Purna Venkateswarlu Pula

Kansas City, MO | +1 (913) 263-4108 | pulapurna2707@gmail.com | linkedin.com/in/pula-purna-venkateswarlu

Professional Summary

Cybersecurity Engineer with nearly 4 years of progressive experience across security engineering, Security Operations Center (SOC), incident response, threat detection, vulnerability management, endpoint security, cloud security, network security, malware analysis, and systems administration. Hands-on experience with CrowdStrike Falcon, Microsoft Defender, Splunk, Microsoft Sentinel, AWS Security Hub, GuardDuty, CloudTrail, IAM, Active Directory, SIEM, EDR, IDS/IPS, and vulnerability management technologies. Skilled in investigating complex security incidents, analyzing endpoint and network telemetry, identifying indicators of compromise, remediating vulnerabilities, strengthening IAM and cloud security controls, and automating security operations using Python, PowerShell, and Bash. Proven ability to collaborate with Infrastructure, Networking, IAM, Cloud, Application, and Security teams to reduce cyber risk and strengthen enterprise security posture.

Technical Skills

Security Engineering: Cybersecurity Engineering, Security Architecture, Security Operations, Security Monitoring, Security Hardening, Security Controls, Risk Mitigation, Security Configuration, Security Remediation

SIEM & Security Monitoring: Splunk, Microsoft Sentinel, SIEM, KQL, SPL, Log Analysis, Event Correlation, Detection Engineering, Alert Triage, Security Analytics, Detection Rule Tuning

Endpoint Security & EDR: CrowdStrike Falcon, Microsoft Defender for Endpoint, EDR, Endpoint Protection, Endpoint Detection, Endpoint Investigation, Endpoint Isolation, Malware Detection, Threat Hunting

Incident Response & SOC: Incident Response, Incident Investigation, SOC Operations, Alert Triage, Threat Detection, Containment, Eradication, Root Cause Analysis, IOC Analysis, Incident Documentation

Vulnerability Management: Vulnerability Assessment, Vulnerability Management, CVE Analysis, Risk Prioritization, Patch Management, Remediation Tracking, Security Configuration Review, System Hardening, CIS Benchmarks

Cloud Security: AWS, AWS Security Hub, Amazon GuardDuty, Amazon Inspector, AWS IAM, IAM Access Analyzer, AWS CloudTrail, VPC Flow Logs, AWS WAF, CSPM, Cloud Workload Protection

Identity & Access Management: Active Directory, Microsoft Entra ID, AWS IAM, RBAC, MFA, Least Privilege, Access Reviews, Security Groups, Privileged Access, Identity Security

Network Security: TCP/IP, DNS, DHCP, HTTP/HTTPS, VPN, VLANs, Firewalls, IDS/IPS, SSL/TLS, Network Monitoring, Network Traffic Analysis, VPC Security

Malware Analysis & Forensics: Malware Triage, Static Analysis, Dynamic Analysis, Digital Forensics, Memory Forensics, Volatility, Ghidra, IDA Pro, x64dbg, IOC Analysis

DevSecOps & Application Security: SAST, DAST, SCA, Container Security, CI/CD Security, GitHub Actions, GitLab CI, Infrastructure as Code, OWASP Top 10, Shift-Left Security

Automation & Scripting: Python, PowerShell, Bash, AWS Lambda, Amazon EventBridge, Security Automation, Automated Remediation

Systems Administration: Windows Server, Windows 10/11, Linux, Active Directory, Group Policy, Microsoft 365, Patch Management, Endpoint Administration

Frameworks & Compliance: NIST Cybersecurity Framework, CIS Controls, CIS Benchmarks, SOC 2, Security Control Validation, Risk Management, Security Documentation

Professional Experience

Juniper Networks — United States, Remote

Cybersecurity Engineer — Apr 2025 – Jul 2026

- Investigated escalated endpoint, user-access, application, authentication, and connectivity incidents using enterprise security and support tools to restore secure business operations.
- Troubleshot Windows, Microsoft 365, Active Directory, endpoint security, authentication, VPN, DNS, and network-related issues to identify root causes and minimize service disruption.
- Supported Active Directory and Microsoft Entra ID account, access, authentication, and permission issues to maintain secure and efficient user access to enterprise resources.
- Analyzed Microsoft Defender and CrowdStrike Falcon endpoint events to diagnose security-related workstation issues and coordinate corrective actions with technical teams.
- Investigated user-reported phishing, malware, account compromise, suspicious authentication, and endpoint incidents to protect users and maintain secure enterprise operations.
- Collaborated with Service Desk, Infrastructure, Networking, IAM, Cloud, Application, and Security teams to resolve escalated incidents requiring cross-functional technical support.
- Performed root cause analysis on recurring technical and security incidents to identify underlying problems and recommend corrective actions that improved service reliability.
- Validated Windows patches, endpoint security updates, configuration changes, and remediation activities to maintain secure and stable production environments.

- Automated recurring administrative, reporting, log-analysis, and troubleshooting activities using PowerShell and Python to improve operational efficiency.
- Maintained incident documentation, technical findings, troubleshooting procedures, configuration records, and SOPs to support consistent issue resolution and knowledge transfer.
- Communicated technical findings and remediation steps to technical and non-technical stakeholders to support timely incident resolution and informed decision-making.

Pasonet Technologies Pvt Ltd (Client: Morgan Stanley) Chennai, India

SOC Analyst L2 Mar 2023 – Dec 2023

- Investigated escalated security incidents using Splunk, Microsoft Sentinel, Microsoft Defender, endpoint telemetry, and network logs to identify threats and coordinate containment.
- Correlated endpoint, identity, authentication, firewall, VPN, DNS, and network events to determine attack scope and identify indicators of compromise during complex investigations.
- Investigated malware, phishing, suspicious authentication, unauthorized access, endpoint compromise, and network threats to recommend appropriate containment and remediation actions.
- Analyzed endpoint processes, authentication events, user activity, network connections, and security telemetry to distinguish malicious behavior from legitimate enterprise activity.
- Reviewed Active Directory accounts, privileged access, authentication activity, and security groups to identify excessive permissions and potential identity-related risks.
- Analyzed firewall, IDS/IPS, DNS, VPN, and network-security telemetry to detect suspicious communications and identify potential network-based attacks.
- Performed vulnerability assessments and validated endpoint patches, Windows updates, and security configurations to reduce exposure to known vulnerabilities.
- Prioritized security incidents based on severity, affected assets, threat indicators, and business impact to accelerate response to high-risk events.
- Coordinated containment and remediation activities with Infrastructure, Networking, IAM, Endpoint, Application, and Security teams to restore secure operations.
- Tuned security monitoring and detection logic based on recurring alerts and investigation findings to improve signal quality and reduce unnecessary analyst workload.
- Produced incident reports, root cause findings, technical evidence, investigation timelines, and remediation recommendations to support security operations and management reviews.
- Maintained incident-response playbooks, investigation procedures, technical runbooks, and SOPs to improve SOC consistency and response readiness.

SOC Analyst L1 Jul 2022 – Mar 2023

- Monitored Splunk, Microsoft Sentinel, Microsoft Defender, IDS/IPS, Windows Security Events, and network telemetry to detect and triage enterprise security incidents.
- Triaged malware, phishing, suspicious authentication, unauthorized access, endpoint, and network alerts to determine severity and escalate validated threats for investigation.
- Analyzed Windows, Active Directory, endpoint, DNS, VPN, firewall, and network logs to identify suspicious activity and indicators of compromise.
- Investigated Microsoft Defender endpoint alerts by reviewing process execution, user activity, authentication events, and network connections to validate potential threats.
- Investigated phishing emails, malicious URLs, suspicious attachments, and credential-harvesting attempts to identify threats and support timely containment.
- Correlated SIEM alerts with endpoint, identity, authentication, DNS, and network telemetry to provide actionable context for advanced security investigations.
- Escalated confirmed incidents with technical evidence, affected assets, severity, IOCs, and investigation findings to improve L1-to-L2 response continuity.
- Validated endpoint patches, software updates, and security configuration changes to support vulnerability remediation and secure workstation operations.
- Collaborated with Infrastructure, Networking, IAM, Help Desk, and Security teams to investigate and remediate enterprise security incidents.
- Documented alert analysis, investigation findings, escalation decisions, remediation actions, and supporting evidence to maintain accurate security records.

EMTECH Solutions Pvt Ltd (Client: IISC Bangalore) Pune, India

IT Systems Administrator Nov 2019 – Dec 2020

- Administered Windows Server, Windows 10/11, Active Directory, Group Policy, Microsoft 365, DNS, DHCP, VPN, and enterprise endpoints to maintain secure and reliable IT infrastructure.
- Managed Active Directory accounts, security groups, access permissions, password policies, and authentication controls to enforce secure access to enterprise resources.

- Monitored Microsoft Defender, Windows Security Events, endpoint health, and authentication activity to identify security and operational issues requiring corrective action.
- Applied operating-system patches, application updates, endpoint security configurations, and system-hardening controls to reduce exposure to known vulnerabilities.
- Analyzed TCP/IP, DNS, DHCP, VPN, firewall, and network-connectivity issues to identify root causes and maintain reliable enterprise communications.
- Diagnosed Windows, Microsoft 365, Active Directory, application, hardware, software, and network incidents to minimize user downtime and maintain business operations.
- Installed, configured, upgraded, and maintained enterprise applications, endpoints, security tools, and Windows systems to support reliable and secure infrastructure.
- Validated patches, security configuration changes, and remediation activities to confirm stable and secure system operation.
- Collaborated with Infrastructure, Networking, Security, Help Desk, Application, and vendor teams to troubleshoot escalated technical and security issues.
- Maintained technical documentation, configuration records, troubleshooting guides, knowledge base articles, security procedures, and SOPs to improve operational consistency.

Education

University of Central Missouri — USA
Master of Science in Cyber Security and Information Assurance — Dec 2025

KKR& KSR Institute of Technology and Sciences — India
Bachelor of Technology in Electronics and Communication Engineering — Apr 2023

Certifications

- CompTIA Security+ (SY0-701)
- Cisco Certified Network Associate (CCNA)
- Palo Alto Networks Cybersecurity Professional Certificate
- Google Cybersecurity Professional Certificate (GCPC)
- CompTIA A+
- Certified Cybersecurity Educator Professional (CCEP)