Augustine George

crissaugustine@gmail.com • linkedin.com/in/augustine-george-2b85aa65
India. • +91-9846787077 / +91-8137885978

PROFESSIONAL SUMMARY

8+ years of experience working as Cyber Security Engineer and Incidents Response Analyst. Has a master's degree in computer applications, certified CompTIA Security+, AZ-500, AZ-900, and possesses a thorough knowledge of monitoring, Use case creation, documentation, analysis, integration, and implementation.

Tools Specialization

SIEM Monitoring: Microsoft Sentinel, Splunk, DNIF, ArcSight
EDR and Network: Carbon Black, CrowdStrike, Microsoft Defender, Fidelis Endpoint, and Fidelis Network
Operating Systems: Windows, Linux, Android
Ticketing and Tracking Tools: ServiceNow, JIRA, Confluence, E-Helpline.
MS Office: Excel, Word, PowerPoint.
Framework: MITRE ATTACK Framework, Cyber kill chain, NIST.
Automation: DevOps, Terraform.

WORK EXPERIENCE

Lead I - Cloud Infrastructure Services

Oct 2021 - Present

CyberProof • Kochi, India

- Usecase and Investigation guidelines, Incident response steps writing and review.
- Creating playbooks and investigation guidelines for easy triage of alerts monitored, supporting L1.
- Deployment of Microsoft Services (Sentinel, ADX, EventHub, etc.) using DevOps pipeline with Terraform code.
- Creating flow for automation of incident response using LogicApps for Azure Sentinel.
- Creating parsers and performing tuning of SIEM filters and event correlations to ensure continuous monitoring improvements.
- Identified the false positives and fine-tuned the rules for legitimate activities.
- Created and fine-tuned rules according to the device integration changes or when a false-positive is observed.
- Provide support, guidance, and delegation of work tasks to SOC operators and analysts.
- Oversee monitoring activities and conduct security investigations as required.
- Coordinating incident response to ensure timely incident resolution.
- Weekly meetings with clients to discuss new requirements as well as suggest new performance upgrades.
- Development, testing, and validation of the effectiveness of security analytics rules and queries aligned to risk analysis and common threat modeling techniques.

- End-to-end delivery of project and content development as a team lead.
- Assisting Solution Architect with integration and implementation, platform management, and onboarding.

Senior Cyber Security Consultant Feb 2021 - Oct 2021
Ernst & Young Global Limited GDS • Trivandrum, India

- Establish and implement policies and procedures for information systems as per the customer requirements.
- Created and migrated Daily, Weekly, and Monthly reports and Dashboards which were shared with stakeholders.
- Created separated dashboards, and active channels, drilled down queries, and monitored critical activities in addition to **real-time monitoring** and reporting the same if found suspicious.
- Meeting with clients to discuss system requirements and specifications.
- Maintained regular connections with customers through review calls.
- Following up with customers regularly and whitelisting the genuine traffic/user details from rules and reports, hence focusing on the real threats.
- Team lead, leading a team of 8+ members, training, and mentoring SOC analysts.
- Assigning, coordinating, and reviewing projects with team members.
- Identified the false positives and fine-tuned the rules for legitimate activities.
- Created and fine-tuned rules according to the device integration changes or when a false positive is observed.
- Phishing mail analysis and IOC hunts.

Systems Engineer Oct 2018 - Jan 2021
Tata Consultancy Services • Kochi, India

- Involved in Implementation, Integration and, Use-case design for Security monitoring using SIEM tools.
- Created, Migrated Daily, Weekly and Monthly reports and Dashboards which were shared to stake holders.
- Created separated dashboards, drill down queries and monitor critical activities in addition to real time monitoring and report the same if found suspicious.
- Leading team of 12+ members, training, and mentoring SOC analysts.
- Following up with customers regularly and whitelisting the genuine traffic/user details from rules and reports, hence focusing on the real threats.
- Installing and configuring SIEM agent on customer critical servers/devices and monitoring the events.
- Adaptor, Datastore troubleshooting – Resolved situations like adaptor down, parsing issues, exceeding EPS limit, event mapping issues, caching issue.
- Performed health checkup of SIEM tool and components.
- Troubleshooting of integrated log sources.

Project Engineer Feb 2016 - Oct 2018
Wipro Technologies • Kochi, India

- Involved in monitoring to protect infrastructure and systems, as well as performed security

incident response and remediation when an issue is found.
- Involved in Security monitoring using ArcSight, Splunk.
- Worked on security-related user requests and served as point of escalation for the user support team.
- Performing Log Analysis from different network devices.
- Part of a flexible rotating on-call roster to support our global operation.
- Communicating with concerned teams for blocking hash files and IPs.

EDUCATION

Master of Computer Applications Jun 2012 - Nov 2015
Amal Jyothi College of Engineering • India

Bachelor of Computer Science Jun 2009 - Apr 2012
College of Applied Science • India

SKILLS

SIEM Engineer

- Installing and configuring SIEM agents on customer-critical servers/devices and monitoring the events.
- Adaptor, Datastore troubleshooting – Resolved situations like adaptor down, parsing issues, exceeding EPS limit, event mapping issues, and caching issues.
- Performed health checkup of SIEM tool and components.
- Worked on mail notification and alert creation.
- Troubleshooting of integrated log sources.

SIEM Analyst

- Demonstrated strong knowledge in the following areas: security information and event management (SIEM) platforms, EDR, and penetration testing tools.
- Wide range of technical experience across Security, Incident, and Event Management platforms (particularly Azure Sentinel, Splunk, ArcSight, and DNIF).
- Taking ownership of operational issues, as well as project-based work as a lead engineer and delivering from conception through to completion.
- Experience with tools used in security event analysis, incident response, EDR, and other areas of security operations.
- Knowledge of incident response methodologies e.g., NIST.
- Understanding of networking and TCP/IP.
- Use Case and content development including threat modeling to open standards, using the MITRE ATT&CK framework, Cyber Kill Chain.
- Strong troubleshooting and analytical skills.
- Strong investigative skills and mindset.
- Phishing mail analysis and IOC hunts.
- Strong leadership and mentorship skills, Team lead, leading a team of 8+ members, training and mentoring SOC Analysts.
- Ability to work autonomously with attention to detail.

- Assigning, coordinating, and reviewing projects with team members.
- Ability to communicate effectively and write concisely and clearly.
- Identified the false positives and fine-tuned the rules for legitimate activities.
- Created and fine-tuned rules according to the device integration changes or when a false positive is observed.

PROFESSIONAL CREDENTIALS

- CompTIA Security+ Certification
- Microsoft Azure Fundamentals AZ-900
- Microsoft Azure Security Engineer AZ-500
- Splunk User 7. x
- **IELTS General Score**: 7
- **PTE Academics** Language Test Level – **Proficient User (72/90).**