Tanya Priya

tanya.priya.blue@gmail.com | in/tanyapriyaofficial | github.com/tanya-priya | tanya-priya.github.io

Skills

Security Operations: Wazuh, Sysmon, Linux Auditd, Suricata IDS, PLG Stack (Promtail, Loki, Grafana), Log Pipeline Monitoring.
Detection Engineering: Sigma Rule Authoring & Transpilation, YARA, Wazuh XML Rules, LogQL, KQL.
Threat Hunting & Analysis: MITRE ATT&CK Mapping, Atomic Red Team, Hypothesis-Driven Hunting, Process Tree Reconstruction.
Technical Foundations: Python, Bash, SQL; Mathematical Analysis (Statistical Reasoning, Pattern Recognition, Logic).
Operational Strengths: Incident Documentation, Investigative Thinking, Collaborative Triage, Technical Communication, Decision-Making Under Uncertainty.

Projects

Hunt-Forge: Behavioral Detection & Adversary Emulation Lab April 2026

- **Objective:** Designed a blue-team lab to demonstrate the full attack lifecycle, from emulation to automated detection and manual hunting.
- **Actions:** Simulated post-compromise behaviors including PowerShell download cradles (T1059.001) and LSASS credential dumping (T1003.001) using Atomic Red Team.
- **Impact:** Detected "Living off the Land" (LotL) patterns by reconstructing process execution chains (cmd.exe → powershell.exe → rundll32.exe) and engineered a custom Sigma rule (win-rundll32-comsvcs-minidump.yml) to alert on suspicious memory dumps.

Wazuh-EDR: End-to-End Incident Response & Forensic Lab March 2026

- **Objective:** Orchestrated a multi-stage attack scenario to validate the SIEM detection pipeline and incident reconstruction capabilities.
- **Actions:** Executed SSH brute-force attempts and privilege escalation via sudo, correlating telemetry from auth.log and auditd.
- **Impact:** Engineered a custom ingestion pipeline by modifying the ‘¡localfile¿‘ block in ‘ossec.conf‘, enabling real-time visibility into kernel-level auditing and unauthorized file access events within the Wazuh Dashboard.

Sigma-Unified: Cross-Platform Detection-as-Code Pipeline March 2026

- **Objective:** Standardized security logic across Windows and Linux environments using a consistent Sigma-based schema to reduce alert fatigue.
- **Actions:** Transpiled platform-agnostic Sigma rules into production-ready Wazuh XML detections and validated triggers using ‘wazuh-logtest‘.
- **Impact:** Developed automated workflows for detecting Scheduled Task persistence (T1053.005) and Sudo privilege abuse (T1548.003) across diverse operating systems.

PLG-Stack: Observability-Driven Security Monitoring March 2026

- **Objective:** Implemented a lightweight centralized log management pipeline for real-time security monitoring and SOC visibility.
- **Actions:** Developed a SOC workflow using LogQL to filter and alert on Linux authentication failures and applied Promtail labels for efficient log indexing.
- **Impact:** Designed customized Grafana dashboards to visualize attack frequency and sources, significantly reducing the time to identify credential-guessing attempts.

Certification and Education

Google Cybersecurity Professional Certificate Coursera
Credential: *View Credly Badge* *February 2026*

Bachelor of Science in Mathematics Patna, Bihar, India
J.D. Women's College | Patliputra University *2022 – 2025*