Contact

www.linkedin.com/in/deekshitha-pullaiah-0136b2296 (LinkedIn)

Top Skills

Qualys
Tenable Nessus
Malware Analysis

Certifications

Phishing Analyser
Computer Hacking Forensic Investigator (CHFI)
Cisco Certified Network Associate Routing and Switching (CCNA)
Phishing Expert
Foundations of Operationalizing MITRE ATT&CK

Deekshitha Pullaiah

Sr. SIEM Administrator / Network Engineer - ArcSight, SOAR ,Splunk, Securonix,Vulnerability Management,CyberArk IAM, Phishing Expert,Check Point,Fortigate,Palo Alto,Cisco ASA
Greater Cleveland

Summary

Hello! I have 9+ years of experience in network security, SIEM Engineer with expertise in ArcSight solutions and incident response management. In addition to this, I have a strong background in managing firewalls, including Cisco, Palo Alto, and FortiGate, as well as Checkpoint, SSL VPN, and F5 Big IP. This diverse experience further enhances my ability to contribute effectively to organizations' security strategies.

Expertise:

- ArcSight Proficiency: Crafting tailored ArcSight SIEM solutions and optimizing configurations for unique security requirements.
- Incident Response: Expertly managing incident procedures and leveraging SIEM tools for rapid identification and resolution.
- Firewalls: Proficient in managing Cisco, Palo Alto, and FortiGate, in addition to Checkpoint, SSL VPN, and F5 Big IP. Expertise in firewall management, network design, and problem-solving, ensuring robust data protection and infrastructure resilience.
- Device Integration: Seamlessly integrating diverse devices into SIEM environments, enhancing overall threat awareness.
- Logger & ESM Insight: Harnessing the power of ArcSight Logger and ESM for real-time insights into security events.
- Parser & Regex Skills: Skillfully creating parsers and utilizing regex to normalize log data, enabling precise threat detection.
- Vulnerability Assessment (VA): Proficiently conducting comprehensive assessments to identify and mitigate system weaknesses.
- Practical Penetration Testing (PT): Gaining hands-on experience in evaluating and fortifying security measures.
- Forensic Analysis : Having a foundational expertise of forensic analysis techniques.

Additional Skills:

- Windows Server Management: Proficiently administering Active Directory, ensuring secure user authentication.
- ISO 27001 Awareness: Possessing foundational knowledge of ISO 27001 standards, contributing to robust information security.
- CrowdStrike & McAfee Familiarity: Grasping the essentials for enhancing malware defense capabilities.
- PAM Basics: Understanding Privileged Access Management principles to bolster control over critical systems.

Dedicated to staying current with evolving trends, I am committed to crafting resilient security solutions and embracing new technologies. Feel free to connect!

Experience

PwC
Security Engineer
January 2021 - Present (2 years 10 months)
Dallas-Fort Worth Metroplex

SEI Investments Distribution Co.
SIEM Administrator
December 2018 - November 2021 (3 years)
Oaks, Pennsylvania, United States

Truist Securities
Security Operations Center Analyst
August 2016 - October 2018 (2 years 3 months)
Charlotte, North Carolina, United States

Flex
Systems Engineer
April 2014 - July 2016 (2 years 4 months)
Austin, Texas, United States

Education

Campbellsville University

Master's degree, Cyber/Computer Forensics and Counterterrorism · (August 2013 - May 2015)

SCSVMV University

Bachelor of Engineering - BE · (June 2010 - May 2013)