Ian Sugg
ian.m.sugg@gmail.com | https://ian-m-sugg.com

Overview:

Security Engineer with a special interest in security automation and Elastic stack. Experience in almost any security tool on the market, from my time in many diverse environments at MSSP SOCs. SOC automation and detection experience in Elasticsearch and Zendesk. Dedicated work ethic, positive attitude, and concise communication.

Education:

Arizona State University | B.S. in Computer Science - Cybersecurity concentration | 2019-2023

Certifications:

CompTIA A+, Security+, CySA+, (ISC)2 Certified in Cybersecurity

Experience:

Lumifi Cyber

Product Development Engineer | January 2025 - Present

-Re-engineered and optimized threat detections for in-house tool, expanding attack surface coverage by 43% while reducing false-positive ticket generation by over 200x. Accomplished through experimentation in a lab developed by myself.
-Refined multiple detections, enabling high-confidence true positives that would have otherwise been missed by the SOC.
-Created custom Elastic ingest pipelines utilizing painless scripting, grok expressions, and more to create custom Elastic integrations. Followed up with SOC detections and administrative dashboards to create comprehensive, client-facing, content packs, earning direct client praise and adoption.

Threat Detection Engineer | October 2024 - January 2025

-Optimized queries using short circuit evaluation, DeMorgan's laws, and boolean simplification. This, combined with optimizations from the development team, resulted in a decrease in load of >96% for the Elastic stack.
-Created and translated multiple rules in languages such as Microsoft KQL, Cortex XQL, Netwitness's query language, and Lucene query syntax.
-Participated in daily threat research to ensure proper coverage of emerging CVEs, and APTs. Engaged customers from different sectors to ensure at-risk organizations were taking proper precautions.

L1 SOC Analyst | January 2024 - October 2024

-Monitored incoming alerts spanning many client ecosystems, while communicating clearly and succinctly. Accurately identified actionable events by staying up to date on emerging threats, and cybersecurity news.
-Identified erroneous and low fidelity alert queries, passing them on to appropriate channels for higher quality alerting opportunities.

Novawatch

Tier 2 SOC Analyst/Support Engineer | August 2023 - December 2023

-Managed and tuned Elastic Security SIEM comprising 20% of total client base, reducing false positives by 80%+ by writing custom detection rules and exceptions.
-Fully automated daily reporting of Elastic security and AlienVault event reporting through python script using Elasticsearch, zendesk, and pandas libraries and APIs, saving 4 hours a day.

Tier 1 SOC Analyst | October 2022 - August 2023

-Quickly adapted to handle workload of multiple SOC analysts during emergency division reassignment.
-Communicated environments, and SOC visibility to clients via status calls, as well as successfully identifying true and false positives in a variety of tools.
-Utilized JavaScript and Amazon S3 buckets creating a custom tool for dynamically parsing JSON logs from multiple security tools. Leveraging this tool, and rising to highest cases closed and escalations sent to clients in first 6 months. (Lowest MTTD and MTTR) (https://tool-to-zendesk-parser.s3.us-west-1.amazonaws.com/index.html)

Projects:

https://ian-m-sugg.com/ - **Resume Website**

This is a collection of my work to date. Including nearly all my ventures in computer science from ASU coursework to security experiments. Developed in Wordpress using custom CSS and JavaScript, hosted in AWS.

https://ian-m-sugg.com/portfolio - **Portfolio of Security Experiments**

Built on a Dell PowerEdge R720, the lab has gone through a few configurations, but currently: Proxmox hypervisor, 2 Ubuntu servers running personal Elastic stack, 1 DC, 1 Kali box, and 1 Win10 machine. Development, deployment and detection and containment of ransomware, infostealers, and other malware. General Elastic knowledge.