SAURABH CHAVAN

CYBER SECURITY ANALYST

+1(248)947-7171 • Saurabh.chavan0330@gmail.com • Canton, MI, 48187 • LinkedIn

PROFESSIONAL SUMMARY

Dedicated Cybersecurity Analyst with over 5 years of experience across SOC Tier 2 operations, incident response, and threat detection. Proven expertise in SIEM correlation rules, SOAR automation, vulnerability management, and compliance with NIST, ISO 27001, and PCI-DSS. Adept at securing cloud and hybrid environments, supporting Zero Trust architecture, and reducing risk exposure through proactive analysis and policy enforcement. Strong team collaborator with a sharp eye for threat patterns and operational efficiency.

SKILLS

Security Operations & Threat Detection

- SIEM Monitoring: Splunk, IBM QRadar, ArcSight, Elastic SIEM, Datadog
- SOAR Platforms, MITRE ATT&CK, IOC Analysis, Threat Hunting, Correlation Rule Tuning
- EDR/XDR: CrowdStrike, Carbon Black, Windows Defender ATP
- Malware Analysis, Incident Response, Root Cause Analysis, Insider Threats

Network & Infrastructure Security

- Network Protocols: TCP/IP, DNS, DHCP, VPN
- Firewalls: Palo Alto, Fortinet, Cisco ASA
- IDS/IPS: Snort, Suricata, Proxy Policies, NAC

Cloud Security & Virtualization

- AWS: CloudTrail, GuardDuty, Security Hub
- Azure: Azure Security Center, Azure AD, Conditional Access
- GCP Security Command Center
- Docker, Kubernetes, IAM, S3, EC2

Vulnerability & Risk Management

- Scanning: Nessus, Qualys, Rapid7, OpenVAS
- Penetration Testing: Metasploit, Burp Suite
- Third-party Risk Assessment, SOC 2, Risk Register Maintenance

Scripting & Automation

- Python, PowerShell, Bash
- SOAR Integration, Task Automation, Log Parsing Scripts

Governance, Risk & Compliance

- **Frameworks:** NIST 800-53, ISO 27001, PCI-DSS, CIS, HIPAA, GDPR
- **Tools:** ServiceNow GRC, Confluence, Policy Development

PROFESSIONAL EXPERIENCE

TECH MAHINDRA | *Sep 2020 to Oct 2022*

CYBERSECURITY ANALYST

- Acted as SOC Tier 2 analyst monitoring 24/7 alerts via Splunk and QRadar, triaging and escalating 300+ incidents.
- Reduced critical security risks by 35% through proactive vulnerability scanning using Nessus and Qualys.
- Contained endpoint threats using CrowdStrike Falcon, ensuring zero lateral movement across impacted systems.
- Collaborated on phishing awareness and simulation programs, lowering click rates by 60%.
- Created SIEM correlation rules to fine-tune detection of brute force, privilege escalation, and lateral movement attempts.
- Investigated malware via sandbox environments, performing RCA and coordinating cross-team remediation.
- Conducted third-party security reviews and evaluated SOC 2 reports for compliance assurance.
- Managed incident workflow in ServiceNow GRC and provided risk assessments to internal stakeholders.
- Supported firewall audits and VPN access policies using Palo Alto and Cisco ASA.
- Delivered dashboards and executive summaries in Power BI for leadership review.

MPHASIS | *Jul 2018 to Aug 2020*

INFORMATION SECURITY OPERATIONS ANALYST

- Monitored security logs and incidents in a hybrid environment, improving triage time by 30%.
- Assisted in deploying and reviewing IDS/IPS rules and firewall changes to harden the network perimeter.

- Managed IAM operations including RBAC, provisioning, and deprovisioning in Azure AD and Active Directory.
- Collaborated with threat intel to correlate alerts with emerging vulnerabilities and IOC feeds.
- Automated daily alerting and reporting tasks using PowerShell and Python scripts.
- Executed endpoint and server scans using Nessus/Qualys and ensured CVSS-based prioritization.
- Contributed to HIPAA and PCI-DSS audit readiness by gathering evidence and performing policy updates.
- Built dashboards and SLA trackers for incident metrics using Power BI.
- Responded to after-hours security events as part of the on-call escalation rotation.
- Delivered internal security awareness training aligned with Zero Trust principles.

MINDTREE | *Jan 2018 TO Jun 2018*
CYBERSECURITY ANALYST INTERN

- Supported daily log analysis and SIEM monitoring (Splunk) for over 500 security events.
- Conducted internal vulnerability scans with OpenVAS and Nessus and validated remediations.
- Created incident response playbooks and improved reaction times during tabletop exercises.
- Designed phishing simulation reports that informed future training initiatives.
- Assisted in aligning internal security practices with ISO 27001 during compliance audits.

EDUCATION

Lawrence Technological University – Southfield, MI | Jan 2023 – May 2025
Master of Science | Artificial Intelligence | 3.85/4

Savitribai Phule Pune University, India | Aug 2015 – May 2018
Bachelor of Engineering | Electronics and Telecommunication

CERTIFICATIONS

- ISC2 CC (Certified in Cybersecurity)
- Cisco Introduction to Cybersecurity
- Cisco Ethical Hacker
- TryHackMe SOC Level 1
- University of Michigan Applied Data Science with python specialization
- Deep Learning AI Deep learning specialization