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

Overview:

Security Analyst with a special interest in security automation and engineering. Experience in multiple EDRs, NIDS, SIEMs and SOARs. MSSP SOC Automation experience in Elasticsearch and Zendesk.

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

L1 SOC Analyst | January 2024 - present

-Communicate and monitor many diverse environments for multiple clients through EDRs such as Carbon Black, Crowdstrike, Microsoft Defender, Sentinel One, NIDS such as Extrahop and behavioral tools such as Exabeam.

Novawatch

Tier 2 SOC Analyst | 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.

-Utilized multiple EDRs, NIDS such as Darktrace, and SIEMs and SOARs such as Swimlane, Alienvault and Microsoft Sentinel.

-Joined client calls to explain SOC visibility and analyst view of customer environments.

-Rose to highest cases closed and escalations sent to clients in my first 6 months. (MTTD and MTTR)

-Leveraged javascript and Amazon S3 buckets creating custom tools for parsing JSON logs from Rapid 7 Insight IDR, Elastic Security, and Carbon Black for ticket writing.

Arizona State University

Information Assurance Undergraduate Teaching Assistant | January 2022 - May 2022

-Taught binary reversal, linux, python for hacking and buffer overflows to over 400 computer science students doubling average homework grades.
(https://www.youtube.com/playlist?list=PLPGBWVcBRjY-fS2KC4D3iCg6_XYtbEdd9)

Projects:

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

This is a collection of my work to date. It includes nearly all of the ventures I've taken in computer science from ASU coursework to security experiments.

https://ian-m-sugg.com/portfolio - **Portfolio of security experiments**

Setting up my lab in my poweredge r720, deploying ransomware, writing detection rules and more are documented here. Includes examples of SIEM and programming experience.