

**JENIFER PRINCY RAJA**

📍 Chennai, India – 600069

☎ +91 9962475618 | ✉ jeniferprincy25@gmail.com

---

**Professional Summary**

Cybersecurity professional with over **11 years of hands-on experience** in managing Security Operations Centers (SOC), **implementing SIEM/EDR solutions**, and designing scalable threat detection use cases. Specialized in **Google Chronicle SIEM, YARA-L-based detection engineering**, and **automation using Chronicle SOAR**. Demonstrated success in onboarding complex log sources, developing enterprise-grade detection content, and aligning use cases with **MITRE ATT&CK** framework. Recognized for improving threat visibility, reducing false positives, and proactively identifying advanced persistent threats (APTs) through **retrospective threat hunts and IOC correlation**. Strong communicator with experience supporting both technical and executive stakeholders across global cybersecurity environments.

---

**Core Competencies**

<b>SIEM Platforms</b>	<b>Google Chronicle, Custom SIEM Solutions</b>
<b>EDR Tools</b>	CrowdStrike Falcon
<b>Detection Engineering</b>	YARA-L Rule Development, UDM Field Mapping, Alert Tuning
<b>Incident Response</b>	SOC Monitoring, Triage,
<b>Threat Frameworks</b>	MITRE ATT&CK, OWASP Top 10
<b>SOAR &amp; Automation</b>	Chronicle SOAR – Playbooks, Enrichment, Escalation
<b>Threat Intelligence</b>	IOC Mapping, Retrohunt, External Feed Integration
<b>Log Integration</b>	Syslog, API, Agent, FTP, DB, File-based Onboarding
<b>Cloud Security</b>	AWS, Azure – CloudTrail, VPC Flow, Collector Deployment
<b>Compliance &amp; Risk Management</b>	ISO 27001, Security Policy Enforcement, Audit Support

---

**Professional Experience**

**Accenture Solutions Pvt Ltd – Chennai, India**

**Security Delivery Specialist | May 2020 – Present**

**Project Focus:** Google Chronicle SIEM Implementation, Threat Detection Engineering, SOAR Automation, IOC Threat Hunting

- **Google Chronicle SIEM Implementation:**  
Successfully led the migration of over **50+ enterprise clients** from legacy SIEM platforms to

**Google Chronicle** by architecting log ingestion pipelines using **Chronicle Forwarder** and **cloud-to-cloud APIs**. Ensured accurate field normalization, compliance with UDM schema, and uninterrupted data ingestion from varied sources including firewalls, proxies, DNS, EDR, VPC flow logs, and IAM services.

- **Detection Rule Engineering using YARA-L:**  
Authored and maintained advanced **YARA-L rules** to detect attacker behaviour across the kill chain—ranging from initial access and credential abuse to privilege escalation and exfiltration. Mapped detection content directly to **MITRE ATT&CK TTPs**, improving detection maturity and providing clear mapping for threat correlation and reporting.
- **Retrohunt & IOC Validation:**  
Conducted proactive **retrohunt operations** by searching historical UDM logs using IOCs derived from internal threat intelligence, public advisories, and Mandiant feeds. Identified stealthy attacker activity and ensured appropriate alerts and SOAR playbooks were in place to catch similar events in real time.
- **SOAR Integration & Workflow Automation:**  
Developed and optimized **Chronicle SOAR playbooks** to automate key tasks like IOC enrichment (e.g., VirusTotal lookups), case escalation, analyst task assignments, and ticketing integrations. Reduced **mean time to respond (MTTR)** by over 40% and significantly lowered operational overhead.
- **Detection Optimization & False Positive Reduction:**  
Collaborated with L2/L3 analysts to review alert quality and fine-tune rule logic. Modified thresholds, filter criteria, and pipeline mappings to reduce noise without sacrificing detection fidelity.
- **Stakeholder Engagement & Training:**  
Provided Chronicle operational training to internal SOC teams and client-side analysts. Created and maintained a **detection use case library**, playbook documentation, and Chronicle deployment guides.

---

## Symantec Corporation – Chennai, India

Security Engineer | Feb 2014 – Apr 2020

**Project Focus:** SOC Monitoring, Log Onboarding, Infrastructure Management, Parsing & Enrichment

- **SOC Monitoring & Real-Time Security Operations:**  
Operated in a 24x7 Global SOC supporting clients across regions. Monitored telemetry from network security appliances, EDR agents, and perimeter defense tools. Responded to high-priority security alerts, led triage, and escalated validated incidents for containment and remediation.
- **Infrastructure & Log Collector Deployment:**  
Deployed and managed **log collection infrastructure** in **Azure, AWS, VMware**, and on-premises. Integrated logs via **Syslog, DB connectors, REST APIs, FTP**, and **agent-based collectors**, ensuring data health and reliability.

- **SIEM Parsing & Alert Optimization:**  
Identified and resolved field mapping issues and parsing gaps in proprietary SIEM systems. Customized data parsers to ensure alerts fired with appropriate context, reducing false positives and alert fatigue for SOC analysts.
  - **Client Support & Vendor Coordination:**  
Acted as a liaison between internal teams, clients, and vendors (Cisco, Sourcefire) for resolving device-specific bugs, configuration errors, and logging issues. Ensured SLA compliance and timely client communication.
  - **Process Improvement & Automation:**  
Developed internal scripts and onboarding documentation to streamline log source integration. Reduced manual effort by automating health checks and device validation routines.
- 

## **Education**

### **Bachelor of Technology (B.Tech) – Information Technology**

Apollo Engineering College, Chennai – 2013

---

## **Declaration**

I hereby declare that the information presented above is accurate and complete to the best of my knowledge.

**(Jenifer Princy Raja)**