Soma Nitin

Detection & Response Engineer

somanitin18@gmail.com +91 9849956140 Hyderabad, India

linkedin.com/in/somanitin

Summary

Cybersecurity engineer with 10+ years of experience across Endpoint Detection & Response (EDR), Extended Detection & Response (XDR), threat detection, security investigations, and security operations. Experienced in engineering and operationalizing endpoint security capabilities, onboarding 20+ XDR customers and 500+ EDR customers, and developing custom detections and response workflows across leading security platforms. Brings a combination of hands-on detection and response engineering, customer security assessments, endpoint investigations, and SOC leadership to improve security visibility, detection coverage, and response effectiveness.

Core Competencies

Detection Engineering · EDR & XDR Engineering · Threat Detection & Hunting · Incident Response & Security Investigations · Endpoint Security Engineering · EDR/XDR Onboarding · Custom Detection Development · Security Policy & Prevention Configuration · Response Automation · Threat Intelligence · SOC Operations & Leadership · Security Assessments

Technical Skills

EDR Platforms: CrowdStrike Falcon, SentinelOne, VMware Carbon Black, Microsoft Defender for Endpoint, Cisco AMP, Trend Micro
XDR Platforms: Palo Alto Cortex XDR, Cisco XDR
Detection & Response Engineering: Custom detections, detection rules, endpoint security policies, prevention controls, security configurations, CrowdStrike Fusion workflows, SentinelOne STAR rules, response workflows, endpoint investigations
SIEM & Security Monitoring: LogRhythm, ELK Stack, ArcSight
Email Security: Proofpoint, Symantec MessageLabs, Google Workspace / G-Suite, e-discovery
Proxy & DNS Security: Websense Content Gateway, Cisco Umbrella
Incident Management: IBM Resilient, BMC Remedy, ServiceNow, Jira
Cloud: Amazon Web Services (AWS)

Certifications

CERTIFICATIONS
- Palo Alto Certified XDR Engineer (Cortex)
- CrowdStrike Certified Falcon Administrator
- SentinelOne Certified Administrator
- SentinelOne Incident Response
- Trend Micro Vision One for Administrators
- Certified Ethical Hacker (CEH)
- MITRE ATT&CK Defender
- CompTIA Security+
- AWS Certified Cloud Practitioner

Professional Experience

Principal Security Engineer — Endpoint Detection & Response, *Proficio* 09/2022 – Present

- Engineered and operationalized EDR/XDR capabilities across customer environments, supporting endpoint visibility, security policy configuration, detection, investigation, and response.
- Onboarded and supported 20+ XDR customers and 500+ EDR customers across enterprise security environments.
- Designed, configured, and maintained endpoint security policies, prevention controls, exclusions, application controls, policy assignments, and related configurations across CrowdStrike Falcon, SentinelOne, VMware Carbon Black, and Microsoft Defender for Endpoint.
- Develop custom detections in Microsoft Defender for Endpoint and design and build CrowdStrike Fusion workflows and SentinelOne STAR rules to support threat identification, detection automation, and response use cases.
- Performed initial technical assessments of customers' existing environments, reviewing security configurations, endpoint policies, prevention controls, exclusions, detection capabilities, and operational readiness.
- Managed EDR deployment activities, including agent or sensor onboarding, endpoint health checks, policy assignments, upgrades, troubleshooting, and configuration-related issue resolution.
- Investigated endpoint alerts and suspicious activity using EDR telemetry, supporting threat analysis, triage, escalation, containment recommendations, and response activities.
- Investigated phishing emails and managed customer phishing mailbox requests, including suspicious-email analysis, validation, documentation, and escalation.

SOC Shift Lead — Security Response & Investigations, *Uber* 04/2020 – 09/2022

- *Led SOC shift operations* supporting security monitoring, incident response, threat investigations, and endpoint security operations, prioritizing and coordinating response to security events.
- *Coordinated end-to-end incident response*, including alert triage, validation, investigation, escalation, containment, and remediation of security incidents.
- *Guided analysts through complex security investigations*, analyzing network and endpoint findings, assessing incident impact, determining remediation actions, and supporting escalation decisions for high-priority threats.
- *Conducted threat hunting and host-based investigations* using SIEM and EDR platforms, applying threat intelligence to identify suspicious activity, indicators of compromise, and emerging threats.
- *Improved SOC operational effectiveness* through EDR optimization, workflow automation, SOP improvements, incident documentation, and knowledge transfer while collaborating with stakeholders on vulnerability mitigation and security improvements.

Security Analyst II - Threat Intelligence & Investigations 05/2018 – 04/2020

Diyar United Company

- Reviewing all the alarms and reporting any mistakes to the engineering team for correction
- Monitored and analyzed security events across SIEM, network, host-based intrusion detection, firewall, system, application, and database logs to identify suspicious activity and potential security incidents.
- Investigated security alerts, scan results, logs, and files throughout the incident response lifecycle, identifying indicators of compromise and recognizing potential cyber intrusions.
- Reviewed SIEM alerts and security monitoring use cases, identifying errors and recommending improvements to log correlation and security analytics.
- Supported analyst onboarding and knowledge transfer by training new team members on attack and malware analysis using LogRhythm and IBM Resilient for incident escalation and management.

Senior Executive — Cyber Defence Operations, *Vodafone* 07/2017 – 05/2018

- Supported cyber defence operations, security monitoring, incident analysis, and response activities across enterprise security environments.
- Investigated security alerts, assessed potential threats, and escalated incidents in accordance with established response procedures.

- Collaborated with security teams and stakeholders to support timely incident handling, monitoring effectiveness, and operational improvements.

First Line Security Support Engineer – CDO, *Vodafone* 05/2015 – 06/2017
- Provided first-line SOC support through security alert monitoring, initial analysis, triage, and escalation.
- Created and tracked incident tickets, coordinating with relevant teams to support investigation and resolution.
- Supported enterprise security monitoring technologies and day-to-day SOC operations, including foundational troubleshooting and response activities.

Education

Bachelor's in Computer and Information Sciences 2010 – 2014
Jawaharlal Nehru Technological University Hyderabad (JNTUH)

Pre University, *State Board of Intermediate Education* 2008 – 2010

HIGH SCHOOL, *St. Peters Public School* 1998 – 2008