JEREMIAH PHILLIPS

Phone: (229) 343 - 5257 | Email: jeremiah_phillips2000@yahoo.com

PROFESSIONAL SUMMARY:

Highly motivated professional with a strong foundation in cybersecurity, specializing in threat detection, incident response, and vulnerability management. Currently applying customer support expertise in a software development environment to ensure seamless software usage for customers. Committed to advancing my career by integrating cybersecurity principles into customer support and contributing to improved user experiences.

TECHNICAL SKILLS:

Sentinel One, CrowdStrike Falcon, Forensic Analysis, OSINT Tools, Incident Response, Security Frameworks, Armis, Kali Linux, NIST CSF, Proofpoint, IBM QRadar, Risk Mitigation, Wireshark, Nmap, Tenable Nessus, Splunk Enterprise Security, Jira, Darktrace Intrusion/Detection, Sophos Antivirus, Carbon Black Cloud Antivirus, Active Directory, Network Monitoring, Checkpoint Firewall, Salesforce, Logrocket, Sentry, Confluence, Amazon Connect.

PROFESSIONAL EXPERIENCES:

Software Support Analyst I

Mark43 – Remote | Aug 2024 – Present

- Maintain a 100% CSAT score and 100% First Response Rate, consistently exceeding service expectations.
- Resolve an average of 64+ support cases monthly, with 81% of all cases fully resolved without engineering involvement, demonstrating strong technical autonomy and product knowledge.
- Achieve an average support-only closure rate of 70.85%, reflecting consistent independent resolution of customer issues.
- Reduced customer contact-to-resolution workflow time by 50% by implementing AI tools to streamline initial triage and Jira ticket creation.
- Collaborate with engineering and product teams during P0/P1 incidents, ensuring rapid resolution and clear documentation.
- Participate in testing new product features and contribute to internal knowledge base improvements using Confluence.
- Utilize tools such as Salesforce, Jira, LogRocket, Sentry, and Amazon Connect to investigate, replicate, and resolve software issues across staging and demo environments.

Cyber Security Analyst I

Phoebe Putney Health System – Albany, Ga | Feb 2024 – Aug 2024

- Manage the KnowBe4 platform and plan the organization's monthly phishing email tests and create training materials for organization wide security training.
- Give users multi-factor authentication access in Active Directory after verifying user credentials to ensure correct user information and data confidentiality in Microsoft Entra Identity.
- Monitor the network in Darktrace for anomalous behavior, investigate over 50 alerts every day, and triage each alert after thorough investigation.
- Collaborate with network engineers to add known bad IP addresses and domains to the Checkpoint firewall to restrict access to the network.
- Investigate alerts in Carbon Black Cloud platform for malicious hashes, files, network connections and triage each alert by declaring it a true or false positive after thoroughly investigating each artifact.
- Run reports on over 4,000 users for email phishing test failures, phish-prone percentages, user risk scores, training activity, and overall phishing failures for management to create a security training initiative for the most at-risk individuals.
- Investigate emails in Proofpoint TAP/TRAP that are reported as phishing to determine the validity of the email and block any malicious email domains or IP addresses.
- Utilize open-source tools such as VirusTotal, AbuseIPDB, and WHOIS to assist in investigating IP addresses, hashes, files, and domains.
- Perform troubleshooting such as password resets for users that need multi-factor authentication access and enabling the Phish Alert button in the Outlook application for phishing reporting.

SOC Analyst

CyberNow Labs – Remote | Aug 2023 – March 2024

- Configure and manage EDR/XDR tools to monitor for specific threats and vulnerabilities, determine the severity and scope of security alerts, collect forensic evidence from compromised systems, perform root cause analysis to identify the source of security incidents, and develop and implement mitigation strategies to prevent future attacks.
- Utilize SIEM solutions to identify suspicious activity in log data, such as failed login attempts, unusual network traffic, and unauthorized changes to system files. Correlate log data from multiple sources to build a complete picture of a security incident and continue to identify patterns in log data that may indicate a new or emerging threat. Provide recommendations to technical teams on how to improve security and reduce risk.
- Scan files for known malware and vulnerabilities and upload files in a sandbox to observe their behavior. Check domains and email addresses against blacklists and other threat intelligence feeds using Open-Source technology.
- Operate network packet capture tools to capture network traffic and analyze packet capture files to identify malicious activity. Inspect infected host details to identify the source of the infection and gather evidence to create Indicators of Compromise (IOCs) in executive

reports to help other security professionals identify and mitigate similar threats.
- Ensure compliance with NIST Risk Framework by identifying and assessing organizational risks and developing and implementing risk mitigation strategies.

Police Officer

Marine Corps Logistics Base – Albany, GA | Oct 2018 – Jan 2024

- Demonstrates expertise in law enforcement, effectively executing responsibilities including fixed post security, commercial vehicle inspections, and emergency response, resulting in consistently accomplished outcomes.
- Exhibits advanced proficiency in integrating police equipment and automated crime information systems, exemplifying the fusion of cybersecurity principles with law enforcement operations to ensure data protection, access control, and operational resilience.
- Proactively applies fundamental cybersecurity principles, including access control, threat detection, and social engineering defense, to identify and mitigate a range of security risks such as unauthorized access, social engineering attacks, impersonation threats, and identity breaches.

EDUCATION:

Bachelor’s Degree, Cybersecurity & Information Assurance – Western Governors University – Oct 2025

CERTIFICATIONS:

ISC2 SSCP; CompTIA CySA+, Security+, Network+, Project+ and A+; ITIL v4 Foundations.