage workflow changes, cutting alert handling time.

Professional Experience

Cyber Security Analyst | Sciensus | Mar 2023 – Present

I’m a part of the cybersecurity team at Sciensus, where we help to deliver life changing medicines across Europe. In my role, I focus on protecting our digital infrastructure and keeping sensitive patient data secure. Here are some of the key areas I am responsible for:

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.

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

Certifications

OSCP (Offensive Security Certified Professional) – *In Progress*
SC-900: Microsoft Security, Compliance & Identity Fundamentals – *June 2025*

Education

ICSI: Cybersecurity Masterclass – *July 2022 to March 2023* (Self-Paced Learning)
Fortinet: NSE 1,2,3 – *October 2022*
IT Career Switch: First Line IT Support – *2020* (Self-Paced Learning)
ICSI: Certified Network Security Specialist – *2020* (Self-Paced Learning)
