LOGAN ELLIOTT, CASP+

Senior Cybersecurity Analyst

Threat Hunting | Incident Response | DFIR | Threat Intelligence

Active Secret Clearance | Panama City Beach, FL | 850.238.9610 | LoganElliott612@gmail.com | LinkedIn

PROFESSIONAL SUMMARY

Cybersecurity professional with 5+ years of experience supporting Department of Defense operations across incident response, threat hunting, digital forensics, vulnerability management, detection engineering, and threat intelligence. Led 73% of enterprise cybersecurity incidents and 78% of threat hunting operations across 120+ Air Force and Space Force locations. Built 94% of detection queries used by the analyst team, improving detection fidelity and response efficiency. Strong background in SIEM analysis, malware triage, ICS security, and intelligence-driven defense.

CORE SKILLS

Threat Hunting • Incident Response • Detection Engineering • Threat Intelligence • Digital Forensics • Malware Analysis • SIEM Analysis • ICS Security • Vulnerability Management • Security Consulting

TOOLS & TECHNOLOGIES

Security: Microsoft Defender for Endpoint (MDE), ACAS/Tenable, HBSS, Elastic Security, IDS/IPS, Cisco ASDM, Trellix
Detection/Query: KQL, ES|QL, SQL, MITRE ATT&CK, IOC Analysis, CISA KEV, CVE Analysis
Infrastructure: Windows Server, RHEL, Active Directory, SCCM, WSUS, eMASS
Forensics: Eric Zimmerman Tools, Sandbox Analysis, Artifact Collection, Timeline Reconstruction

PROFESSIONAL EXPERIENCE

Senior Cybersecurity Analyst | General Dynamics | Mar 2024 – Present

- Secure Industrial Control System (ICS) environments supporting 120+ Air Force and Space Force locations.
- Lead 73% of enterprise cybersecurity incidents from triage through containment, eradication, recovery, and root cause analysis.
- Lead 78% of enterprise threat hunting operations across multiple security platforms.
- Develop and maintain 94% of threat detection queries, improving detection fidelity and analyst efficiency.
- Created a daily threat intelligence briefing using CISA KEV, BleepingComputer, SANS, and DFIR research to prioritize emerging threats and exploitable CVEs.
- Perform digital forensics, log correlation, artifact collection, and timeline reconstruction; map adversary TTPs to MITRE ATT&CK.
- Conduct malware sandbox analysis to identify indicators of compromise and malicious behavior.
- Developed, implemented, and tuned Trellix endpoint firewall, threat prevention, and Data Loss Prevention (DLP) policies.
- Generated enterprise vulnerability reports highlighting risk severity and remediation priorities.
- Troubleshot and maintained enterprise logging infrastructure to ensure reliable log collection.

- Led the evaluation and introduction of incident response tooling to improve investigation capabilities.
- Authored and maintained incident response playbooks.
- Prepare executive reports, mentor analysts, and refine IR policy with security leadership.

System Administrator | General Dynamics | Jul 2023 – Mar 2024

- Led AFNORTH/1AF technology refresh initiative and delivered executive project status reporting.
- Troubleshot endpoint hardware and software issues to restore functionality and minimize user downtime.
- Installed and deployed endpoint equipment with minimal disruption to end users during technology refresh initiatives.
- Managed technology refresh inventory, tracking hardware assets, deployments, and lifecycle replacements.

System Administrator | Forge Forward | Sep 2022 – Aug 2023

- Supported 140+ Navy systems and resolved 80+ daily support requests with 85% first-contact resolution.
- Utilized ACAS to identify, assess, and remediate vulnerabilities across enterprise systems.
- Managed Active Directory administration, including user accounts, group policies, and access management.
- Patched and maintained enterprise infrastructure, including network devices, Windows servers, RHEL systems, and end-user laptops.
- Troubleshot and maintained RHEL Ansible playbooks and PowerShell scripts to support system administration and automation.

IT Specialist | Florida State University | Oct 2021 – Oct 2022

- Provided enterprise endpoint support and Active Directory administration.
- Installed, maintained, and troubleshot physical network rack infrastructure, including cable management, equipment installation, and hardware replacements to support campus IT operations.

CERTIFICATIONS

CASP+ • PenTest+ • CySA+ • Security+

EDUCATION

Western Governors University — B.S. Cybersecurity and Information Assurance