Samuel Gresty
Worksop, Nottinghamshire | Email: samgresty1@icloud.com | Phone: 07546 839 545
Website | GitHub

## 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.

## Technical Skills:

Detection & response:

SIEM (Microsoft Sentinel, Arctic Wolf) • KQL queries • alert creation/tuning • Incident triage • phishing investigation

Vulnerability & Risk Management:

Nessus • Defender • Pentanar & 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

Automaton & Scripting:

PowerShell (intermediate) • Python (foundational) • KQL scripting (intermediate)

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.

Highlighted entries show key achievements and measurable impact within each role.

### 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.

## Earlier 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

*Summary*

Documenting how I use KQL and Microsoft Excel to showcase the current software vulnerabilities within a business, this includes: age & groupings, device information of effected users. Using a pivot table for easy viewing and clearer understanding of the current security risks.

*Outcome*

A report that can be displayed to the higher management team or easy collaboration within the IT team (Service Desk and any other IT Departments.

*Find the document here.*

### Incident Response Plan (IRP)

*Summary*

Created a full IRP that outlines how a business should detect, contain and recover from a security incident, I wanted to capture a consistent and well-coordinated approach.

*outcome*

The IRP strengthens the organisation readiness; it improves response times and helps with clearer decision makings during an incident.

*Find the document here.*

## Certifications & Education:

### Certifications

- Microsoft SC-900 (Achieved)

### Education

- ICSI: Cybersecurity Masterclass – July 2022 to March 2023
- Fortinet: NSE 1,2,3 – October 2022
- IT Career Switch: First Line IT Support – January to December 2020
- ICSI: Certified Network Security Specialist- 2020

Highlighted entries show key achievements and measurable impact within each role.