E: adrian@tancomedia.com

P: +49 (173) 6955013

A: Pforzheim, Germany

LinkedIn:

https://www.linkedin.com/in/itsadriantan/

Portfolio:

https://adriantanasse.github.io/

Github:

https://github.com/adriantanasse/SOC-Portfolio/

CERTIFICATIONS

CompTIA | Security+ | Certification

Pearson | Certified Ethical Hacker (CEH)

Cisco | Network Support & Security

Google | Cybersecurity Certificate

TECHNICAL SKILLS

SIEM & Monitoring: Splunk, Wazuh

Network Analysis: Wireshark, PCAP Analysis, tcpdump, and more

Security Tools: Suricata, Sysmon, Auditd, Hydra, Nmap, and more

Scripting: Bash, Python

OS: Linux, Windows, MacOS

Programming: HTML, JavaScript, PHP, SQL

Frameworks: NIST CSF, MITRE ATT&CK

Others: Azure Cloud

SOC SKILLS

- Alert triage and prioritization
- Log analysis and event correlation
- Network traffic investigation
- IOC identification and analysis
- Detection rule creation and tuning
- Incident investigation and reporting

LANGUAGES

- English (Fluent)
- German (Intermediate)

ADRIAN TANASE

Cybersecurity Professional | SOC Analyst

SUMMARY

Aspiring SOC Analyst with hands-on experience building and operating SOC labs using Splunk and Wazuh SIEM platforms. Experienced in simulating and investigating realistic attack scenarios including phishing, SSH brute-force attacks, malware infections, and network-based threats, with a focus on log analysis, alert triage, threat detection, and incident investigation.

Passionate about understanding attacker behavior, developing detection logic, and improving visibility through behavioral and correlation-based detection techniques rather than relying solely on signatures. Currently seeking an opportunity to contribute to a SOC or Blue Team environment while continuing to grow in threat detection, incident response, and security operations.

PROJECTS

SOC Incident Labs | Detection & Response (GitHub Link)
(SIEM Splunk/Wazuh)

- Built and investigated multiple SOC scenarios including SSH brute-force, DDoS traffic flood, and phishing attacks, using custom detection rules, alert correlation, and automated response actions

Malware PCAP Analysis | Threat Investigation (GitHub Link)
(Wireshark + tcpdump)

- Analyzed real-world malware traffic (IcedID, NetSupport RAT, STRRAT) to identify C2 communication, extract IOCs, and confirm infections through network behavior analysis

EXPERIENCE

Founder & Digital Marketing Consultant — TancoMedia LLC
2016 – Present

- Monitored website and server performance, identifying traffic anomalies and irregular behavior
- Investigated issues using a structured, data-driven approach and root cause analysis
- Worked with real-time dashboards, responding to abnormal activity in time-sensitive environments
- Produced clear reports and managed multiple parallel tasks efficiently

Freelance Web Developer
2013 – Present

- Developed web applications using HTML, JavaScript, PHP, MySQL, and Python
- Built backend functionality handling HTTP requests and data processing
- Created scripts and automation to improve workflows
- Troubleshot and optimized applications; applied web knowledge to security projects