PRATHMESH VISHNU

@ prathameshvishnu12@gmail.com

☎ 8830987448

Hyderabad, TG 500038

EDUCATION

Bachelor Degree, Computers
Swami Ramanand Tirth Marathwada University, Nanded, India
May 2020

PROFESSIONAL SUMMARY

Proactive SOC Analyst with over 4 years of experience in cybersecurity operations, specializing in monitoring, detection, and mitigation of advanced cyber threats.

Proficient in using cutting-edge tools like Splunk SIEM, Azure Sentinel, SentinelOne EDR/XDR, and Microsoft Defender solutions. Expertise in analyzing firewall, proxy, and IDS/IPS logs to identify threats such as lateral movement, command and control (C2) traffic, and persistence techniques. Adept at improving security posture through meticulous investigation and incident response.

SKILLS

Technical Skills:

- **SIEM Tools**: Splunk SIEM, Azure Sentinel
- **Cloud Security**: Microsoft Defender for Cloud, O365 Defender
- **Threat Hunting**: Command and Control traffic detection, Lateral Movement, Persistence alerts
- **EDR/XDR Solutions**: SentinelOne EDR/XDR, Microsoft Defender for Endpoints
- **Log Analysis**: Firewall logs, Proxy logs, IDS/IPS logs
- **Security Tools**: Antivirus solutions, DLP tools, and Vulnerability Management

WORK HISTORY

April 2022 - Current
Genpact - SOC Analyst, Hyderabad, India

- Monitor and analyze security events using Splunk SIEM to detect potential threats.
- Investigate and respond to endpoint incidents using SentinelOne EDR/XDR and Microsoft Defender for Endpoints.
- Analyze firewall, proxy, and IDS/IPS logs to identify anomalous activities, including lateral movement and persistence attempts.
- Detect and mitigate command and control (C2) traffic by correlating logs and leveraging threat intelligence.
- Conduct root cause analysis for security incidents and implement measures to prevent recurrence.
- Collaborate with IT and network teams to strengthen security posture and minimize vulnerabilities.
- Analyzed PowerShell-related alerts, new process creation, and unauthorized lateral movement attempts.
- Investigate traffic patterns in firewall logs to identify unauthorized access, port scans, and unexpected data exfiltration attempts.

- Analyze intrusion detection and prevention system logs for potentialindicators of compromise (IoCs).
- Investigate alerts related to known signatures, suspicious traffic patterns, and rule violations.
- Monitor web proxy logs for unauthorized web access, malware-hosting domains, and anomalous outbound traffic.
- Identify and block access to malicious websites and suspicious IPs.
- Track activities such as PowerShell commands, registry changes, and fireless malware behavior.
- Monitor logs from O365 Defender or email security gateways to identify phishing attempts, spam, malware attachments, and spoofing attacks.
- Participated in threat-hunting activities, focusing on persistence techniques and privilege escalation.
- Monitor Windows, Active Directory, and Linux authentication logs for failed logins, privilege escalations, or lateral movement attempts.

May 2020 - March 2022
Sonata Software - Security Analyst, Hyderabad, India

- I was monitored and analyzed security events using Azure Sentinel SIEM to identify potential threats.
- We investigated and mitigated endpoint security incidents with SentinelOne EDR/XDR, including malware containment and lateral movement prevention.
- Performed advanced threat detection and response using O365 Defender, addressing phishing, spam, and ransomware incidents.
- Conducted proactive log analysis of firewalls, IDS/IPS, and proxy logs to identify suspicious activities and potential breaches.
- Continuously monitor and analyze logs from multiple sources, including firewalls, IDS/IPS, proxy servers, antivirus, email gateways, and DLP solutions.
- Responded to phishing and business email incidents using O365 Defender, reducing email-based attacks.
- Proactively analyzed firewall, IDS/IPS, and proxy logs to identify anomalies and suspicious activities.
- Investigate traffic patterns in firewall logs to identify unauthorized access, port scans, and unexpected data exfiltration attempts.
- Analyze intrusion detection and prevention system logs for potential indicators of compromise (IoCs).

CERTIFICATIONS

- Splunk Core Certified User
- Microsoft Certified: Security Operations Analyst Associate
- SentinelOne Certified Engineer (S1CE)

ADDITIONAL INFORMATION

Key Accomplishments:

- Reduced incident response time by 30% by optimizing SIEM correlation rules and tuning alert thresholds.

- Successfully mitigated a phishing attack campaign targeting O365 by identifying compromised accounts and implementing MFA.
- Detected and remediated a C2 server communication incident through advanced log correlation and threat hunting activities.
- Enhanced the organization's threat detection capabilities by implementing MITRE ATT&CK-based correlation rules.