ARUNATHISH R V

Nagercoil, Tamil Nadu, India | +91 REDACTED | arunrishi.zxc@gmail.com

linkedin.com/in/arunathish | github.com/Arunathish | portfolio: arunathish.github.io

PROFESSIONAL SUMMARY

Cybersecurity Analyst with 3+ years of dedicated cybersecurity learning and hands-on practice across SOC investigations, threat hunting, malware analysis, incident response, and SIEM-based detection. Skilled in analyzing Windows and Linux telemetry, investigating and enriching IOCs, correlating security events, and mapping adversary behavior to the MITRE ATT&CK framework using Splunk, Wazuh, ELK Stack, and Suricata. Experienced in phishing investigations, Windows forensics, network traffic analysis, and threat intelligence, with additional exposure to penetration testing and adversary techniques. Focused on turning security telemetry into actionable intelligence, improving detection, and supporting effective incident response.

CORE SKILLS

SIEM & Detection: Splunk, Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana), Suricata IDS, EDR

Threat Detection & Incident Response: Security Monitoring, Alert Triage, Threat Hunting, Log Correlation, IOC Investigation, Timeline Reconstruction, Malware Analysis, Phishing Investigation, MITRE ATT&CK Mapping, Detection Tuning, Case Management

Windows & Endpoint: Windows Event Logs, Sysmon, Process Monitor, Process Explorer, Registry Analysis, Scheduled Tasks, Services, Process Tree Analysis

Networking: TCP/IP, DNS, HTTP/HTTPS, SMB, Kerberos, Wireshark, Network Traffic Analysis

Identity & Authentication: Active Directory, Kerberos & NTLM Authentication, Group Policy, Authentication Log Analysis

Scripting & Querying: Python, PowerShell, SQL, OSQuery

Threat Intelligence: VirusTotal, URLScan, IOC Enrichment

Operating Systems: Windows, Windows Server, Ubuntu, Debian, Kali Linux

WORK EXPERIENCE

Network Support Engineer Intern *Mar 2025 – May 2025*

Amrita Vishwa Vidyapeetham — Nagercoil

- Configured VLAN segmentation and ACL policies across enterprise network infrastructure to improve network isolation and security.
- Diagnosed DNS, IP addressing, routing, and connectivity issues in production environments using protocol-level troubleshooting.
- Maintained network configurations and access control documentation, supporting operational stability and audit readiness.
- Gained hands-on experience with enterprise network architecture, authentication workflows, and Windows-based environments relevant to SOC investigations.

PROJECTS

Detecting Cyber Threats Using IPS/IDS Honeypot with Distributed Log Management *2024 – 2025*

Final Year Project, Amrita College of Engineering

- Designed and deployed a centralized security monitoring platform integrating Cowrie Honeypot, Suricata IDS, Wazuh SIEM, Elasticsearch, Logstash, and Kibana.
- Simulated SSH brute-force attacks, reconnaissance activity, and malicious login attempts to generate realistic security telemetry.
- Tuned Suricata detection rules, reducing recurring false positives during simulated attack scenarios.
- Correlated Windows Event IDs (4624, 4625, 4672, 4688, 7045) to reconstruct attack timelines and identify attacker behavior.
- Built Kibana dashboards visualizing authentication events, brute-force activity, and privilege escalation, and produced structured incident reports with IOCs, MITRE ATT&CK mappings, and remediation recommendations.

Active Directory Lab & Identity Control *2025*

Self-Directed Lab

- Built a lab-based Domain Controller and integrated Windows clients for authentication testing.
- Configured users, groups, and basic Group Policy Objects for access enforcement.
- Analyzed authentication logs to detect abnormal login patterns and privilege usage.

SOC Operations Simulation — Threat Hunting, Phishing & Malware Analysis, Windows Forensics *2025 – 2026*

Hack The Box Academy, LetsDefend, TCM Security, TryHackMe

- Performed security monitoring and alert triage across endpoint, authentication, and network telemetry by following SOC investigation playbooks and case management workflows in realistic SOC scenarios.
- Investigated phishing attacks by analyzing email headers, URLs, attachments, hashes, and domains using VirusTotal and URLScan.
- Conducted static and dynamic malware analysis to identify persistence mechanisms, command-and-control activity, behavioral anomalies, and indicators of compromise (IOCs).
- Performed Windows forensic investigations using Event Viewer, Sysmon, Process Monitor, Process Explorer, Registry artifacts, Scheduled Tasks, and Services.
- Correlated endpoint telemetry, Windows logs, and network events to reconstruct attack timelines and determine incident scope.
- Applied MITRE ATT&CK techniques to classify adversary behavior and documented investigative findings, response actions, and remediation recommendations in structured case reports.
- Validated alerts and identified recurring false positives across simulated SOC scenarios, recommending improvements to detection logic.

SOC Investigation Portfolio (HTB Sherlocks • LetsDefend • Malware Analysis) - github.com/Arunathish/investigations

- Authored structured incident reports covering phishing, malware, Windows forensics, and threat hunting.
- Documented attack timelines, IOC enrichment, MITRE ATT&CK mappings, and remediation recommendations.
- Investigated realistic SOC alerts from HTB Sherlocks and LetsDefend using SIEM workflows and endpoint telemetry.
- Published reports and supporting evidence in a public portfolio and GitHub repository.

SECURITY RESEARCH & RESPONSIBLE DISCLOSURE

Responsible Disclosure — Institutional Web Infrastructure *Feb 2026*

- Identified and responsibly disclosed multiple web infrastructure misconfigurations, including exposed Git repositories, directory listings, unauthenticated JSON endpoints, and publicly indexed sensitive documents.
- Demonstrated a realistic attack path by chaining reconnaissance, information disclosure, and credential exposure findings.
- Mapped identified techniques to the MITRE ATT&CK framework.
- Delivered structured remediation recommendations and received formal institutional acknowledgment for the responsible disclosure.

CERTIFICATIONS & PROFESSIONAL TRAINING

TCM Security

- SOC 101 – Security Operations Center Fundamentals
- SOC 201 – Intermediate Security Operations & Incident Response
- Windows Forensics
- Practical Malware Analysis & Triage

Hack The Box Academy

- Penetration Tester Job Path

LetsDefend

- SOC Analyst Learning Path

TryHackMe

- Blue Team Labs

EDUCATION

Bachelor of Engineering — Computer Science *2021 – 2025*

Amrita College of Engineering, Nagercoil, Tamil Nadu