Jordan Millar

Lead Detection Engineer · SOC Build-Out & Team Lead · Microsoft Sentinel & Defender XDR

Relocating to the UK from the UAE — available immediately, no notice period required | Inverness, Scotland (returning)

+44 7405 820199 | Jordan.millar@hotmail.co.uk | LinkedIn · TryHackMe · Credly

British citizen — full, unrestricted UK right to work, no sponsorship required

Open to permanent or contract (inside IR35 / PAYE) — onsite, hybrid or remote, UK-wide

PROFILE

Lead Detection Engineer who built a multi-tenant MSSP SOC from the ground up and led a team of five, sustaining a 91% detection validity rate across client tenants. Nine years across five SOCs, specialising in Microsoft Sentinel and Defender XDR detection engineering, detection-as-code and SOAR automation.

Several years as a Senior/Lead analyst mentoring and developing junior staff across both MSSP and internal SOC environments, comfortable owning the interface between service provider and client. Seeking a Lead, Principal or SOC Management role in the UK, permanent or contract.

CORE TECHNICAL SKILLS

Leadership: SOC build-out & operating model design, team management (5 analysts), shift & workload planning, process/procedure authorship, analyst mentoring & development, SOC QA/QC

SIEM / XDR: Microsoft Sentinel, Microsoft Defender XDR, Splunk, Elastic, ArcSight, IBM QRadar, LogRhythm, Huntsman

Detection Engineering: KQL, detection-as-code (versioned YAML detection packages), MITRE ATT&CK mapping & coverage assessment, rule tuning & lifecycle management, BAS (AttackIQ), Sigma & YARA

SOAR / Automation: Azure Logic Apps (Playbooks), Python (automation & tooling)

EDR: CrowdStrike, Defender for Endpoint, Carbon Black, FireEye

Cloud / Multi-tenant: Azure, Azure Lighthouse, cross-tenant querying (union / workspace()), Sentinel Content Hub

Domains: Incident Response, Threat Hunting, Digital Forensics, Exposure Management, SOC QA/QC

PROFESSIONAL EXPERIENCE

Lead Detection Engineer / CSOC Analyst L3 — Blackford Technologies (Abu Dhabi, UAE) Feb 2026 - Aug 2026

Role ended by redundancy - the company ceased trading and closed its UAE office. Available immediately; written confirmation available.

- Led the build-out of a multi-tenant MSSP SOC from the ground up in a startup environment, defining the operating model, processes, procedures and overall detection strategy.
- Managed five SOC resources: shift coverage, holiday planning, workload allocation and the direction of the detection engineering pathway.
- Sustained a 91% detection validity rate across the client estate (proportion of fired alerts confirmed as actionable), through systematic tuning and rule lifecycle governance.
- Owned the end-to-end detection lifecycle across multiple client tenants in Microsoft Sentinel and Defender XDR, authoring, tuning and retiring KQL analytics mapped to MITRE ATT&CK.
- Operated a detection-as-code workflow: detections packaged as versioned YAML with structured metadata, reviewed and deployed repeatably across tenants rather than hand-configured per environment. Built cross-tenant hunting via Azure Lighthouse and union / workspace() federation.
- Designed and shipped Azure Logic Apps automation for high-volume alert classes, and authored SOPs and playbooks spanning incident response, detection engineering and SOAR.

Senior SOC Analyst — BestSecret (Germany) Sep 2024 - Jan 2026

- Senior analyst in an internal Microsoft/Azure SOC, leading incident response across the Azure stack from triage through containment to post-incident review.
- Authored KQL detections for the internal estate and validated coverage through breach-and-attack simulation (AttackIQ), closing gaps identified against MITRE ATT&CK.
- Automation-focused remit: built multiple Azure Logic Apps playbooks that removed repetitive workload from the daily analyst queue, and developed Python tooling for enrichment and parsing.
- Led an exposure-management initiative, improving overall security posture through research, prioritisation and remediation recommendations.
- Ran baseline and hypothesis-driven threat hunts, feeding findings back into the detection backlog.

Senior Threat Analyst (progressive roles) — Proficio Jan 2020 - Aug 2024

Senior Threat Analyst Oct 2022 - Aug 2024

- Senior SIEM/EDR incident response across Elastic, Splunk, ArcSight, CrowdStrike, Defender and Microsoft Sentinel in a multi-client MSSP environment.

- Built and owned the SOC Quality Assurance / Quality Control system, driving consistency of analysis and investigation quality across the analyst team.
- Designed the Skills Development Matrix, giving analysts a structured framework for progression and capability development within the SOC.
- Delivered rule analysis and tuning that raised true-positive quality, improving the value delivered to clients and reducing wasted analyst effort.

Splunk Content Developer Feb 2021 - Oct 2022

- Developed custom detection use cases to client specification across authentication, malware/ransomware, suspicious geolocation and other scenarios, spanning multiple industries and sectors.
- Applied MITRE ATT&CK to build rules, dashboards and reports that measurably improved detection coverage across the client base.
- Troubleshot dashboards, rules, data models and other Splunk SIEM components, improving security visibility and lowering Mean Time to Detect (MTTD).

Advanced Threat Analyst Jan 2020 - Feb 2021

- Intermediate and advanced incident response across the full tool suite, with a focus on customer and SOC impact: reducing alert volume and improving documentation and process.
- Direct customer interaction by phone and email, providing recommendations, support and escalation of significant issues.
- Consistent top performer across all measured metrics: ticket volume, customer impact and tuning recommendations.

Threat Analyst to Senior Threat Analyst — ReliaQuest (Dublin, Ireland) Apr 2018 - Dec 2019

- Advanced SIEM and EDR analysis across authentication attacks, ransomware and malware, phishing and other threat classes.
- Tooling included LogRhythm, Splunk, IBM QRadar, Carbon Black and FireEye.
- Consistently excelled across ticket volume, tuning recommendations, customer recommendations and critical incident handling.
- Promoted twice during tenure (Associate T1 to T1 to T1 Senior) and awarded the ReliaQuest Excellence Award.

Security Analyst / Service Centre Analyst — Capgemini Aug 2015 - Apr 2018

Security Analyst Jul 2016 - Apr 2018

- SIEM investigation using Huntsman, and later IBM QRadar and Splunk, responding proactively to potential threats and delivering accurate analysis.
- Developed detection rules within Huntsman and QRadar.
- Engineering tasks including log backup, IDPS signature updates (TippingPoint), health checks and reporting.
- Managed customer relationships directly, by phone and in meetings.

Service Centre Analyst Aug 2015 - Jul 2016

- First-line service desk across multiple B2B client environments: troubleshooting, escalation and account management actions including unlocks, resets and credential management.

EDUCATION & ONGOING DEVELOPMENT

Master in Cybersecurity & Threat Intelligence — MIA Digital University (dual degree with UDIMA, Spain) In progress

Accredited online master's covering threat intelligence, offensive & defensive security, cloud security, secure development, and AI applied to cyber defence.

Certified Junior Detection Engineer (CJDE) — Security Blue Team In progress

Practical detection engineering: Sigma & YARA, Zeek, detection rule creation and tuning, threat-intelligence integration.

HNC Computing / NC Computing — North Highland College (UHI) 2012 – 2014

Deloitte Employability Award.

CERTIFICATIONS

Microsoft: SC-200 Security Operations Analyst Associate (2024)

Blue Team: Blue Team Level 1 (2022), CompTIA PenTest+ (2021), CompTIA CySA+ (2021), CompTIA Security+ (2019)

Splunk: Core Advanced Power User (2021), Core Certified Power User (2020), Core Certified User (2020)

EDR: Carbon Black Advanced Analyst (2019)

VOLUNTEERING & OUTREACH

- Junior Achievement Ireland - delivered cyber security and IT careers presentations in all-female schools in Ireland, representing ReliaQuest.
- North Highland College - volunteered to return and deliver a careers talk to computing students at my former college.
- Dublin Tech Summit - represented ReliaQuest at the recruitment stall, engaging students and professionals.

References and recommendation letters available upon request.