Tyler Boire

Email: tyler.boire@gmail.com
Website: https://tylerboire.github.io
GitHub: https://github.com/TylerBoire

Tyler is a seasoned security professional, that takes a multi-faceted approach to risk management by incorporating Offensive, Defensive and Policy knowledge to create holistic solutions for internal and external stakeholders.

Communication Skills:

- Consulting for businesses up to Fortune 50 space.
- Experience speaking to Security, Risk, and Financial stakeholders to drive policies that reduce exposure.
- Experience in interacting with technical and executive audiences.
- Provide written and verbal guidance on improving security posture.
- Written documentation and guidance on technical processes & policy.

Security Strategy:

- Defense-in-depth models
- Kill-chain analysis and interdiction.
- Firewall config review and best practices layer 4 and 7
- Network logging and alerting
- Least privileged models
- Knowledge of multiple firewall, IDS and IPS vendors
- Experience with multiple EDR, AV, and Network security products
- Experience with multiple compliance frameworks

Threat Intelligence:

- Strategic, Operational, and Tactical analysis of threats facing unique customers.
- Experience in tying Geo-political and non-cyber activities to cyber based threats.
- Briefing executives on risks to their specific organization and business vertical.

Offensive Security:

Network and Host recon:

- Port, Host and Service discovery
- Vulnerability identification
- OSINT and Confidential document discovery
- Password leak identifications

Exploitation:

- Use and modification of public exploits
- LLMNR & WPAD poisoning
- Kerberos and Service Principal Name abuse.
- Password Cracking using curated dictionaries and rule sets
- Phishing

Post exploitation:

- Shell persistence
- Credential harvesting
- Pivoting between network segments
- Power user identification/hunting
- Privilege escalation
- Identifying incident response and countermeasures
- Living off the land

DFIR:

- Static and Dynamic Malware Analysis
- Host, Network, and Memory forensics
- Familiar with *Nix triage
- IOC and Threat Intelligence aggregation
- Log analysis

Work Experience

March 2022 — Present

Sr Threat Intelligence Analyst at Resilience

- Define milestones for developing a robust Cyber Threat Intelligence Program
- Provide strategic business vertical intelligence to insureds.
- Oversee reporting on threats that may affect customer verticals.
- Assist in creating repeatable procedures for intelligence gathering and reporting.
- Guide staff level analysts in their day-to-day analysis.
- Iterative Research & Development improving products and services

June 2020 — February 2022

Targeted Attacks Analyst at Accenture CTI

- Tracked and report on APT style threat groups
- Cross team collaboration with Geopolitical, Malware, and Vulnerability analysts
- Weekly reporting on threats that may affect customer verticals
- Assisted in creating repeatable procedures for intelligence gathering and reporting
- Aided DFIR team with customer engagements
- Responded to customer requests for information.

January 2018 — June 2020

Penetration Tester at Verizon

- Provided customers with Internal, External and Wireless penetration tests
- Identified and reinforce good security practices deployed in customer networks
- Provided customers with detailed reports regarding their vulnerabilities
- Helped maintain infrastructure used in day to day operations
- Worked towards automating common tasks and procedures
- Designed and implement repeatable and reliable gold images for consultant laptops and VMs

June 2016 — January 2018

Threat Specialist at Palo Alto Networks

- False positive and false negative verdict determination
  - Sandbox dynamic analysis, URL categorization, C2 communication detection
- Coverage for emerging vulnerabilities and malware variants
- Triaged reports of perceived product vulnerabilities
- IPS signature development, improvement, and tuning
- Aided in identification and signatures for various malware families.
- Automated information gathering via internal REST APIs with Python
- Maintained internal replication lab

December 2015 — May 2016

Network Admin & Researcher at Leahy Center for Digital Investigation

- Maintained network functionality
- Oversaw junior admins and maintained critical infrastructure
- Performed vulnerability assessments and inventory tracking
- Improved documentation on existing procedures
- Researched forensic uses for JTAG/ChipOff techniques
- Provided consultation on Amazon Alexa research

June 2015 — April 2016

Incident Response Intern at Dell Secureworks

- Aided the Threat Intelligence department in analyzing a kill chain for Threat Group 3390
- Reported on threat assessments of hostile countries and capabilities based on OSINT
- Consolidated and reworked best practice and remediation suggestions.
- Reviewed SANS GCIH material with new hires prep for their test.

Dec 2012 — Nov 2016

Sr.Helpdesk/Helpdesk at Champlain College

Responsible for immediate response to classroom issues, directing other techs to complete tickets and long term projects.

Sept 2013 — May 2014

Teaching Assistant at Champlain College

Responsible for ensuring labs ran smoothly and working 1-on-1 with students who had questions during class.

Education

June 2018	Pen-testing with Kali
May 2016	Bachelor's degree in Computer Networking & Information Security, Champlain College Specialization in Cybersecurity & Minor in Digital Forensics
May 2012	College prep courses, Clinton Community College