A logo for security company

Description automatically generatedA black sign with white text

Description automatically generatedA blue and white square with black text

Description automatically generated**Kumar M**

**Sr. Security Analyst**

**PROFESSIONAL SYNOPSIS:**

* Information Security Professional with 9+ years of expertise in **Data Loss Prevention**, implementing network & security infrastructure systems, and Endpoint security.
* Led the administration and management of SOAR platforms such as Cortex XDR & Splunk Phantom.
* Led the evaluation and implementation of industry-standard security technologies, ensuring compliance with industry standards and best practices for **endpoint security** and **Data loss prevention**.
* Analyzed and compared technical features of various **endpoint protection tools (EDR)** such as **McAfee**, **Symantec**, **Traps/Cortex**, **Bluecoat**, and **Windows Defender**, enabling informed decision-making for deployment.
* Designed, deployed, and provided ongoing support for multiple endpoint protection tools, including hands-on configuration of **EDR solutions**, resulting in enhanced security posture and threat detection capabilities.
* Successfully executed security tool implementations and migrations, ensuring seamless transitions while maintaining operational efficiency and minimizing disruption to critical business processes.
* Developed and implemented data loss prevention strategies, including the configuration of policies and rules, to safeguard sensitive information and prevent unauthorized data disclosure.
* Demonstrated strong troubleshooting skills in resolving endpoint security-related issues, collaborating with system administrators and vendor support teams to quickly identify and resolve incidents, minimizing business impact.
* Established expertise in security incident management and incident response processes, enabling swift and effective response to security incidents, minimizing potential damage, and facilitating timely recovery.
* Implemented supplier and vendor security management procedures, ensuring that third-party providers adhered to necessary security controls and met the organization's security standards.
* Successfully managed projects throughout the entire lifecycle of evaluating, deploying, testing, monitoring, remediating, and supporting the Global IT Security framework, delivering projects on time and within budget.
* Leveraged exceptional communication and interpersonal skills to inspire and engage individuals, fostering a collaborative and motivated team environment to drive successful security initiatives.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Technology** | **Tools** |
| **Security Management** | McAfee ePolicy Orchestrator (McAfee ePO), Symantec, Proofpoint, Forcepoint, MS O365 & Bluecoat administration, sentinel |
| **SOAR** | Cortex SOAR, Splunk Phantom. |
| **Corporate Anti-virus solutions / HIPS** | McAfee, Symantec & Bluecoat |
| **CASB** | Proofpoint and O365 security (Purview) |
| **Endpoint Management** | Symantec / McAfee XDR / Cortex XDR |
| **Data Loss Prevention** | McAfee DLP, Proofpoint, O365 & Digital Guardian |
| **Web Filtering solution** | Websense/Forcepoint |
| **Email Security** | Cisco IronPort, Digital guardian, Proofpoint |
| **Disk Encryption solution** | McAfee FDE |
| **Two Factor Authentication** | RSA Secure ID, Vasco (Digi pass), Gemalto & DUO authentication |
| **GRC Tools** | Logic gate &ServiceNow. |
| **Compliance** | ISO27001, NIST & SOC2 |

**PROJECTS:**

**Client: FORTNA GA, USA.**

**Role: Sr. Security Analyst.**

**Duration: May 2024- Till Now.**

**Responsibilities:**

* Converted SPL queries into KQL queries for use in Microsoft Sentinel, ensuring accuracy and effectiveness in threat detection.
* Tested and validated detection queries, ensuring readiness for production deployment in a live environment.
* Created and optimized correlation rules and detection queries in Microsoft Sentinel to enhance threat detection and response capabilities.
* Proficiently worked with both SPL and KQL, leveraging expertise to create efficient and accurate detection rules.
* Collaborated with cross-functional teams to ensure the seamless integration of detection rules into Microsoft Sentinel and other security tools.
* Administered and deployed SOAR platforms, leading the design, testing, and automation of security controls.
* Created and managed automation playbooks within SOAR for streamlined incident response workflows.
* Integrated threat intelligence feeds into SOAR and Sentinel platforms to improve detection and response times.
* Oversaw firewall access controls and conducted regular exception reviews to ensure compliance with security standards.
* Configured and optimized XDR policies, and performed incident investigations based on events triggered in Cortex EDR.
* Coordinated vulnerability management efforts, working alongside the vulnerability team to ensure timely patching and remediation.
* Responsible for Cortex EDR endpoint and SOAR administration and deployment.
* Design, test, and deploy security controls aligned with industry standards.
* Drafting SOAR using run books.
* Technical leadership in operationalizing SOAR technology.
* Integration of new and existing tools into SOAR.
* Developing testing and deploying automation playbooks within the organization environment.
* Incorporate threat intelligence feeds into the SOAR platform to improve incident detection and response.
* Upgrade Endpoint Security consoles to the latest versions following best practices and defined processes.
* Perform firewall access controls and exception reviews.
* Work on new technology requirements, from analysing and testing to deploying the tools.
* Validate and approve security exceptions.
* Publish reports on security posture, incidents, and security implementations to the management team in weekly Management Review Meetings.
* Create runbooks to assist the team in investigating events and validating their impact and risk.
* Configure XDR rules and policies in line with the company's posture and security trends.
* Investigate incidents and take appropriate actions on events triggered on Cortex.

**Environment: Microsoft Sentinel, KQL, SPL, SOAR, Cortex EDR, XDR, Security controls, Automation Playbooks, Firewall Access Controls**

**Client: Equifax, NY, USA**

**Role: Security Analyst.**

**Duration: April 2023- April 2024**

**Responsibilities:**

* Work on designing and deploying security tools and technologies.
* Administer McAfee enterprise suite, including McAfee EDR (ENS), DLP, HIPS, Web Gateway, CASB, Application Control, and Encryption (FDE).
* Experience developing custom Phantom SOAR playbooks, workflows, and configurations.
* Experience integrating the Phantom SOAR platform with other tools from both a data and automation perspective.
* Focus on daily deployments, operations, and maintenance of solutions in the customer environment.
* Provide implementation and migration plan documentation before the scheduled upgrade.
* Perform Endpoint incident analysis for DLP and EDR incidents and take appropriate action.
* Work on security exceptions and apply them as per requirements.
* Collaborate with Data-centre engineers and Security teams to address complex networking issues, recommend configurations, and more.
* Administer Endpoint protection, Antivirus, HIPS, HDE, and EDR solutions.
* Play a key role in identifying cyber security risks and designing appropriate mitigation measures.
* Manage all Cyber Security systems, applications, policies, and processes on a day-to-day basis.
* Develop and implement the cybersecurity strategy and objectives.
* Perform final reviews of incident analysis reports from team members to initiate remediation actions.
* Ensure the incident identification, assessment, quantification, reporting, communication, mitigation, and monitoring.
* Establish supplier/vendor management procedures, create questionnaires, and implement required supplier security standards in compliance with requirements.
* Ensure compliance with SLAs, process adherence, and process improvement to achieve operational objectives.
* Revise and develop processes to enhance the current Security Operations Framework, review policies, and address challenges in managing SLAs.
* Manage the team and vendors, utilize resources effectively, and initiate corrective action when necessary for Security Operations.
* Coordinate with stakeholders and build and maintain positive working relationships.
* Serve as the Incident Manager to oversee all IT-related incidents.
* Conduct Information security Awareness training across the organization.

**Environment: ENS, DLP, HIPS, SOAR, Splunk phantom Web Gateway, CASB, Application Control, Encryption (FDE), Antivirus, HDE, EDR.**

**Client: Market Data Forecast Hyderabad, TE**

**Role: SOAR Analyst**

**Duration: October 2021- November 2022**

**Responsibilities:**

* Perform final reviews for analysis reports from team members to take remediation actions.
* Configure, maintain and monitor Websense Security Suite.
* Create rules/signatures in security tools to identify threats, respond to security alerts, and handle security incident remediation.
* Manage the relationship with Dell SecureWorks for IDS and firewall intrusion monitoring.
* Evaluate and monitor all IDS and IPS appliances.
* Complete quarterly firewall reviews to meet company security standards.
* Monitor Virus and Trojan infections and collaborate with the Helpdesk to resolve issues.
* QRadar (SIEM) monitoring and administration.
* Monitor the network for malicious activity and coordinate with various groups for a prompt response.
* Administer malware detection tools (Antivirus and Malware tools).
* Gather intelligence from multiple sources and take action to prevent attacks.
* Experience in email header analysis to verify email legitimacy.
* Monitor security logs for attempted intrusions through Checkpoint and individual Firewalls.

**Environment:** **Websense Security Suite, Dell SecureWorks (for IDS and firewall monitoring), IDS and IPS appliances, QRadar, Checkpoint, and individual Firewalls.**

**Client: Warner Bros Discovery/Cognizant Hyderabad, TE**

**Role: Security Analyst**

**Duration: April 2018 – September 2021**

**Responsibilities:**

* Team Lead responsible for Management of Security Information and event Management Solutions, integrating network components, applications, and servers to SIEM solutions. Exposure to troubleshooting SIEM integration issues pertaining to network components, applications, and Servers and managing a team of 8 L1 Security engineers
* Validate rules/signatures in security tools that are designed to identify threats in the environment. Respond to security alerts, triage events, and handle remediation of security incidents. Perform system forensic analysis to identify, contain, and remediate sophisticated threats.
* Perform advanced monitoring and reporting related to IT security systems. Analyze network traffic patterns, system logs, and audit files to ensure they are compliant with existing security policies.
* Maintain documentation (CSRT) related to the organization's network, network security management systems, procedures, and administrative stats reports.
* Configure, implement and troubleshoot a variety of Hardware / Software Products, including SSL VPN, Firewalls, IPS, NAC, Routers, Switches, email gateway, internet proxy, and endpoint security solutions.
* Member of the incident management team.
* Tracking and assisting in the management of the resolution of reported operational security issues.
* Recommend actions, review plans, and monitor the progress of remedial actions.
* Resolving security risks identified as a result of reviews and audits, of the customer environment, changes in operating practices or processes, changes in technology, etc.
* Remote monitoring and analysis of security events on IDS and IPS devices with the help of SourceFire.
* Identifying different types of attacks on Celgene host machines and suggesting appropriate decisions to the management.
* Escalating suspicious events to senior analyst and director of IT security operations
* Identifying malicious hosts and software in across all machines of my client
* Identifying the risk hosts with the help of NAC (Network access controller) through SIEM

**Environment: Security Information and Event Management Solutions, Security tools for validating rules and signatures, System forensic analysis tools, SSL VPN, Firewalls, IPS, NAC, Routers, Switches, email gateway, internet proxy, and endpoint security solutions, Sourcefire, Network Access Controller (NAC), SIEM.**

**Client: Synchrony Financial Hyderabad, TE**

**Role: Technical Support Executive**

**Duration: June 2016 – March 2018**

**Responsibilities:**

* Handling level 2 calls for tech support.
* Monitor, facilitate, and develop training activities for new agents.
* Actively used quality management system to compile, track, and trend agent performance.
* Coach team members regarding their performance and suggest and implement corrective actions as required.
* Handling team-huddles.
* Part of all access management team.
* Create and manage user administration and access control documentation. Planning activities for team motivation.
* Took part in projects to increase employee and customer satisfaction.
* Responsible for Team Engagement and controlling attrition.

**Education:**

**Bachelor’s in Bharat Institute of Engineering and Technology- 2017**