George Morganstern

george@morganstern.tech
linkedin.com/in/gmorganstern · https://morganstern.tech

Cyber Security Consultant with SOC roots, specialising in reducing and managing risk for enterprise clients. Proficient in incident response, leading use-case workshops and threat-modelling sessions, and running service reviews that make risk clear to technical and C-level audiences - while staying hands-on driving improvements across Sentinel and Datadog.

Experience

Feb 2026 - Present

Cyber Security Consultant, SecurityHQ

Use-Case Workshops & Threat Modelling: Lead client workshops and threat-modelling sessions against the MITRE ATT&CK framework - identifying business-specific risk, shaping SIEM coverage, and closing detection gaps.

Executive Reporting & QBRs: Build custom monthly security posture reports for the specific needs of clients - turning raw SOC data into risk-based roadmaps.

Incident Response & Estate Management: Support technical and non-technical clients through major incidents from triage to remediation.

Detection & Tuning: Write and refine analytic rules across Microsoft Sentinel and Datadog Cloud SIEM - tuning detections and building custom use cases for clients.

Apr 2025 - Feb 2026

Cyber Security Associate Consultant, SecurityHQ

Client Delivery: Primary point of contact for a portfolio of enterprise clients - owned day-to-day service delivery, rebuilt stakeholder confidence where needed, and helped clients define and reach their security goals.

SecOps Reviews: Directed weekly technical reviews, explaining trends in environmental risk week by week based on SIEM data and distilling high-volume telemetry - EPS trends, identity/auth patterns.

Technical Bridge: Served as lead liaison and technical POC between SOC engineering and client IT teams, landing high-priority deployments and remediation.

Jan 2024 - Apr 2025

SOC Analyst, Solace Global

End-to-End Incident Ownership: Owned and handled incidents from first alert through to containment and remediation for clients.

Operational Governance: Authored the SOP and playbook library used across the analyst team, standardising incident handling.

Technical Escalation & Mentorship: Primary escalation point for the L1 team - upskilled and mentored new engineers and peer-reviewed investigations.

Security Consulting & Hardening: Delivered Microsoft Secure Score improvement projects and Conditional Access policies.

Education

2020 - 2023

BSc (Hons) Computer Networking & Cyber Security, London Metropolitan University

First Class Honours

Technical Skills

- **SIEM Platforms:** Microsoft Sentinel, Datadog Cloud SIEM, QRadar, Darktrace
- **Detection Engineering:** KQL, analytic rule development & tuning, custom use-case design
- **Threat Modelling:** MITRE ATT&CK-based workshops, business-risk identification, SIEM coverage & detection-gap analysis
- **Incident Response:** end-to-end incident ownership - triage, containment, remediation
- **Microsoft Security:** Defender XDR, Entra ID, Intune, Secure Score, Compliance Manager
- **Network & Endpoint:** FortiGate, FortiEDR, FortiAnalyzer, Sophos, SentinelOne
- **GRC & Posture:** ISO 27001 remediation roadmaps, executive risk reporting