JOHN ALTHAUSEN

SECURITY OPERATIONS ANALYST · DETECTION ENGINEERING · NETWORK SECURITY · IDENTITY & PKI

Loudon, TN · (865) 316-8282 · jack@althausen.me · linkedin.com/in/althausenjohn

HSPD-12 PIV Credential · Active DOE Site Access

SUMMARY

Security operations analyst with three years supporting a federal environment, spanning detection engineering, incident response, network security, and PKI. Sole author of a custom detection library across Elastic, Splunk, and CrowdStrike Falcon covering web application attacks, identity abuse, endpoint intrusion, and security-control failure. 24/7 on-call for external-facing production systems, consistently detecting and remediating attacks before customer or management notification. Additional depth in Juniper network security engineering, 802.1X certificate-based access control, post-quantum cryptographic migration, and Entrust PKI operations.

EXPERIENCE

Edgewater Federal Solutions, Inc. — DOE Office of Scientific and Technical Information (OSTI)

Oak Ridge, TN · February 2023 – Present (3 yrs 7 mos)

Promoted through four roles in eighteen months, from IT support intern to sole security operations analyst for the environment.

Security Operations Center Analyst | June 2024 – Present

DETECTION ENGINEERING

- Author and maintain the organization's entire custom detection library across Elastic, Splunk, and CrowdStrike Falcon, mapped to MITRE ATT&CK techniques.
- Built web application attack detection covering nine signature families: SQL injection, cross-site scripting, local file inclusion and path traversal, remote code execution including Log4j JNDI strings, server-side template injection, deserialization exploits, vulnerability scanner user agents, and hidden-endpoint probing.
- Created behavioral abuse detection using requests per second, average payload size, and error rate to identify volumetric scrapers, slow-hang sessions, high-error scanners, and resource exhaustion conditions.
- Engineered a tuned allowlist of approved crawler IP ranges and individual hosts, surfaced in-dashboard as approved traffic, to eliminate false positives against legitimate customers before deployment.
- Built Active Directory identity detection covering account creation and deletion, security group modification, break-glass account usage, account disablement, password modification, AppLocker events, local account creation, repeated authentication failure, and firewall-blocked internal traffic.
- Authored CrowdStrike custom IOAs for anomalous LOLBin parent processes, temp-directory execution with user mismatch, privileged account lateral movement, Linux shell history tampering, and removable media or mobile device connection to government-furnished equipment.
- Built control-assurance detection for the security stack's own failure modes: duplicate agent IDs indicating VM clone or imaging faults, Falcon sensor reduced-functionality mode and version drift, log ingestion failure and volume-drop conditions, and credentialed scanner authentication failure following password rotation.
- Designed multi-dimensional analyst dashboards with filtering by time range, application domain, IP or subnet, user agent, and download volume, including an analyst-level toggle controlling client-to-subnet aggregation.

INCIDENT RESPONSE & OPERATIONS

- 24/7 on-call responder for all external-facing production web applications, with no rotation or secondary escalation.
- Detect, analyze, contain, and remediate application-layer attacks and availability incidents — routinely restoring service before customer or management notification, maintaining an internal-detection rather than externally-reported posture.

NETWORK SECURITY ENGINEERING

- Upgraded the Juniper EX2300 access switch fleet from JunOS 18 to JunOS 24, closing multiple LTS generations of accumulated vulnerability exposure on live production infrastructure.
- Supported a core network refresh delivering an approximately 40x throughput increase and establishing a post-quantum resistant cryptographic foundation.
- Implemented switch-port network access control using RSA and smartcard certificate-based authentication.
- Configure port security, VLAN tagging, and network segmentation; deployed zero trust frameworks and security baselines to IoT device populations.

IDENTITY & PKI

- Serve as Entrust encryption administrator: backend S/MIME configuration, user certificate issuance, and certificate publication enabling encrypted email across Microsoft Outlook.
- Administer Entra ID user provisioning and role-based access control for SIEM platform access; maintain identity alerting across hybrid on-premises Active Directory and cloud identity.

VULNERABILITY MANAGEMENT

- Operate Tenable Nessus for scheduled credentialed scanning, with reporting dashboards surfacing remediation priorities to system owners.

Help Desk Support | July 2023 – June 2024

- Administered the Alloy ticketing system, resolving user-reported issues with documented guidance for self-resolution.
- Created and deployed standardized Windows images and maintained patch currency across the desktop fleet.
- Administered Adobe enterprise software deployment, licensing, and troubleshooting.
- Mentored incoming interns and staff on imaging procedures, security protocols, and networking fundamentals.

Information Science Specialist — Archivist Support / Help Desk | May 2023 – June 2023

- Supported archival operations and help desk functions, including user issue resolution.

IT Support Specialist Intern | February 2023 – April 2023

- Delivered hands-on IT support including hardware troubleshooting and system imaging.

EDUCATION

Roane State Community College — Cyber Defense and Networking Administration
2021 – Present

Mt. San Antonio College — Network and System Administration
2018 – 2020

Relevant coursework: Cisco CCNA, Windows Server Network Security, Network Vulnerability Analysis, Digital Forensics, Penetration Testing, Network Defense, Linux LPIC-I, Telecommunications Networks, Programming I & II.

CERTIFICATIONS

- CompTIA Security+
- Palo Alto Networks Cybersecurity Fundamentals: Security Solutions
- TestOut Security Pro · TestOut Network Pro · TestOut PC Pro
- National Cyber League — Individual Game, Fall 2020

TECHNICAL SKILLS

Detection & SIEM — Elastic Security, Splunk (SPL), CrowdStrike Falcon custom IOAs, Cortex XDR, MITRE ATT&CK mapping, behavioral and signature-based detection authoring, dashboard engineering

Endpoint & Threat — EDR administration, LOLBin and living-off-the-land detection, lateral movement detection, insider threat and removable media monitoring, sensor health and coverage assurance

Network — Juniper JunOS (EX2300), Ubiquiti, VLAN segmentation, port security, 802.1X certificate-based NAC, zero trust architecture, IoT security baselines, post-quantum cryptographic migration

Identity & PKI — Entrust certificate administration, S/MIME, Active Directory, Entra ID provisioning and RBAC, smartcard authentication

Vulnerability & Analysis — Tenable Nessus, Wireshark, tcpdump, NetworkMiner, Nmap, packet analysis, network forensics

Development & Automation — Swift, application development, security tooling