# TAMEEN KASSEM

Toronto, Canada • tameenyt@gmail.com • + 1 (647) 325-9717 • LinkedIn

Blue team security analyst with 3+ years in SOC operations, incident response, SIEM analysis, and cloud security. Experienced with Splunk, Wazuh, Wireshark, and SOAR automation. BTL1 Gold | Security+ | Google ACE | Top 800 HackTheBox globally.

## PROFESSIONAL EXPERIENCE

**THEIA INVESTMENTS** **Dubai, UAE**
**Independent Vulnerability Assessment - Freelance Security Consulting** **January 2026 - April 2026**

- Performed vulnerability assessment for a 'Multi-Family' wealth management business, identifying 2 critical and 2 High severity findings across network and web application attack surfaces using WPScan, Nmap, OpenVAS, and Burp Suite.. Delivered a formal penetration testing report with prioritized remediation recommendations.
- Identified critical WordPress vulnerabilities including an exposed XML-RPC endpoint, unauthenticated user enumeration, and absent brute force protections through manual testing and passive reconnaissance techniques.
- Conducted manual review of collaboration tools and file shares, assessing permissions, data exposure and sharing configurations. No critical findings identified, confirming appropriate access controls were in place.
- Conducted structured retest following client remediation, verifying implemented fixes against original findings and providing formal sign off on confirmed resolutions.
-

**ALO** **Dubai, UAE**
**Security Operations & Automation Engineer** **February 2025 - December 2025**

- Designed a reusable SOC reference architecture for a small business using Windows 10 endpoints, Wazuh Manager, Shuffle SOAR, and TheHive on Vultr cloud VMs.
- Configured Wazuh agents and detection rules to centralize endpoint telemetry, generate alerts, and trigger active responses to suspicious behaviour.
- Developed SOAR playbooks in Shuffle to automatically enrich IOCs with OSINT sources and open structured cases in TheHive with mapped observables, severity, and triage tasks.
- Used TheHive as the central case management system, enabling consistent incident workflows, documentation, and audit trails.
- Automated email alerting and response instructions, reducing manual triage effort and demonstrating how small teams can scale their incident handling with automation.

**PARTYSOCIAL** **Dubai, UAE**
**Network Solutions Consultant** **October 2024 - February 2025**

- Connected multiple networks, allowing devices to communicate across them efficiently.
- Designed a Layer 2 Wi-Fi bridging solution, and implemented Access Points (AP) to bridge the networks.
- Manually assigned static IPs to key devices, and tested to ensure efficient communication.
- Reduced Wi-Fi latency by ~50% by optimizing Layer 2 bridging and wireless settings based on latency tests.
- Implemented email protection for phishing on Google Workspace.
- Created SPF, DKIM and DMARC records, adding them to the DNS to prevent email spoofing.
- Performed incident response and remediation, quarantining a system following an email-based attack.
- Performed analysis using DeepBlueCLI and Windows Event Viewer on a compromised system.
- Used hashing tools via PowerShell and CMD to generate file hashes to cross-reference with OSINT tools.

**LOG IMPACTFUL TECH SOLUTIONS** **Lisbon, Portugal**
**Cyber Security Analyst** **June 2024 - August 2024**

- Learned and utilized GVM and OpenVAS, a network security scanner, to configure and deploy a vulnerability scanner, which was used to perform reconnaissance and assess exposure via specific ports and hosts on the target network.
- Disabled unused ports and services and eliminated false reports to address vulnerabilities in the network.
- Developed a virtual machine (VM) with a pre-configured vulnerability scanner for company-wide use.
- Wrote official documentation to conduct system scanning, standardizing deployment and ensuring operational efficiency.

**INVISIBLE MEANING** **Lisbon, Portugal**
**Network Security Analyst** **May 2023 - May 2024**

- Conducted phishing analysis using OSINT tools (URL2PNG, VirusTotal, domain analysis) to verify email authenticity.
- Reduced phishing email delivery by 30% through email quarantining, email filtering and sender blocking.
- Investigated suspicious attachments in sandboxed VMs, identifying malicious executables via Autopsy.
- Analyzed PCAP logs in Wireshark, isolating malicious traffic and attack patterns.
- Used Splunk to detect anomalies, visualize security threats, and analyze persistence mechanisms in compromised systems.
- Recommended remediation steps to address varying levels of security incidents.

**MACDONALD SAGER MANIS LLC** **Toronto, Canada**
**Law Firm Summer Internship** **2018 and 2019**

## CERTIFICATIONS

**SECURITY BLUE TEAM** **February 2025**
***Blue Team Level 1 Junior Defensive Cybersecurity Certification*** | **Gold Coin Recipient**

**GOOGLE CLOUD PROFESSIONAL** **November 2024**
***Associate Cloud Engineer Certification***

**COMPTIA** **February 2024**
***Security+ (Plus) Certification***

## EDUCATION

**UNIVERSITY OF TORONTO; School of Continuing Studies, *Cybersecurity Program*** **February - August 2023**

**UNIVERSITY OF TORONTO; *Honours B.A Major in Criminology, Major in Sociology*** **2017-2022**

## PROJECTS

**SOC AUTOMATION & INCIDENT RESPONSE PIPELINE**
*Personal Home Lab* - ***Security Operations / Automation Project*** **November - December 2025**

- Designed a self-hosted SOC pipeline on Vultr: Windows 10 endpoints → Wazuh Manager → Shuffle SOAR → TheHive.
- Developed and tuned Wazuh agents to collect security events from multiple PCs, apply detection rules, and trigger active response actions on monitored hosts.
- Built Shuffle workflows that fork Wazuh alerts into parallel branches for IOC enrichment using OSINT sources, and automatic case creation in TheHive with mapped observables, severity, tags and task templates.
- Integrated TheHive as the incident response platform to centralize alerts, track investigations, and coordinate analyst workflows.
- Implemented automated email notifications and response guidance, demonstrating end-to-end SOC automation from detection through enrichment to case management and response.

**INFRASTRUCTURE AS CODE (IaC) - Secure 3-Tier app**
***Cloud Security Project*** **July 2025**

- Provisioned a secure 3-tier web application in AWS using Terraform (network, application and database tiers).
- Implemented least-privilege IAM roles, NSGs, and network segmentation.
- Enforced data security with encrypted S3 buckets, RDS encryption at rest, and TLS in transit.
- Added compliance checks with tools to scan code for misconfiguration before deployment.
- Demonstrated secure infrastructure automation aligned with cloud security best practices.
-

**SECURE CI/CD PIPELINE**
***DevSecOps Project*** **June 2025**

- Built an automated CI/CD pipeline for a containerized FastAPI app using GitHub Actions and Docker.
- Integrated security automation: CodeQL for SAST and Trivy for dependency and image scanning.
- Enforced test coverage thresholds and blocked deployments on high-severity vulnerabilities or failing checks.
- Deployed to staging and production on Cloud Run using OIDC-based authentication to avoid long-lived service keys.

**HACKTHEBOX LABS**
***Cybersecurity Practitioner*** **February 2024 - Present**

- Ranked in the top 800 globally on HackTheBox in one season by solving hands-on labs in vulnerability assessment, cryptography, reverse engineering, and forensic analysis.
- Completed 20+ end-to-end penetration test simulations in controlled lab environments, identifying issues such as SQL injection, XSS, insecure deserialization, and buffer overflows.
- Performed network and web reconnaissance using tools like Nmap and Burp Suite, then validated findings with proof-of-concept exploits and documented remediation/hardening steps.
- Wrote PowerShell and Bash scripts to automate enumeration, simulate reverse shells and persistence, and test corresponding detection and response approaches.

## TECHNICAL SKILLS

- **SIEM & Detection:** Splunk, Wazuh, DeepBlueCLI, Windows Event Viewer
- **Incident Response & Forensics:** TheHive, Autopsy, FTK Imager, Volatility, CyberChef, Scalpel, KAPE, PECMD, ProcDump
- **Network & Penetration Testing:** Wireshark, Burp Suite, Nmap, Metasploit, PowerShell, Bash
- **Cloud & DevSecOps:** AWS, GCP, Terraform, Docker, Kubernetes, GitHub Actions, Trivy, Checkov, Grafana

- **OSINT & Threat Intelligence:** VirusTotal, URL2PNG, WannaBrowser, MITRE ATT&CK