AYHAN AYTAC

CYBERSECURITY ANALYST

IRVINE,CA | aytaclv@gmail.com | 7029370019

SUMMARY

Accomplished Security Engineer with a proven track record at Solvent Cybersecurity, specializing in cloud security, incident response, and mentoring junior analysts. Expert in vulnerability assessment and leveraging SIEM tools like MS Sentinel,Splunk. Demonstrated leadership in enhancing cybersecurity postures, achieving significant risk reduction. Skilled in fostering team growth and resilience in fast-paced environments.

PROFESSIONAL EXPERIENCE

Security Analyst,SAIC **Apr 2022 - Present**

- Monitored and analyzed SIEM (Security Information and Event Management) alerts to detect potential threats, vulnerabilities, and policy violations.
- Triaged incoming security events and conducted in-depth investigations to determine severity and incident classification.
- Logged and tracked security incidents using IT ticketing systems, ensuring complete and accurate documentation for each case.
- Managed the full lifecycle of security incidents—from initial detection and analysis through containment, remediation, and closure.
- Collaborated with cross-functional IT teams to investigate and resolve security issues efficiently.
- Leveraged threat intelligence feeds and external sources to assess and contextualize security events.Generated routine and ad-hoc security reports, ensuring timely and accurate delivery to stakeholders.
- Escalated complex or high-impact incidents to Tier 2 Analysts or SOC Leads in accordance with escalation protocols.
- Adhered to and maintained SOC Service Level Agreements (SLAs) for timely security alert response and resolution

Security Analyst,Cognizant Technologies **July 2021 - Mar 2022**

- Developed and maintained custom Splunk searches, reports, and dashboards to facilitate proactive threat hunting and incident detection.
- Conducted regular tuning of Splunk alerts and queries to reduce false positives and enhance detection accuracy.
- Followed detailed operational processes and procedures to appropriately analyze, escalate, and assist in remediation of security incidents.
- Experience with EDR solutions including Carbon Black, SentinelOne, FireEye HX, CrowdStrike.
- Experience analyzing log and packet data in a SIEM Azure Sentinel.
- Documented and maintained detailed case logs and incident reports for phishing incidents.
- Conducted regular security assessments and audits using Prisma Cloud's scanning and threat detection capabilities, identifying and mitigating risks related to misconfigurations, vulnerabilities, and anomalous activities.
- Managed Data Loss Prevention (DLP) tools and enforced incident response processes to prevent data exfiltration.
- Developed and updated comprehensive Cybersecurity Incident Response Plans, with 2+ years of experience in modernizing IR strategies.

- Delivered advanced cybersecurity expertise and leadership, effectively resolving complex issues in Incident Response, Threat Intelligence, GRC, Privacy, Vulnerability Management, and Engineering Operations.
- Performed analysis of log files of Firewall, IPS, IDS, Server, and Proxy via the Splunk SIEM solution.
- Created and tracked incidents and requests with an integrated ServiceNow (SNOW) ticketing and automation system.
- Analyzed pcap files for malware analysis and identified details of infected hosts, writing IOCs for executive summary reports.
- Identified, tracked, and investigated high-priority threat campaigns and malicious actors with specific TTPs (Techniques, Tactics, and Procedures).
- Provided oversight and mentoring to junior analysts, guiding them on best practices in security operations and response.
- Familiar with enterprise security tools such as Proofpoint, Mimecast, Zscaler, Cisco ISE, IPS, and IDS.

Information Technology Instructor,Coral Academy of Science **Aug 2018 - Aug 2021**

- Planned, organized, controlled, and evaluated IT and electronic data operations.
- Facilitated and monitored a comprehensive, school-wide Technology Plan.
- Managed an online lab environment and installed and deployed online learning tools.
- Developed computer training materials.
- Developed and implemented needs assessments, evaluations, and long-term plans related to technology initiatives, equipment, and software.

SKILLS

Vulnerability assessment	Endpoint Security	Malware Analysis
Cloud Security	ProofPoint,Crowdstrike	Incident Response
Risk Analysis	SIEM Tools(Splunk,Sentinel)	Data loss prevention

EDUCATION

Masters Degree in Cyber Security | National University (San Diego, CA) **Sep 2021 - Feb 2023**

ADDITIONAL INFORMATION

- **Languages:** English, Turkish
- **Certifications:** Certified Ethical Hacker (CEH), CompTIA Cybersecurity Analyst (CySA+), CompTIA Security+, Azure Administrator Associate certification (AZ-104), AWS Certified Cloud Practitioner, SC-20
- **Activities:** OSINT Summit ,SANS Community Events,Austin summit cybersecurity