P | V

PRAKHAR VARMA

INFORMATION SECURITY LEAD

Pune, India | +91-7021811469 | prakharjbp09@gmail.com

ABOUT ME

With more than a decade of experience in Information Security, I am eager to align my expertise with a forward-thinking organization that values professional growth and global contribution. With a strong commitment to enhancing my skills and knowledge, I aim to make an impactful contribution to the field while staying abreast of industry advancements.

EDUCATION

B.E. (ELECTRONICS & TELECOM)

Vindhya Institute of Technology and Science / Jabalpur / 2013

WORK EXPERIENCE

Amdocs

Oct 2022 - Present
Pune

INFORMATION SECURITY LEAD

- Spearheaded the planning and strategization of project timelines to ensure timely delivery of information security initiatives.
- Engaged stakeholders to define the scope, select optimal tools, and harness innovative technology.
- Analyzed and understood the architecture design to implement robust solutions that enhance the overall security posture.
- Developed comprehensive policies, procedures, and guidelines that align with industry best practices.
- Established metrics, KPIs, and dashboards to drive risk governance and identify gaps effectively.
- Crafted and implemented High-Level Designs (HLD) and Low-Level Designs (LLD) for proactive monitoring use cases.
- Collaborated with cross-functional teams to ensure seamless integration and execution of security initiatives.
- Integrated and optimized SOC monitoring platforms including SIEM, ELK, and SOAR for enhanced security visibility.
- Delivered impactful reports to management and clients, offering a holistic view of activities, threat landscapes, accomplishments, and strategic plans.
- Partnered with multiple vendors for efficient issue resolution, continuous feature enhancements, and streamlined license management.

Amdocs

Apr 2020 - Present
Pune

INFORMATION SECURITY ANALYST - SPECIALIST

SKILLS

Information Security, SIEM Admin (Arcsight), Splunk, ELK, McAfee ESM, Q-radar.

FIM (Tripwire), XDR (Cortex), EDR (CrowdStrike), Imperva DAM, WAF (Imperva & F5 ASM) IPS (Cisco Sourcefire & Palo Alto), Vulnerability Management (Cloud Agent CSPM, WIZ.IO, Rapid7 Nexpose, Nessus, Cloud Native Services (CloudTrail, guard-duty, security Hub)

LINK

LinkedIn:
https://www.linkedin.com/in/prakhar-varma-b19116aa/

LANGUAGES

English

Hindi

HOBBIES

- I love listening to music and playing musical instruments like the guitar.
- I also enjoy traveling to explore vibrant places & swimming.
- Playing outdoor games such as basketball and badminton.

(SIEM ADMIN ENGINEER)

- Tools |SIEM ArcSight (Admin), Splunk, ELK, McAfee ESM, Q-radar, Log Analysis, Use case & Logical Rule creation Log integration | (OS Audit & application logs, Security Tools integration i.e: IPS, IDS, WAF, XDR Cortex, EDR CrowdStrike, firewall & network devices, Cloud Native Services such as CloudTrail, guard duty, security Hub, AWS WAF & DB integration, Custom Application integration) Log Analysis, Use case Key Responsibilities.
- System Management: Install, configure, ArcSight SIEM components (ESM, Logger's & Connectors) and comply with support metrics.
- Monitor system performance and troubleshoot issues.
- Data integration and Log Management: Configure data sources to ensure logs and events are correctly mapped and segregated in SIEM.
- Manage data retention policies and storage and archive.
- Configuring Health based alert for any anomaly within integrated log sources.
- Dashboard, Reporting, Compliance: Creating dashboards for Monitoring and Compliance.
- Generate and distribute regular security reports.
- Ensure compliance with relevant security standards and regulations.
- Documentation and Best Practices: Maintain documentation for configurations, procedures, and incident responses.
- Implement and promote best practices for SIEM management and security operations.
- Security Monitoring and Incident Response: Create and manage correlation rules to detect suspicious activities.
- Monitor security events and alerts generated by the SIEM for proactive measures and reducing false Positives.
- Creating correlated Trend and IOC based alerts for any Zero-day attacks.

Amdocs
Jun 2018 - Mar 2020
Pune

INFORMATION SECURITY SOC ANALYST

- Monitoring and securing network and infra on 24*7 operations from Global SOC for client and inhouse SOC.
- Managing Rules and creating Use case for new thereat scenarios.

COURSES

SPLUNK

SPLUNK ENTERPRISE SYSTEM ADMINISTRATION Aug 2022

SPLUNK FUNDAMENTALS CERTIFIED

Splunk

Oct 2019

ISO 27001
Lead Implementer

Exemplar Global

Arp 2025 - May 2025

LEARNING GDPR

LinkedIn

Oct 2021 - Oct 2021

PERSONAL DETAILS

Nationality:
Indian

- Maturing (fine-tuning) the current rules helping in reducing the Noise in traffic monitoring to add value to the system and organization.
- Streamlining the process and workflow for better efficiency of the team.
- Worked on a smooth transition of SOC workflow from traditional SIEM tool (Arc-sight) to SOAR.
- Creating multiple repots and providing data to higher Management.

General Mills

Feb 2016 - Feb 2018
Mumbai

TECHNICAL SPECIALIST

- The primary roles included incident response to all the risk and issues addressed to CSIRT Prime job to work on the incidents with deep investigation on the end device for remediation using tools such as SIEM IBM (Q-Radar).
- Reach the root cause for the incident and look for ways to fill the gap.
- Cleaning Host machine (Manual) using Kansa report.
- Keeping an eye on special rules from Symantec Endpoint Protection (SEP).
- Working on Phishing mails, categorization and recall using PhishMe.
- General understanding of Threat intelligence.

Reliance Jio Infocomm

Jun 2014 - Jun 2016
Mumbai

ASSISTANT MANAGER

- I have experience on Security Information and Event Management (SIEM), as a result I am familiar with the McAfee's Nitro ESM (9.5).
- My prime work includes Security Log Monitoring from various organizational network devices.
- I do log monitoring and event analysis as a part of my daily activity.
- Develop a correlated picture of what is occurring right now in an enterprise through integration of information from a variety of devices with SIEM tool (McAfee Nitro), then normalizing and correlating the information to develop modules that provides real-time (or near real-time) reporting in SOC.
- Understanding Security Log, Monitoring from various organizational network devices.
- I have a good log reading capability for Firewall, PIM, Windows security Events, Active Directory, AV log.
- Understanding of Correlation rules to reduce the false positives and to generate the alerts/offenses/notifications for the attac