Jason Lynch
email: jmlynch [@] gmail.com

Employment

Target Corporation

Lead Engineer, Threat Intel Detection Engineering

February 2018 - Present

- Pioneered the development and execution of process to track and collect on identified high priority threat actors.
- Developed standards and guidance for documenting, storing and tagging of collected intel & indicators of compromise.
- Analyzed externally/internally sourced intelligence and identified collection and detection opportunities for actor TTPs.
- Prioritized, researched, prototyped, created and deployed collection and detection content
  - Network and host based content to include SIEM, Suricata, Bro, Sysmon, Tanium and Yara based rules.
- Collaborated with strategic intel team to identify intel gaps and develop relationships within law enforcement organizations and private industry.
- Product Owner for platforms/services devloped in house by organization's CTI Tools team.
  - Championed new features and capabilities for multiple unique, internally developed CTI oriented products.
- Prototyped system that allows CTI analysts and engineers to track and be notified of subjects of interest related to collection responsibilities on VirusTotal and Twitter.

Vigilant Technology Solutions

Lead Detection Analyst

January 2017 - December 2017

- Responsible for establishing the vision, direction and execution of detection planning, engineering and development in support of hunt team operations.
- Led response team efforts for several customer compromises.
- Developed and delivered threat assessments and customer communication templates.
- Prototyped, built and deployed Threat Intel Platform to store collected intel and indicators of compromise.

Target Corporation

Lead Engineer, Threat Defense Operations

November 2014 - January 2017

- Designed, architected and deployed what is currently the largest known corporate Network Security Monitoring sensor grid.
- Developed custom detection content and other solutions that target adversary TTPs in the environment.
- Prototyped, built and deployed Threat Intel Platform to store collected intel and indicators of compromise.

Mandiant

Senior Engineer, Threat Analytics Platform

January 2014 – November 2014

- Assisted TAP customers with the planning and deployment of product in their environment.
- Hunted for threat group activity in customer environments using TAP product.
- Developed and deployed detection content

General Electric

Detection Architect

January 2012 - January 2014

- Designed, developed and deployed detection and response solutions.
  - Product planning, design/build/run of very large NSM sensor grid supporting detection and response operations of CSIRT.

Education

Xavier University. BA, Classical Humanities.

Technologies and Skillset

- DFIR Techniques: Static and dynamic analysis, memory forensics.
- DFIR Technologies: Bro/Zeek, Suricata, YARA, Volatility, ElasticSearch, Elastalert, Kibana, Sigma
- Programming: SaltStack, some Python

Membership in multiple intel sharing/collaboration groups