

Saer Ndiaye

Senior Security Analyst · Security Operations, Incident Response & Automation · CEH · CySA+

New York / New Jersey area · hi.sajer@outlook.com · linkedin.com/in/saern · saerndiaye.com

SUMMARY

Cybersecurity professional with 7+ years in a critical-infrastructure security operations center: incident response, threat hunting, threat intelligence and security automation. Hands-on with Microsoft Sentinel, Defender XDR, Defender for Endpoint and Office 365, Purview, Entra ID and Splunk. Owns incidents from detection to closure and communicates clearly with users and stakeholders. Built a Splunk investigation dashboard that saves analysts 4+ hours a day, and started an AI-assisted investigation tool now sponsored by management.

EXPERIENCE

Senior Security Analyst · Large energy utility (critical infrastructure), New York, NY Feb 2019 – Present

- Worked independently during the early security operations center buildout, writing investigation procedures, documentation and onboarding materials as the team grew from one shift to a full multi-shift operation.
- Own the full lifecycle of phishing and social-engineering incidents: identify indicators, block IOCs, coordinate password resets, notify affected users and escalate complex cases to digital forensics.
- Investigate phishing, malware, endpoint and email incidents with Microsoft Sentinel, Defender XDR, Defender for Endpoint, Defender for Office 365, Splunk and Phantom SOAR.
- Hunt proactively with KQL in Sentinel and Defender Advanced Hunting to scope incidents, sweep for indicators and assess impact.
- Trace phishing campaigns in Defender Explorer: message delivery, affected users, containment and IOC analysis.
- Investigate DLP incidents involving PII/PHI in Microsoft Purview, including quarantine and release decisions.
- Review Entra ID sign-in and authentication activity to support identity-related investigations.
- Assess exposure to new vulnerabilities: validate affected devices in Defender and hand prioritized findings to the Vulnerability Management team.
- Coordinate vendor-compromise investigations and validate vendor remediation before trusted relationships are restored.
- Hosted daily cross-utility threat intelligence calls with peer organizations and contributed intelligence to E-ISAC.
- Built a Splunk investigation dashboard that reduced analyst workload by 4+ hours per day.
- Self-initiated an AI-assisted investigation tool on Gemini Enterprise (in development, management-sponsored): multi-agent support for alert analysis, query generation and investigation consistency, with analyst approval.
- Mentor analysts; led onboarding and day-to-day work for a team of 3.

Cyber Security Contractor · KPMG, Montvale, NJ May 2018 – Aug 2018

- Reviewed application security findings in Fortify and built Excel dashboards tracking vulnerabilities across projects.

Network Engineer · Electric.ai, New York, NY Mar 2017 – Feb 2018

- Sole on-site engineer for client builds: scoped, designed and deployed secure office networks; found security weaknesses such as default device credentials.

IT support roles · Telovox · Fordham University · SUNY Polytechnic Institute 2015 – 2017

PROJECTS

Smart Phishing Email Analyzer (personal project, 2025): Outlook → urlscan.io → AI risk score → Jira and Slack routing; cut manual triage from hours to minutes. Presented to management; led to the AI-assisted investigation tool.

Jolof AI (personal project): production Wolof-language voice and chat assistant with monitoring and automatic model/key failover.

EDUCATION, CERTIFICATIONS & TRAINING

B.A. Network and Computer Security, SUNY Polytechnic Institute, May 2016

Certifications: CEH · CompTIA CySA+ · CompTIA Linux+ · CompTIA A+ · PAPA, Practical AI Pentest Associate (TCM Security, 2026) · IBM Generative AI for Cybersecurity Professionals

Training: Mandiant Windows Enterprise Incident Response (WEIR), Google Cloud Security (Oct 2026) · TCM AI Hacking 101

SKILLS

Security operations: Microsoft Sentinel, Defender XDR, Defender for Endpoint, Defender for Office 365, Advanced Hunting (KQL), Defender Explorer, Purview DLP, Entra ID, Splunk, Phantom SOAR, EDR, IDS/IPS, Wireshark

Investigation tools: Exabeam, Gurukul, Attack Analyzer, Imperva, FireEye/Trellix, Tanium

Automation & AI: n8n, Make.com, REST APIs, Gemini Enterprise, LLM integration (AI-assisted development, validated and secured)

Frameworks & other: MITRE ATT&CK, NIST CSF · Azure (investigation-level) · LAN/WAN, TCP/IP, firewalls, VPN · Jira, ServiceNow (user-level)