Samuel Turney

206-377-9828 | samturney24@gmail.com | linkedin.com/in/samuel-turney | github.com/sam-turney

Experience

Threat Hunter & Red Teamer Jul. 2024 – Present

DataQuest on Contract to Rite Aid Corp. *Remote, USA*

- Led proactive, hypothesis-driven threat hunts across 30,000+ enterprise endpoints and network environments using Rapid7 InsightIDR (SIEM) and Zeek/Bro (IDS) to uncover stealthy adversarial activity.
- Engineered a Python-based ingestion pipeline to automatically pull over 500 new OSINT-derived IoCs weekly from threat intelligence platforms (TIPs) and feed them into Zeek sensors, increasing emerging threat coverage by 35%.
- Simulated advanced persistent threat (APT) activity using Kali Linux and open-source adversary emulation frameworks, mimicking real-world tactics, techniques and procedures (TTPs) to validate detection logic.
- Authored 30+ ATT&CK-aligned detection rules and enriched telemetry using correlated data from threat feeds, endpoint events, and network metadata, reducing false positives by 22%.
- Partnered with security operations center (SOC) and incident response (IR) teams on 10+ major incidents to validate findings, reduce false positives, and translate hunt results into actionable detection logic.
- Integrated findings into ServiceNow, SIEM/SOAR playbooks, and threat models, reducing triage time by 25%.

Security Analyst June 2023 – June 2024

Western Washington University *Bellingham, WA*

- Automated enterprise vulnerability management by integrating Nessus, Bash scripting, and Splunk Enterprise, enabling real-time ingestion and distribution of scan results and reducing manual effort by ~15 hours per week.
- Triaged 5,000+ alerts with Microsoft Defender for Endpoint and Sentinel, resulting in zero breaches during tenure.
- Investigated and resolved hundreds of high-risk sign-ins and anomalous authentications in Azure Active Directory, strengthening account integrity and maintaining zero counts of unauthorized access.
- Secured 5+ Azure VMs through custom network security groups (NSGs) and identity and access management (IAM) policies, reducing unauthorized access attempts by 60%.
- Spearheaded a university-wide vulnerability response initiative that cut remediation time by 30%.
- Designed Splunk dashbaords that influenced $25,000+ in funding toward vulnerability scanning infrastructure.

Projects

Malware Zoo | *Malware Analysis, KVM, C, Docker, C2, OpenStack* Sep. 2023 – Jun. 2024

- Designed and deployed a sandboxed malware analysis environment using Debian Linux and Kernel-Based Virtual Machine (KVM), hosted on WWU Cyber Range's OpenStack environment.
- Reverse engineered malware samples to create safe versions in C for hands-on learning without risk of infection.
- Built Docker-based Command and Control (C2) servers to mimic real-world attacker infrastructure and behaviors.
- Developed interactive lessons and walkthroughs to teach malware detection, analysis, and removal techniques.
- Integrated tools for static and dynamic malware analysis utilities (e.g., Ghidra, Wireshark, etc.) into each VM.

Secured Cloud Environment | *Cloud Security, IAM, Firewall, VPC, Event Logging* Mar. 2024 - Jun. 2024

- Secured a multi-account AWS environment by implementing comprehensive security controls.
- Enforced principle of least-privilege IAM policies, reducing risk of unauthorized access by 80%.
- Architected VPCs with subnet segmentation, Access Control Lists (ACLs), and network security groups (NSGs).
- Implemented 20+ firewall rules and VPC peering to control east-west and north-south traffic securely.
- Enabled CloudTrail and AWS Config for full logging, auditing, and compliance monitoring across 100% of services.

Education

Western Washington University Bellingham, WA

Bachelor of Science in Computer Science *June 2024*

Certifications: CompTIA Security+, CompTIA Network+

Technical Skills

Languages: Python, Bash, PowerShell, C, C++, C#, Assembly (x86, x64), JavaScript, Java, SQL
Security: SIEM/SOAR, IDS/IPS, Vuln Scan/Mgmt, Atomic Red Team, IR, Reverse Engineer, Malware Analysis
Cloud & Infra: AWS, Azure, Docker, OpenStack, KVM, Terraform, TCP/IP, DNS, VPN, Routing
OS: Linux (Debian, Ubuntu, RHEL, CentOS, Kali), Windows Server & Workstation, macOS
Tools: Git, GitHub, Gitlab, CI/CD, Docker Compose, Kubernetes, TIPs, Regex, JSON/YAML