

Asim G.

Cyber Security Consultant / Cyber Threat Analyst

TechHive
IT's simple with us

Professional summary

A security engineer with 10+ years of expertise in the cyber security domain. Skilled in various roles including Incident Response Commander, Penetration Tester, Threat Hunter. Proficient in building and managing vulnerability management systems, with a successful track record of deploying CortexXDR from scratch and integrating it with multiple data sources for enhanced data enrichment. Conducts penetration tests when uncertainties arise regarding vulnerabilities or to showcase potential server attacks. Responsible for quarterly ASV scans, PSI DSS standards, and external vulnerability management. Additionally, serves as a key member of the internal incident response team for severe incidents. Specializes in physical security assessments and information gathering without relying on technical tools, achieving remarkable success in previous professional experiences.

Education	Azerbaijan State Oil and Industry University, Bachelor's degree in Information Technology and System Engineering Warsaw School of Computer Science, Master's degree in IT Project Management
Certificates, Licenses and Trainings	System Operations on AWS OWASP-TOP10 CCNA 200-125 Practical DevSecOps Professional Certified Threat Hunting Professional Preparing for Practical Network Penetration Tester (TCM Security) ISC2 Certified Cyber Security CompTIA Security Analyst CySA |CSAP Certified Fortinet Network Security | NSE1 and NSE2 CompTIA Security Symantec Certified Specialist Symantec Security Awareness Advocate

Skills

- Python
- Application Security Tools: Cortex XDR, Nessus, InsightVM, Rapid7, Intruder, Mandiant
- Endpoint Security Tools: CrowdStrike
- Cloud Security Tools: AWS container environments, PrismaCloud
- Content Filtering and Compliance Standards: Content control filtering, OWASP TOP-10, NIST
- Web Application Security Tools: BurpSuitePro, OWASPZAP
- FTK (Forensic Toolkit)
- Network Security Tools: NMAP
- Proxy and Web Security Products: Bluecoat Products, Web Security Services, ProxySG, ProxyASG
- Authentication and Authorization Protocols: SAML, Kerberos, NTLM
- Log Analysis and Monitoring Tools: Splunk, Wireshark, Fiddler, Grafana
- Email Security Technologies: SMTP, SMTP over TLS, Antispam, Antivirus, SPF, DMARC, DKIM
- Google Hacking

- Cyber Threat Intelligence (CTI)
- Cyber Threat Hunting (CTH)
- Cyber Security Assessment
- Threat and Vulnerability Management
- Threat Analysis
- Incident Management
- Web Application Security
- Web Application Firewall
- Vulnerability Assessment
- Penetration testing

Company	UK Fashion Retailer (NDA)
Period	Sep 2023 – till now
Role	Cyber Security Engineer
Technologies	AWS, Security Design, Defence in Depth Approach, Incident Response, Threat Intelligence, Vulnerability Management, Security Awareness, MDM, SOC, CrowdStrike EDR, Intruder IO, AppCheck, OWASP

Responsibilities

- Responded to and resolved security incidents raised by the MDM and SOC monitoring provider;
- Initiated deployment of CrowdStrike EDR, handling configuration, tuning, and integration with multiple enterprise solutions from the ground up;
- Replaced the DAST solution AppCheck with Intruder IO, improving performance, scan quality, detection rates, and usability through a more user-friendly portal;
- Proposed the implementation of a DevSecOps process to strengthen security integration within development and operations workflows;
- Migrated external vulnerability scanning tools (web application and network) to more effective technologies, enhancing detection and coverage;
- Led replacement of the legacy antivirus solution with an advanced Endpoint Detection and Response (EDR) tool;
- Cleared accumulated security incidents from the portal and collaborated with the MDM provider to optimize incident reporting and improve data quality.

Company	**Pasha Bank**
	the leading corporate bank of Azerbaijan
Period	Apr 2020 – Sep 2023
Role	Cyber Security Analyst / Threat Hunter / Penetration Tester
Technologies	Cortex XDR, Nessus, InsightVM, Rapid7, Intruder, Mandiant, SocRadar, CrowdStrike, PrismaCloud, BurpSuitePro, AWS container environments, BurpSuitePro, NMAP, OWASPZAP, FTK (Forensic Toolkit)

Responsibilities

- Participated in internal penetration testing for critical vulnerabilities;
- Used Cortex XDR data lake and XQL queries to hunt for threats internally;
- Deployed Prisma Cloud on-premises and AWS container environments for configuration hardening and vulnerability patching;
- Researched Dark and Deep web threat actors targeting Azerbaijan and banking sector;
- Conducted threat modelling and recommended security improvements for architecture flaws;
- Ran PoCs of security products based on company needs and reported to executive management;
- Conducted web application penetration testing using BurpSuitePro, NMAP, OWASPZAP, and other tools;
- Deployed Cortex XDR, integrated with multiple tools, and tuned rules and policies;
- Administered and managed internal vulnerability management, assisted patch managers with reporting and remediation plans;
- Assisted in building processes for Vulnerability Management, Digital Forensics, Incident Response;
- Conducted digital forensic acquisition and preservation using FTK;
- Handled SOC level 2 incidents, isolation, response, and tuning for prevention of future attacks;
- Tuned and automated processes on various tools to reduce effort.

Company	**Symantec**
	Symantec Enterprise Cloud delivers data-centric hybrid security for the largest, most complex organizations in the world – on devices, in private data centres, and in the cloud
Period	Feb 2017 – Mar 2020
Role	Security Engineer
Technologies	Bluecoat Products, Web Security Services, ProxySG, ProxyASG, SAML, Kerberos, NTLM, CPL, Splunk, Wireshark, Fiddler, Grafana, HTTP, HTTPS, SMTP, SMTP over TLS, Antispam, Antivirus, SPF, DMARC, DKIM, Content control filtering, OWASP TOP-10, NIST, Google Hacking

Responsibilities

- Supported Products: Email Security, Bluecoat Products, Web Security Services, ProxySG, ProxyASG;
- Replicated customer incidents in the lab environment to fix them, including installation, deployment, integration, etc;
- Handled authentication using SAML, Kerberos, NTLM;
- Installed policies/rules with scripts using CPL (proprietary language for ProxySG);
- Worked with Splunk, Wireshark, Fiddler, and Grafana to analyse captured packets and identify errors;
- Diagnosed and resolved cases raised by customers of Symantec cloud services, including support for Web Security Services (HTTP, HTTPS, web content filtering, proxies) and Email Security Services (SMTP, SMTP over TLS, Antispam, Antivirus, SPF, DMARC, DKIM, content control filtering);
- Handled incoming customer contacts via emails, phone, customer portal, and chat sessions;
- Performed pentesting using OWASP TOP-10, NIST, and Google Hacking.

Company	Halal P Technology & Solution
Period	Feb 2016 – Jan 2017
Role	Network and System Administrator

Responsibilities

- Was responsible for network efficiency and maintenance;
- Created new accounts giving permission to specific groups and users files in Server;
- Set up and configured a new server in new branches and sales centres;
- Provided technical support to computer system users on reported issues and service requests;
- Troubleshot, supported, configured, and maintained PC hardware, printers, and PC peripherals;
- Assisted in installing new desktop systems for new employees.