Josh Liburdi
email: liburdi.joshua@gmail.com

Employment

Target Corporation. Lead Engineer (Cyber Fusion Center). March 2017 - Present.

- Lead developer for Target's 1,800+ sensor network security monitoring (NSM) deployment
  - Developed dozens of custom Bro/Zeek scripts and Suricata rules, including detection of attacker tactics and logging new network metadata from HTTP, SMTP, and TLS
  - Developed framework for stable, high-volume file extraction (~400 files/second)
- Created Strelka, an open-source file analysis system built on Python 3.6, YARA, and 0MQ
  - Supports 60+ types of files, designed to scan hundreds of millions of files per day
- Contributed crucial discovery, design, and development work on a 9-month project to upgrade and re-engineer NSM platform to use Docker containers
  - Created data-driven testing procedures and led selection of system components
  - Developed methodology for balancing server resources via CPU pinning and isolation
- Designed and developed a secure, tool-agnostic packet capture (PCAP) retrieval system using gRPC that reduced PCAP retrieval time from minutes to seconds
- Developed continuous delivery systems for Suricata and YARA that reduced rule deployment time from days to minutes
- Collaborates across the team and technology organization to ensure end user needs are met through quality and availability of telemetry data

Sqrrl (acquired by Amazon). Security Technologist (Research). May 2016 - March 2017.

- Led research on attacker tactics that leverage DNS which fully defined a product release (Sqrrl v2.7) and increased customer-facing detection analytics by 50%
- Led endpoint research that focused on the effective use of process execution records
- Regularly created, tested, and validated new threat hunting hypotheses and techniques across endpoint, network, and file metadata
  - Significant focus on testing effectiveness of underutilized visualization techniques

CrowdStrike. Senior Consultant. June 2014 - April 2016.

- Performed threat hunting and incident response for Fortune 500 customers
- Lead researcher and developer for CrowdStrike Services' NSM platform
  - Boosted productivity of investigation and analysis by building a custom Splunk application that unified event data from four network detection tools
  - Created RDP analyzer for Bro/Zeek (included in open-source project)
- Created and taught two threat hunting training courses (one publicly taught at Black Hat)

General Electric. Analyst (Detection Operations, CIRT). May 2013 – June 2014.

- Actively contributed to the identification and eradication of adversaries as part of an intelligence-driven incident response team
- Developed methods of validating, enriching, and scaling tens of thousands of indicators of compromise (IOCs) across the enterprise

Education

Eastern Michigan University. Bachelor of Science, Information Assurance. April 2013.

Skills

- Programming/DevOps: Python, ZeroMQ/0MQ, gRPC, Go, Git, Docker, SaltStack, Drone
- Industry: Bro/Zeek, Suricata, YARA, Falcon Endpoint, osquery, Volatility, Splunk, Kibana

Community Contributions

Presentations

- "Beyond AV: Detection-Oriented File Analysis". BSides San Francisco, Mar. 2019.
- "Threat Hunting for Command and Control". Sqrrl webinar, Nov. 2016.
- "Beyond IDS: Practical Network Hunting". BSides New York, Jan. 2016.
- "Adversary Hunting and Incident Response: Network Edition". Black Hat EU, Nov. 2015.
- "Hunting Through RDP Data". BroCon 2015, Aug. 2015.
- "Analyzing RDP Traffic with Bro". Bro4Pros 2015, Feb. 2015.

Open-Source Projects

- Strelka (Target, Lead)
- Stenographer (Google, Contributor)
- Bro/Zeek (ICSI, Contributor)
- Laika BOSS (Lockheed Martin, Contributor)

Writing

- "Stenographer + gRPC". Medium, Jan. 2019.
- "Building Distributed, Scalable Python Apps". Medium, Jun. 2018.
- "Laika BOSS + Bro = LaikaBro (?!)". Medium, Feb. 2017.
- "THE HUNTER'S DEN: COMMAND AND CONTROL". Sqrrl blog, Feb. 2017.
- "Hunting for PowerShell Using Heatmaps". Medium, Jan. 2017.
- "THE HUNTER'S DEN: INTERNAL RECONNAISSANCE (PART 1)". Sqrrl blog, Nov. 2016.
- "Maximizing Network Threat Intel with Bro". CrowdStrike blog, Dec. 2014.