Making a Career in Security Operations

SOC & Blue Team

Detect. Investigate. Respond. The frontline of cyber defence.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 08 of 12
AUDIENCE	Students and professionals entering the blue team and SOC

[08:26:34] INFO PROXY-01 Periodic outbound beacon

SOC

Contents

Digitally signed by Baba Shaheer Gutappa
Date: 2026.04.22 10:43:22 +01'00'

1. What Is a Security Operations Centre?

A Security Operations Centre — SOC — is the team responsible for monitoring an organisation's systems 24 hours a day, seven days a week, looking for signs of attack. When something suspicious happens — an unusual login, a process injecting into memory, a server talking to a known malicious IP — the SOC sees it, investigates it and responds.

The SOC is the defensive backbone of any mature security programme. While ethical hackers simulate attacks and AppSec engineers prevent vulnerabilities in code, the SOC is the team that fights real attacks in real time. It is the most common entry point into cybersecurity — and one of the fastest ways to build broad security knowledge across networks, endpoints, cloud and identity.

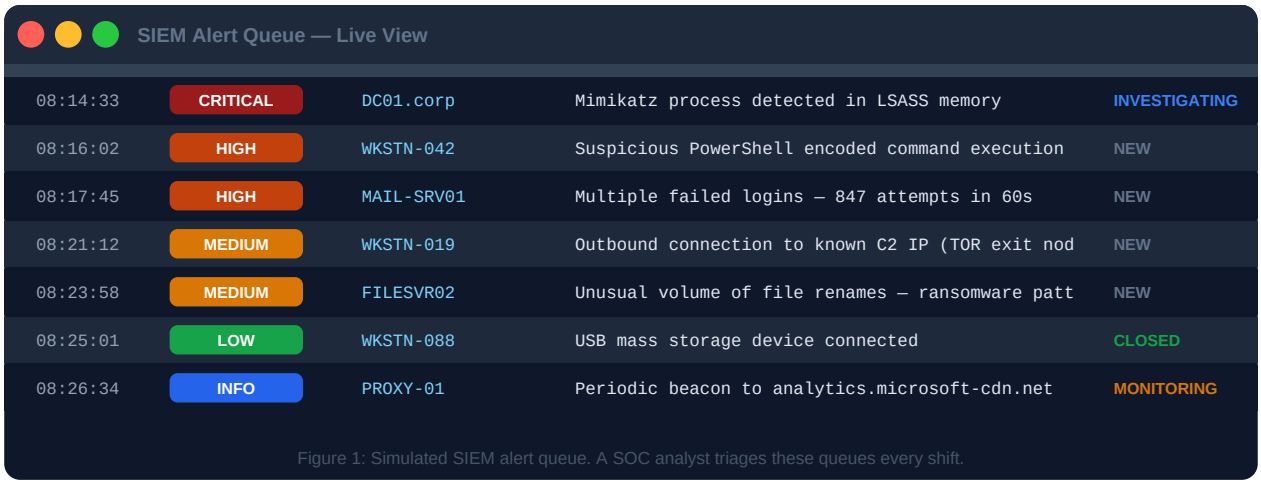


Figure 1: Simulated SIEM alert queue. A SOC analyst triages these queues every shift.

The SOC is the most accessible entry point into cybersecurity.
Tier 1 SOC analyst roles are genuinely available to people with Security+ or BTL1 and 6–12 months of structured study. No degree required.

Level	Typical UK Salary	Roles
Tier 1 / Junior	£22,000 – £35,000	SOC Analyst Tier 1, Junior Security Analyst, NOC/SOC hybrid
Tier 2 / Mid	£35,000 – £55,000	SOC Analyst Tier 2, Senior Security Analyst, Incident Responder
Tier 3 / Senior	£55,000 – £80,000	Threat Hunter, SOC Lead, Detection Engineer, SIEM Engineer
SOC Manager	£70,000 – £100,000+	Head of SOC, Security Operations Manager, VP of SecOps

Table 1: UK salary ranges for SOC and blue team roles (CW Jobs, 2024)

2. SOC vs Blue Team vs Red Team

These terms get used interchangeably — but they mean different things. Understanding the distinction helps you target the right roles.

	SOC	Blue Team	Red Team
Focus	Detecting and responding to live threats	Improving defensive capabilities and detection	Simulating attacker techniques to test defences
Mode	Reactive — monitors and responds to alerts	Proactive — builds better detection and controls	Offensive — attacks with permission to find gaps
Working hours	24/7 shift coverage, rotation	Business hours, project-based	Engagement-based, flexible
Key output	Incident tickets, containment actions	Detection rules, playbooks, architecture improvements	Pentest report, attack simulation findings
Overlap	Heavy — blue team often embedded in SOC	Works closely with SOC and IR teams	Works with blue team on purple team exercises
Entry path	Security+, BTL1, Tier 1 SOC role	From SOC Tier 2/3 or engineering background	From pentesting / ethical hacking background

Table 2: SOC vs Blue Team vs Red Team

3. The SOC Tier Structure

Most SOCs operate a tiered model. Alerts arrive at Tier 1, are investigated and escalated if needed to Tier 2, and the most complex cases go to Tier 3. This is the career ladder — each tier builds on the last.

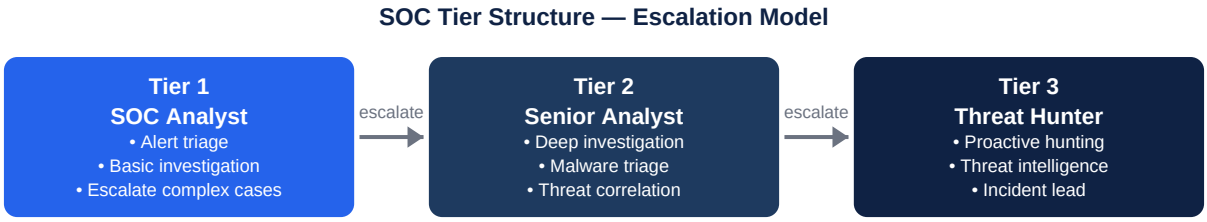


Figure 2: SOC tier structure. Most careers start at Tier 1 and progress upward.

Tier	Role	Experience Needed	What You Learn
Tier 1	SOC Analyst	Entry level — Security+ or BTL1, basic networking	Alert triage at speed, SIEM navigation, playbook execution, ticket writing, escalation judgement
Tier 2	Senior SOC Analyst	1–3 years Tier 1, deeper investigation skills	Malware triage, threat correlation, writing detection rules, mentoring, incident handling

Tier	Role	Experience Needed	What You Learn
Tier 3	Threat Hunter / Detection Engineer	3+ years, strong scripting and threat intel knowledge	Proactive hunting, SIEM rule development, custom tooling, threat intelligence integration
SOC Lead / Manager	Head of SOC	5+ years operational, team leadership experience	Team management, metrics, SLA ownership, vendor management, board-level reporting

Table 3: SOC tier breakdown — roles, experience and what you build

4. What a SOC Analyst Actually Does Day to Day

People imagine SOC analysts sitting in dark rooms watching screens full of scrolling red text. The reality is more structured — and more interesting. A Tier 1 analyst's shift follows a clear rhythm: review the queue, triage alerts, investigate findings, escalate or close, document everything, and hand over cleanly to the next shift. Here is an honest breakdown:

Activity	% of Shift	What This Looks Like
Alert triage	35–45%	Working through the alert queue. For each alert: determine if it is a true positive or false positive. Close clearly false positives. Escalate anything suspicious.
Investigation	20–30%	For confirmed or suspected true positives — pivot across logs, pull endpoint data from EDR, check threat intel feeds, build a timeline.
Ticket management	10–15%	Opening, updating and closing incident tickets. Documentation must be clear — the next analyst picking up the ticket needs to understand exactly what has been done.
Shift handover	5–10%	Briefing the incoming shift on any open incidents, active investigations and anything to watch. Clean handovers prevent things falling through the gaps.
Rule tuning / improvement	5–10%	Flagging noisy rules that generate too many false positives. Suggesting refinements. Writing up patterns seen during the shift.
Training / self-development	5%	Reviewing threat intelligence briefings, reading about new attack techniques, completing platform training.

Table 4: Typical Tier 1 SOC analyst shift breakdown

Shift work is a real part of SOC life.
Most enterprise SOCs run 24/7 — that means nights, weekends and bank holidays.
MSSP SOCs almost always include a shift rotation. Factor this into your decision.

5. Alert Triage — The Core SOC Skill

Alert triage is the most fundamental SOC skill. An alert fires. You have limited time. You need to decide: is this real? How serious? What needs to happen next? Do this badly and real attacks slip through. Do it well and you catch intrusions before they cause damage. Here is the triage process every SOC analyst follows:

- **1. Read the alert — understand exactly what it is saying.** What rule fired? What data triggered it? What host, user and time are involved? Never investigate an alert you have not fully read.
- **2. Check the context.** Is this host normally noisy? Has this user done this before? Is there a maintenance window or software deployment that could explain it? Context turns noise into signal.
- **3. Pivot across data sources.** An alert from the SIEM is just a starting point. Pull the full log, check the EDR for what the process was doing, look at firewall logs for network connections, check authentication logs for the user.
- **4. Check threat intelligence.** Look up IPs, domains and file hashes in your threat intel feeds — VirusTotal, AbuseIPDB, internal IOC lists. Does this match a known threat actor or malware family?
- **5. Make a decision: True Positive, False Positive or Needs More Investigation.** True Positive → escalate or respond. False Positive → close with clear reason. Unsure → keep investigating and flag for Tier 2.
- **6. Document everything.** Every action taken, every data source checked, every decision made. If you escalate, the Tier 2 analyst must be able to pick up exactly where you left off without asking questions.

Common alert types and what they usually mean

Alert Type	Common Cause	True Positive Indicators	Quick Action
Failed login spike	Password spray or brute force	Single source IP, accounts in sequence, off-hours	Block IP, lock account, escalate to Tier 2
Encoded PowerShell	Malware or legitimate admin tool	Base64 decoded payload contains download/exec	Pull full command, check parent process, escalate
Outbound to known C2	Malware beacon or false positive domain	Repeated interval, no user interaction, unusual port	Block domain/IP, isolate host, escalate immediately
Large data transfer	Exfiltration or legitimate backup	Unusual destination, outside business hours, compressed	Identify destination, check user context, escalate
New admin account created	Attacker persistence or legitimate IT change	No change ticket, created by non-IT user, odd name	Verify with IT, disable if unauthorised, escalate
Process injection (EDR)	Malware or pentest	LSASS or svchost as target, unexpected parent	High priority — escalate immediately to Tier 2

Table 5: Common SOC alert types and triage guidance

6. SIEM Platforms — The SOC's Central Tool

A Security Information and Event Management (SIEM) platform collects logs from every source in the environment — firewalls, endpoints, servers, cloud services, identity providers — and correlates them in real time. When a pattern matches a detection rule, an alert fires. The SIEM is where SOC analysts spend the majority of their shift. Knowing how to query it efficiently is non-negotiable.

SIEM Platform	Market Position	Query Language	Free for Learning?
Microsoft Sentinel	Enterprise market leader in UK/Azure shops	KQL — Kusto Query Language	Yes — Azure free trial + many free labs
Splunk	Largest installed base globally, especially financial sector	SPL — Search Processing Language	Yes — Splunk Free / Boss of the SOC CTF
IBM QRadar	Enterprise, common in regulated industries and government	AQL — Ariel Query Language	Yes — QRadar Community Edition
Elastic SIEM	Open-source friendly, growing fast in mid-market	Lucene / EQL / KQL	Yes — Elastic free tier, Elastic SIEM is open-source
Google Chronicle	Cloud-native SIEM, growing in large enterprise	YARA-L, UDM search	Limited — via Google Cloud trial
Exabeam	UEBA-focused, behaviour analytics	Natural language + advanced analytics	Limited — demo environment available

Table 6: Major SIEM platforms — which to learn and how to access them for free

What good SIEM queries look like

Writing efficient SIEM queries is a core SOC skill. Here is an example in KQL (Microsoft Sentinel) — hunting for successful logins after multiple failures, a pattern consistent with a successful brute-force attack:

KQL example — detect successful login after 10+ failures from same IP:

```
let threshold = 10;
SigninLogs
| where ResultType != '0'  // failed logins
| summarize FailCount = count() by IPAddress, bin(TimeGenerated, 1h)
| where FailCount >= threshold
| join kind=inner (SigninLogs | where ResultType == '0') on IPAddress
| project IPAddress, FailCount, SuccessTime = TimeGenerated1
```

Start with Splunk Free and Microsoft Sentinel (Azure free trial).
Boss of the SOC (BOTS) from Splunk is the best free SOC training dataset.
TryHackMe and CyberDefenders both offer free SIEM labs with real log data.

7. EDR — Endpoint Detection and Response

Endpoint Detection and Response (EDR) tools are agents deployed on every endpoint — laptops, servers, cloud instances — that record everything happening at the process level. Every process started, every file written, every network connection made, every registry key modified. This telemetry feeds into the SOC, where analysts use it to investigate alerts and hunt for threats.

EDR goes far beyond traditional antivirus. Where AV matches files against known signatures, EDR uses behavioural detection — spotting process injection, lateral movement, credential dumping and fileless malware even when no known signature exists.

EDR Platform	Market Share	Key Features	Used Most In
CrowdStrike Falcon	Market leader	Excellent threat graph, threat intelligence integration, AI detection	Financial services, large enterprise, government
Microsoft Defender for Endpoint	Very large — native Azure/M365	Deep integration with Sentinel SIEM, identity, cloud. MDE + Sentinel is common UK stack.	Microsoft-heavy organisations, public sector
SentinelOne	Growing fast	Autonomous response (kills malware automatically), strong MITRE ATT&CK; coverage	Tech companies, MSSPs
Palo Alto Cortex XDR	Strong enterprise	XDR — extends beyond endpoint to network and cloud	Large enterprise, financial sector
Carbon Black (VMware)	Established	Strong process tree visualisation, good for forensics investigation	Healthcare, enterprise
Elastic EDR	Open-source friendly	Free tier available. Good for learning EDR concepts in a lab.	SMEs, security-conscious startups, learning labs

Table 7: Major EDR platforms — market position and use cases

8. Threat Hunting — Going Beyond Alerts

Reactive SOC work — waiting for alerts to fire — will always miss some attacks. Sophisticated threat actors operate below detection thresholds deliberately. Threat hunting is the proactive practice of searching your environment for attacker activity that has not yet triggered any alert. Hunters do not wait to be told something is wrong — they go looking.

Figure 3: The threat hunting loop — hypothesis-driven, iterative, intelligence-led.

How a hunt works — a practical example

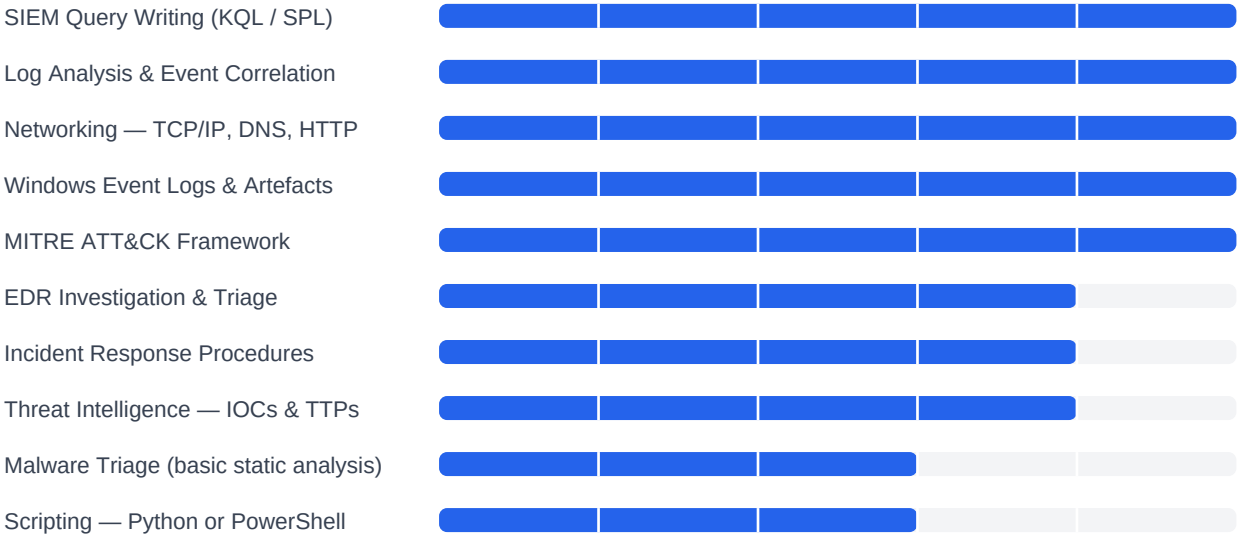
Hypothesis: Based on a threat intelligence report that a ransomware group is targeting UK financial institutions using Living-off-the-Land (LotL) techniques, I hypothesise there may be unusual WMI or scheduled task activity in our environment that has not triggered any alerts.

- **Collect:** Pull 30 days of Windows event logs (Event ID 4698 — scheduled task created) from all servers via the SIEM. Pull EDR telemetry for wmic.exe and schtasks.exe process executions.
- **Analyse:** Baseline what is normal — which hosts regularly create scheduled tasks, which users, which times of day. Filter out the noise.
- **Hunt:** Look for anomalies — scheduled tasks created by users who do not normally create them, at unusual hours, pointing to executables in TEMP directories, or using encoded commands.
- **Discover:** Find a scheduled task on a finance workstation created at 02:30 AM pointing to a PowerShell script in %APPDATA%. No alert fired because the task was created by a legitimate admin account — compromised three weeks earlier.
- **Report:** Escalate to incident response. Document the full finding with evidence. Create a new SIEM detection rule so this pattern triggers an alert in future.

Threat hunting is a Tier 2/3 activity — not for day one.
But understanding the MITRE ATT&CK framework from day one accelerates your progression toward it. Every Tier 1 alert maps to an ATT&CK technique.

9. Core Skills You Need to Build

Skills expected at Tier 2 SOC analyst level:



The MITRE ATT&CK; Framework — essential SOC knowledge

MITRE ATT&CK; is a publicly accessible knowledge base of adversary tactics, techniques and procedures (TTPs) based on real-world observations. Every SOC analyst must know it. Every alert you triage maps to one or more ATT&CK; techniques. Every threat intel report references it. Every detection rule is ideally tagged to it.

ATT&CK; Tactic	What It Represents	SOC Relevance
Initial Access	How attackers get in — phishing, exploit, supply chain	Email gateway alerts, web proxy logs, VPN anomalies
Execution	Running malicious code — PowerShell, WMI, scripts	EDR process alerts, SIEM PowerShell/script events
Persistence	Staying after reboot — scheduled tasks, registry run keys	New scheduled task events, registry modification alerts
Privilege Escalation	Gaining higher permissions — exploit, token theft	Unexpected admin account creation, token manipulation
Defence Evasion	Hiding from security tools — disabling AV, obfuscation	AV disabled events, encoded command execution
Credential Access	Stealing passwords — Mimikatz, LSASS dump, keylogging	LSASS access alerts, unusual process accessing credential store
Lateral Movement	Moving between systems — RDP, SMB, pass-the-hash	RDP from unexpected source, SMB file share access anomalies
Exfiltration	Stealing data — HTTPS, DNS tunnelling, cloud upload	Large outbound transfers, unusual DNS query volumes

ATT&CK; Tactic	What It Represents	SOC Relevance
Command & Control	Attacker communicating with implant — HTTP/S beacons	Periodic outbound to new/suspicious domains or IPs

Table 8: MITRE ATT&CK; tactics relevant to SOC alert triage

10. Career Paths in Security Operations

The SOC is not just a starting point — it is a career in itself with clear progression. It is also one of the best launch pads for almost every other cybersecurity specialism. DFIR, threat intelligence, malware analysis, AppSec — all are much easier to enter after SOC experience.

Role	What You Do	Where You Work	UK Salary
SOC Analyst Tier 1	Alert triage, basic investigation, playbook execution, ticket logging.	MSSP, enterprise SOC, government	£22k–£35k
SOC Analyst Tier 2	Deep investigation, malware triage, threat correlation, playbook writing, Tier 1 mentoring.	MSSP, enterprise SOC	£35k–£55k
Threat Hunter	Proactive hunting for undetected threats. Hypothesis-driven, intelligence-led.	Large enterprises, specialist firms	£55k–£75k
Detection Engineer	Write, tune and maintain SIEM detection rules and EDR policies. Bridge security and engineering.	Tech companies, financial services	£55k–£80k
SIEM Engineer	Build, maintain and optimise SIEM infrastructure. Log onboarding, correlation rule development.	Large enterprises, MSSPs	£55k–£75k
Incident Response Analyst	Lead active incident response — contain, eradicate, recover, report.	IR firms, MSSP, enterprises	£50k–£80k
SOC Manager / Head of SOC	Run the SOC team — staffing, SLAs, metrics, tooling, board reporting.	Enterprises, MSSPs	£70k–£100k+

Table 9: Career paths in security operations (Reed, 2024; CW Jobs, 2024)

The SOC is the best springboard in cybersecurity.
A year in a busy SOC gives you exposure to real attacks across every domain — network, endpoint, cloud, identity, malware. Nothing else builds breadth this fast.

11. The Learning Roadmap

The SOC has the most accessible learning path of any cybersecurity specialism. Good free resources, clear certifications, and entry roles that genuinely accept people without degrees or prior experience. Follow this order.

1 — Learn networking fundamentals
TCP/IP, DNS, HTTP, subnetting, common ports and protocols. You cannot investigate network-based alerts without understanding what normal traffic looks like. Professor Messer's free Network+ course. 4–6 weeks.

2 — Learn Windows fundamentals and event logs
Understand Active Directory, Windows Event IDs (4624, 4625, 4688, 4698, 4732…), the registry, common attacker techniques on Windows. TryHackMe Windows Fundamentals path is free and structured. 3–4 weeks.

3 — Get hands-on with a SIEM
Sign up for Splunk Free. Download the Boss of the SOC (BOTS) dataset. Work through all the challenges — they simulate real SOC investigations across realistic log data. Then try Microsoft Sentinel on the Azure free trial. Ongoing.

4 — Learn the MITRE ATT&CK framework
Go to attack.mitre.org. Read through every tactic and technique. Understand what each one looks like in logs. The ATT&CK Navigator is free — build a heatmap of techniques you have practised detecting. 2–3 weeks.

5 — Practice on TryHackMe and CyberDefenders
TryHackMe SOC Level 1 path (free). CyberDefenders blue team labs — real pcap files, real log data, guided investigations. Blue Team Labs Online for additional challenges. Target: complete at least 20 guided investigation labs. Ongoing.

6 — Study for CompTIA Security+
Validates your broad security foundations. Required for many UK SOC roles — especially government, defence and MSSP positions. Professor Messer's free course. Sit the exam once you have the fundamentals solid. 6–8 weeks study.

7 — Get BTL1 — Blue Team Level 1
The most respected practical certification for junior SOC roles in the UK. Covers phishing analysis, threat intelligence, SIEM, digital forensics, incident response and network analysis. Practical exam — 24 hours. Well worth the investment.

8 — Apply for Tier 1 SOC roles
Write-up your BOTS and CyberDefenders challenge solutions. Create a GitHub with any SIEM queries you have written. Apply to MSSP Tier 1 roles, government SOC apprenticeships and graduate schemes. With Security+ and BTL1, you are genuinely competitive.

Realistic timeline from zero to Tier 1 SOC: 9–14 months.
The SOC has the shortest entry timeline of any cybersecurity role.
Boss of the SOC (BOTS) + TryHackMe SOC Level 1 path is the best free combination.

12. Certifications That Matter

SOC certifications split clearly between theoretical (Security+, CySA+) and practical (BTL1, GCIH). For entry-level roles, practical certifications carry significant weight because they prove you can actually do the work.

Certification	Level	Provider	Focus	Why It Matters
CompTIA Security+	Beginner	CompTIA	Broad security foundations — threats, monitoring, incident response basics	Baseline for many UK SOC roles. Required for government and MOD positions. Good first cert.
BTL1 — Blue Team Level 1	Beginner–Mid	Blue Team Labs Online	Practical SOC skills — phishing, SIEM, threat intel, DFIR, network analysis	Highly regarded by UK hiring managers for Tier 1 roles. 24-hour practical exam. Excellent value.
CompTIA CySA+ (CS0-003)	Mid	CompTIA	Cybersecurity analyst skills — threat detection, analysis, response, reporting	Good step-up from Security+. Validates more analytical capability.
SC-200 — Microsoft Security Operations Analyst	Mid	Microsoft	Sentinel, Defender for Endpoint, Defender for Cloud — the Microsoft SOC stack	Highly valued in organisations running Microsoft security tools — a large portion of UK enterprises.
GCIH — GIAC Certified Incident Handler	Mid	GIAC / SANS	Incident handling — detection, response, containment across attack categories	Respected across industries. Good for Tier 2 and incident responder roles.
GCIA — GIAC Certified Intrusion Analyst	Mid	GIAC / SANS	Network intrusion analysis — packet capture, protocol analysis, network forensics	Excellent for network-heavy SOC roles and Tier 2/3 analysts.
GCFE / GCFA — GIAC Forensics	Mid	GIAC / SANS	Digital forensics — complements SOC work for incident response depth	Natural progression for Tier 2 analysts moving toward DFIR specialisation.

Table 10: SOC and blue team certifications in order of progression

13. Case Study — Catching a Live Intrusion

> This is a fictional case study based on real-world SOC incident patterns.
> It walks through a complete Tier 1 → Tier 2 → Incident Response escalation in real time.

The Organisation and the Tuesday Night Shift

Harrington Financial Services is a UK investment firm with 600 staff. Their SOC runs 24/7 with a two-analyst night shift. At 02:14, Priya — a Tier 1 analyst six months into the role — picks up a new CRITICAL alert from CrowdStrike Falcon: **Suspicious LSASS access — credential dumping detected on DC01.**

02:14 — The alert lands

CRITICAL: Mimikatz-style LSASS access on DC01

Priya reads the alert carefully. CrowdStrike has flagged a process called 'svchost32.exe' attempting to open a handle to lsass.exe with PROCESS_VM_READ permissions — the classic signature of credential dumping.

First action: check if this is a known tool or a scheduled task. She pivots to the process tree in Falcon. Parent process: cmd.exe. Grandparent: winrm.exe. This is not a scheduled task — someone ran a remote command on the domain controller.

02:19 — Pivoting across data sources

Sentinel SIEM investigation — login context

Priya queries Sentinel for authentication events on DC01 in the last 2 hours. She finds a successful WinRM login at 01:58 from WKSTN-019 — a finance workstation. The account: svc_backup — a service account that should never log in interactively.

She queries for svc_backup activity. It last authenticated 14 days ago during a scheduled backup job. Tonight's login came from an IP that also appears in AbuseIPDB as a known Cobalt Strike C2 relay — but the internal source is

02:31 — Escalation to Tier 2

Priya escalates — Tier 2 analyst James takes over

Priya documents everything — the process tree, the WinRM login, the IP, the SIEM query results — and escalates with a clear summary: 'Suspected credential dumping on DC01 by svc_backup account, accessed from WKSTN-019. Possible C2 relay involved.'

James immediately isolates WKSTN-019 via CrowdStrike. He pulls a memory image using WinPmem before isolation completes. Volatility analysis of the RAM image finds an injected Cobalt Strike beacon in explorer.exe — active for 9

The timeline reconstructed

Time	Event	Source	Action
Day -9, 14:32	Phishing email delivered to finance@harrington.co.uk	Email gateway logs	Not detected — bypassed spam filter
Day -9, 14:47	User clicked link — macro-enabled Excel downloaded and opened	EDR process logs	No alert — macro detection not enabled

Time	Event	Source	Action
Day -9, 14:48	Cobalt Strike beacon injected into explorer.exe	Memory (found Day 0)	Silent — 9 days dwell time
Day -6	Attacker enumerates AD — BloodHound run	LDAP query logs	Not detected
Day -2	svc_backup password extracted from cached credentials	Not detected until Day 0	—
02:14 today	LSASS access attempt on DC01 triggers CrowdStrike alert	EDR alert	CRITICAL — Priya investigates
02:31	WKSTN-019 isolated. Memory captured. IR engaged.	SOC action	Containment — attacker evicted

Table 11: Reconstructed attack timeline — 9-day dwell time before detection

What the SOC did well — and what needed improving

- **Well:** Priya read the alert carefully and did not close it as a false positive despite svchost being a common process name
- **Well:** She pivoted across multiple data sources — EDR, SIEM, threat intelligence — before escalating
- **Well:** Her escalation documentation was clear enough that James could act immediately without asking questions
- **Well:** Memory was captured before isolation — preserving evidence including the beacon configuration
- **Improve:** Macro execution in Office documents should have been blocked by policy — this would have prevented initial access
- **Improve:** 9 days of beacon activity with no detection means the C2 domain had not been blacklisted — improve threat intel feed coverage
- **Improve:** Service accounts should have been monitored for interactive logins — a simple detection rule that was missing

Priya was 6 months into her first SOC role.
Her careful triage — not closing a noisy alert, pivoting across sources, documenting clearly — is what caught an active intrusion before it reached the domain controller fully.

14. Breaking In — Getting Your First Role

The SOC is the most achievable first cybersecurity role. MSSPs hire regularly at Tier 1 and are genuinely willing to train people with the right attitude, demonstrable practical knowledge and the right certifications. You do not need a degree or years of IT experience.

Build visible evidence of SOC capability

- **TryHackMe SOC Level 1 path:** Complete the entire free path. Your public profile shows every room completed. Employers in this space know the platform — a completed SOC path is a credible signal
- **Boss of the SOC (BOTS) write-ups:** Work through BOTS challenges and write up your investigation methodology. 'I found X by querying Y and pivoting to Z' — this demonstrates real SOC thinking
- **CyberDefenders blue team labs:** Work through the free labs — they use real log data and real malware. Write up your findings as if they were incident reports
- **Home SIEM lab:** Run a free Elastic SIEM or Wazuh instance at home. Feed it logs from a Windows VM. Write a detection rule. Screenshot the alert it generates. This is a genuine differentiator
- **BTL1 certification:** The certification itself is strong evidence of practical skill. Many UK hiring managers will interview any BTL1 holder for a Tier 1 role

Where to Look	Notes
CyberSecurityJobs.com	Search 'SOC analyst tier 1', 'junior security analyst', 'security operations'
LinkedIn	MSSPs post here constantly. Connect with SOC team leads and hiring managers directly
MSSP direct applications	Apply directly to companies like Secureworks, Trustwave, BT Security, Telefonica Tech, NTT — all run large SOC teams
UK Government / NCSC / MOD	Public sector SOC roles — structured, good training, often accept Security+ as baseline
Graduate schemes	BAE Systems, GCHQ, Leidos, Capgemini all run cybersecurity graduate programmes with SOC rotations
Apprenticeships	Degree apprenticeships in cybersecurity are available at several large employers — fully funded, earn while you learn

Table 12: Where to find SOC and blue team roles

Interview questions to prepare for

- Walk me through how you would triage an alert for a successful login after multiple failures.
- What Windows Event IDs would you look for to detect a user account being added to the Domain Admins group?
- What is the difference between a true positive and a false positive? Give an example of each.
- An EDR alert fires for PowerShell with a base64-encoded command. What do you do first?
- What is lateral movement? Name two techniques an attacker might use and how you would detect them.
- What is the MITRE ATT&CK; framework and how would you use it in your daily work?

- You see outbound traffic to an IP you do not recognise at regular intervals. How do you investigate?
- What is threat hunting and how does it differ from reactive alert triage?

> **The best SOC interview answer:**
> "Here is my TryHackMe profile. Here is a BOTS investigation write-up I did."
> Practical evidence of hands-on work consistently beats theoretical knowledge alone.

15. References

1. Blue Team Labs Online (2024) *BTL1 — Blue Team Level 1 Certification.* Available at: https://www.blueteamlabs.online [Accessed: 10 April 2026].

2. CompTIA (2024) *CySA+ Cybersecurity Analyst Certification.* Available at: https://www.comptia.org/certifications/cybersecurity-analyst [Accessed: 10 April 2026].

3. CrowdStrike (2024) *Falcon Platform — EDR and Threat Intelligence.* Available at: https://www.crowdstrike.com/platform/ [Accessed: 11 April 2026].

4. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 11 April 2026].

5. CyberDefenders (2024) *Blue Team Labs and Challenges.* Available at: https://cyberdefenders.org [Accessed: 11 April 2026].

6. GIAC (2024) *GCIH and GCIA Certification Overview.* Available at: https://www.giac.org/certifications/security-operations [Accessed: 12 April 2026].

7. Microsoft (2024) *SC-200: Microsoft Security Operations Analyst.* Available at: https://learn.microsoft.com/en-us/certifications/security-operations-analyst/ [Accessed: 12 April 2026].

8. MITRE Corporation (2024) *ATT&CK; — Adversarial Tactics, Techniques and Common Knowledge.* Available at: https://attack.mitre.org [Accessed: 12 April 2026].

9. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 13 April 2026].

10. Splunk (2024) *Boss of the SOC (BOTS) — Free SOC Training Dataset.* Available at: https://bots.splunk.com [Accessed: 13 April 2026].

11. TryHackMe (2024) *SOC Level 1 Learning Path.* Available at: https://tryhackme.com/path/outline/soclevel1 [Accessed: 13 April 2026].

12. Verizon (2023) *Data Breach Investigations Report 2023.* Available at: https://www.verizon.com/business/resources/reports/dbir/ [Accessed: 14 April 2026].

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 08 of 12.