



ROSHAN ASHOK SURWADE

cyber Security Specialist Lead

7798456112,8275034180

roshansurwade1198@gmail.com

Bhusaval, IN

<https://www.linkedin.com/in/roshan-surwade-715145155>

Date of Birth: 11/04/1998

Cyber security professional with 4+ years of work experience in Information Technology and information Security looking to secure a challenging Cyber Security Specialist role at your Company. With comprehensive technical acumen, a strong foundation in Ethical Hacking, and experience handling high-level projects, I aim to facilitate robust cybersecurity solutions, effectively protecting sensitive data and network systems. Audit and compliance management

My goal is to leverage my skills to enhance the company's cybersecurity strengths and contribute dynamically to its vision of delivering innovative technology services.

Professional Summary

4+ years of professional experience working extensively in information technology and information security.

Proficient in Endpoint Protection, Endpoint Encryption, DCT, IAM, FAM, NAC, MDM, PATCH MANAGEMENT, Digital Right Management DNS security DLP, Email Security, Web Security, SIEM,

SailPoint IdentityIQ, CyberArk Development, CPM, CCP, PSM, Active Directory, identity Governance and Administration (IGA), and Vulnerability Management framework specialized for VoIP/UC systems. TCP, UDP, SIP, RTP protocols and contains And Security. Expertise in bid process (RFI/REQ/RFP) technical bid response effort estimation and solution design.

CFeSkilled in ethical hacking, initiating, planning, executing, tracking/monitoring, controlling and closing projects as scheduled.

Experience in implementing operational processes for increased efficiency and cost reduction Possess a knack for software implementation and support, network designing and installation.

Proven experience working with cross-functional teams and providing multi-tiered information and assistance.

Audit and compliance management

VAPT, Web Application Mobile Application Network security Malware Analysis and Reverse engineering

Expertise in Symantec Endpoint Protection, ISO 27001, Symantec Endpoint Encryption, McAfee ePO & McAfee EPEPC/FDE systems

Solved challenging and complex IT security issues Including Cryptolocker, Locky, Zepto, WannaCry Petya, and Bad Rabbit

Career Timeline

- Mar 2023 - Feb 2024 **cyber Security Specialist Lead**
Globe active technology limited Bangalore
- Jan 2020 - Mar 2023 **Cyber Security Engineer**
Globe active technology limited

Work Experience

- Mar 2023 - Feb 2024 **cyber Security Specialist Lead**
Globe active technology limited Bangalore
Handled challenging ransomware issues such as Cryptolocker, Locky, Zepto, WannaCry Petya, and Bad Rabbit.
Strong exposure in conducting VAPT engagements with clients starting from effort estimation till project closure. Leading, molding, and mentoring a small team of security testers for efficient security testing. Have conducted VAPT

Soft Skills

- Quick Learner
- Performs well under Pressure
- Excellent Communication
- Effective Team Player
- Kubernetsles tool
- Exceptional Ability to Multitask

Technical Skills

- Malware Analysis
- Computer Forensics
- Digital Forensic
- ISO 27001
- Symantec Endpoint Encryption
- Cloud Computing
- Digital Forensics
- Email Security
- Governance Risk Management
- OWASP
- Firewalls Security
- Symantec Endpoint Protection
- Web Application Security
- Ethical Hacking
- Mobile Security
- VPN
- CompTIA Security
- Vulnerability Management
- CyberArk Development
- ITIL
- Network Security
- McAfee ePO & McAfee EPEPC/FDE
- SOAR

Core Competencies

- Leadership
- Cyber Security
- Project Management
- Technical Knowledge
- Problem Solving

engagements with respect to Web application security, Mobile application security, API and Infrastructure security, Source code review and related audits.

Mobile Device Management by Sophos and Iantel,

Patch Management by Ivanti, Digital Right Management by Byndes and Seclore.

Conducted regular access reviews and audits to ensure compliance with regulatory standards and internal policies.

Kubernetes network policy using SIG

Vulnerability assessment for containers by Clair, Wireshark, Qualys tool, Tenable.

Data leakage protection by Forcepoint

Security control application activity using Falco.

DNS Security by Palo Alto Network DNS and Auto DNS by EfficientIP

Email & Application Security, Research on new malware families

Leveraging threat intelligence, clustering prevalent malware and tracking APTs to establish attack chain.

Performed continuous real-time monitoring of security events and incidents using SIEM tools (Splunk, ELK, Exabeam),

identifying and responding to security threats, vulnerabilities, and suspicious activities. Utilized EDR solutions (CrowdStrike, Carbon Black, SentinelOne, Microsoft Defender) to detect, investigate, and respond to

endpoint threats. Developed and fine-tuned custom detection rules in SIEM and EDR tools to improve threat detection accuracy and reduce false positives. Also, collaborate with cross-functional teams to mitigate security threats.

Monitored user behavior alerts within Azure Active Directory to identify potential security risks, such as unusual sign-ins,

anomalous activities, and unauthorized access attempts. Conducted thorough investigations into flagged alerts, analyzing user activities and access patterns to determine the legitimacy of actions and assess potential threats.

Utilized email gateway solutions (Proofpoint, Mimecast, Microsoft Defender) to analyze inbound and outbound email traffic, identifying and blocking malicious emails such as phishing, spam, and malware. Leveraged sandboxing technologies (Falcon, Triage) to securely execute and examine suspicious email attachments and URLs.

Implemented custom email filtering rules and policies in Proofpoint to enhance threat detection and prevention capabilities, reducing false positives and improving overall email security. Customized policies to block phishing, malware, and spam based on organizational needs, industry best practices, and emerging threat intelligence.

Monitored and analyzed TAP threat intelligence, identifying and mitigating targeted attacks through real-time threat insights and URL Defense technology.

Leveraged TRAP to automatically quarantine malicious emails post-delivery, reducing manual intervention and speeding up response times to email-based threats.

Enforced DLP policies to prevent unauthorized access, transmission, or storage of confidential information, significantly reducing the risk of data breaches. Created customized policies for individual website access based on user roles and business needs. Reviewed website and content categorization, and contacted vendor support (Talos, Cisco) for resolution in case of incorrect categorization.

Managed SOAR platform (Swimlane) and automated incident response workflows, integrating various security tools (SIEM, EDR, threat intelligence) to streamline detection, investigation, and remediation of security threats. Responsible for training new SOC analysts, assisting with intricate cybersecurity investigations as part of threat response activities, and facilitating the escalation of cybersecurity incidents.

Create, maintain, and update SOP documentation for SOC threat response playbooks, manage metrics reporting, and ensure accurate analysis for the cyber defense team.

Conducted threat hunting activities across available security devices after validating the IOCS will proceed to block these threats on all security devices and notify the client accordingly.

Certifications

- **Diploma in Digital Forensic Investigation** (Alison - 2024)
- **ITIL 4 Fundamentals** (Alison - 2024)
- **ISO/IEC 27001** (Alison - 2024)
- **Certified Ethical Hacker** (EC Council - 2024)
- **CompTIA Security** (CompTIA - 2024)
- **Certification of Cyber Security** (The TechUnique Academy - 2023)
- **Digital Forensic Essentials** (EC Council - 2023)
- **Dark Web** (Guvi - 2021)
- **Certified Cyber Warrior** (HackingFlix - 2021)

Education

- **B.Tech**
Zeal College of Engineering and Research Pune
Aug 2016 - Jun 2020

Languages

English Marathi Hindi

Hobbies

Playing Cricket Playing Carrom

Playing Badminton

Hacking Programming

Cybersecurity Reading

Achievements

- **Presale Engineer:**
Working as consultant for cyber security solution of different technologies leading OEMs
Working with sales team and outlining security solution architecture.
Responsible for RFP's response, OEM interaction and solution finalization
Responsible for actively driving and managing the pre-sales process with direct and channel customers.
Articulate the company's technology and product portfolio, positioning to both business and technical folks.
Accomplishes project implementation activities and ensures customer implementations are completed on time and within budget, thereby realizing the firm's sales and profitability targets while meeting customer expectations.
Collaborates with sales, service and technical support resources to ensure implemented projects, accurately

Managed the ITSM tool (ServiceNow) to ensure smooth operation and timely resolution of incidents and requests Monitored and tracked service tickets, ensuring compliance with SLAs and efficient incident management and escalation

Contacting end users and initiating remote sessions to perform necessary remedial steps when required Regularly participated in weekly meetings, offering suggestions, feedback, and opinions to improve SOC processes.

Identity Access Management

Salipoint IQ: (Team Handling)

Orchestrated the implementation of SaliPoint Identity! Q to automate identity lifecycle management reducing manual tasks by 35%.

Experience in all Components of cyberArk ie PVWA, EPV, CPM, PSM, AM, PTACCPA and also an conjur PSM custom connectors CPM plugins Proficient in CyberArk development to perform activities like custom CPM, CCP and PSM plugin and connector development design as per the new requirements.

Customized IdentityIQ workflows, connectors, and role definitions to meet the organization's specific access control requirements.

Collaborated with business units to develop and enforce identity

governance policies and access certification processes Implemented access request and approval workflows, enhancing user experience and security.

Privilege Access Monogment By Cyber ark and Beyond trust

Leveraging threat intelligence, clustering prevalent malware and tracking APTs to establish attack chain.

Reverse Engineering malware (PE, Non-PE, Powershell, Scripts Documents and PUA classification)

Researched and Authored 100+ generic/heuristic signatures to detect malware and incident response

Tracked and blocked advanced malware attacks involving packing obfuscation and anti-analysis features and improved detection efficacy by 30%

- Conducted digital forensic investigations for financial evasion cases.

- Employed industry-standard tools such as Autopsy, Cellebrite Inseyets, Forensic Toolkit (FTK), FTK Imager, Magnet AXIOM, Oxygen Forensic® Detective, PALADIN OS, Kali OS, Cellebrite Digital Collector to acquire, analyse, and preserve digital evidence.

Examine recovered data for information of relevance to the issue at hand like financial fraud forensic

Conducted regular access reviews and audits to ensure compliance with regulatory standards and internal policies.

Lead scope discussions and client interactions to ensure clear understanding and alignment.

Drafting and Reviewing of Policy, Procedure and SOP5

Assisting Team Leader in IT Systems Control Audit, ISO 27001 Internal Audits, ITGC Audit

Identified control gaps in processes, procedures

and systems through in-depth review Preparing working documents, reports and supporting documents for audit findings

Jan 2020 - Mar 2023

Cyber Security Engineer

Globe active technology limited

Performed continuous real-time monitoring of security events and incidents using SIEM tools (SplunkELKExabeam), identifying and responding to security threats, vulnerabilities, and suspicious activities Utilized EDR solutions

(CrowdStrike Carbon Black,

SentinelOne, Microsoft Defender) to detect, investigate, and respond to

endpoint threats. Developed and fine-tuned custom detection rules in SIEM and EDR tools to improve threat detection accuracy and reduce

false positives. Also, collaborate with cross-functional teams to mitigate security threats.

Monitored user behavior alerts within Azure Active Directory to identify potential security risks, such as unusual sign-ins.

anomalous activities, and unauthorized access attempts. Conducted thorough investigations into flagged alerts, analyzing user activities and access patterns to determine the legitimacy of actions and assess potential threats.

Utilized email gateway solutions (Proofpoint, Mimecast, Microsoft defender) to analyze inbound and outbound email traffic identifying and blocking malicious emails such as phishing, spam, and malware. Leveraged sandboxing technologies

(Falcon, Triage) to securely execute and examine suspicious email attachments and URLs.

Implemented custom email filtering rules and policies in Proofpoint to enhance threat detection and prevention capabilities, reducing false positives and improving overall email security. Customized policies to block phishing, malware, and spam based on organizational needs, industry best practices, and emerging threat intelligence.

Monitored and analyzed TAP threat intelligence, identifying and mitigating targeted attacks through real-time threat insights and URL Defense technology

Leveraged TRAP to automatically quarantine malicious emails post-delivery, reducing manual intervention and speeding up

response times to email-based threats

Enforced DLP policies to prevent unauthorized access, transmission, or storage of confidential information significantly reducing the risk of data breaches. Created customized policies for individual website access based on user roles and business needs.

address. customer needs and are appropriately supported by key

customer personnel -Provides

professional development to team-

member sales associates in order to

enhance their product

knowledge, technical

Reviewing website and content categorization, and contacting vendor support (TalosCiscofor resolution in case of incorrect categorization.

Managed SOAR platform (Swimlane) and automated incident response workflows, integrating various security tools (SIEMEDR, threat intelligence) to streamline detection, investigation, and remediation of security threats. Responsible for training new SOC analysts, assisting with intricate cybersecurity investigations as part of Threat response activities, and facilitating the escalation of cybersecurity incidents.

Create, maintain, and update SOP documentation for SOC Threat response playbooks, manage metrics reporting, and ensure accurate analysis for the cyber defense team.

Conducted threat hunting activities across available security devices after validating the IOCSWill proceed to block these threats on all security devices and notify the client accordingly.

Managed the ITSM tool (ServiceNow) to ensure smooth operation and timely resolution of incidents and requests. Monitored and tracked

service tickets, ensuring compliance with SLAs and efficient incident management and escalation

Contacting end users and initiating remote sessions to perform necessary remedial steps when required. Regularly participated in weekly meetings, offering suggestions, feedback, and opinions to improve SOC processes

Identity Access Manegment

Sailpoint Q:

Orchestrated the implementation of SailPoint IdentityQ to automate identity lifecycle management, reducing manual tasks by 35%.

Conducted digital forensic investigations for Financial

Experience in all Components of cyberArk ie PVWA, EPV,CPM,PSM, AAM,PTACCPA and also on conjur.

PSM custom connectors CPM plugins

Proficient in CyberArk development to perform activities like custom CPM, CCP and PSM pilugin and connector development design as per the new requirements.

Customized IdentityIQ workflows, connectors, and role definitions to meet the organization's specific access control requirements.

Collaborated with business units to develop and enforce identity governance policies and access certification processes. implemented

access request and approval workflows, enhancing user experience and security.

Conducted digital forensic investigations for financial evasion cases.

Employed industry-standard tools such as Autopsy, Cellebrite Physical Analyzer, Cellebrite UFED, FTK Enterprise, FTK Imager, Magnet AXIOM, Oxygen Forensic® Detective, PALADIN to acquire, analyse, and preserve digital evidence.

Recovered and examined data from Computer (PC, Linux & Mac), Smartphones (Android & iOS) and Servers (Windows).

Examine recovered data for information of relevance to the issue at hand like bitcoin forensic and financial fraud forensic

• Provide technical summary of findings in accordance with established reporting procedures in the Income Tax Department.

Conducted regular access audits to ensure compliance with regulatory standards and internal policies.

Lead scope discussions and client interactions to ensure clear understanding and alignment.

Drafting and Reviewing of Policy, Procedure and SOP5

Assisting Team Leader in IT Systems Control Audit, ISO 27001 Internal Audits, ITGC Audit Identified control

gaps in processes, procedures and systems through in-depth review Preparing working documents, reports and supporting documents for audit findings

Projects

A leading mobile manufacturing company based out of Finland and a biotechnology company based out of France.

Managed full disk encryption by providing tier three level support for 14000+ encrypted laptops.

Proficient in CyberArk development to perform activities like custom CPM,CCP and PSM connector development as requirements.

Implemented various AV policies to the client infrastructure Prevented virus outbreaks by proactively monitoring viruses and threats.

Email & Application Security, Malware Anaisya threat intelligence End to End Management and Monitoring af End Point Security Services.

Managed Symantec Endpoint Protection infrastructure after migration.

Upgrading client to latest version remotely. Handled challenging ransomware issues.

Symantec Endpoint Protection and Encryption.

Strong excle and reporting concepts

Leading banking firm based out of Canada, HR consultancy firm based out of US, and an Oil Refinery firm based out of US.

Implemented AV policies in the Client's infrastructure.

Prevented virus outbreaks by proactively monitoring viruses and threats.

network to ensure the risks are mitigated on time.

Leveraged strong excel and reporting concepts in project executions.

Email & Application Security, Malware Analsya threat intelligence.

. Part of the migration team, the products migration from McAfree to MBAM

Centralized Management of reporting console to set policies, demonstrate compliancejidentify unencrypted laptop and respond rapidly to loss or theft

Console level management of providing recovery key EEPC Code and work with user to fix login issues remotely.

Managed the monitoring tool SSIM and generated reports

Generated enterprise wide report for multiple security solutions, with detailed compliance reporting. Regional share level

management of maintaining recovery key information providing authentication tokens for encrypting anddecrypting laptops

Played a vital role in mag rating Native BitLocker machines To MBAM Part of the migration team the product migration from McAfee to MBAM