Christopher Schafer

12216 Dolomite Drive
Pineville, NC 28134

(818) 584-6705
chrisp.schafer@gmail.com
http://veryoblivio.us/

Skills/Experience

- Realtime Security Event Correlation (SIEM)
  - Provisioned, tuned, and maintained one of the most advanced and efficient ArcSight instances.
  - Strong understanding of the syslog standard
  - Presented at HP Protect 2015: A deep dive into advanced regex parsing. Received accolades and was invited to return in 2016.
- Linux
  - System Security
  - User Management
  - Heavy Linux user for 14 years
  - System Administration
- Routing and Switching
  - Experience with Cisco and Juniper
  - Earned the JNCIA in December 2013
- Dynamic Malware Analysis
  - Patent US9185128 for a method of repeatable automated malware analysis on physical systems.
  - Identifying behavior such as network traffic, file accesses, and persistence
  - Experience in a variety of related tools including Wireshark and CaptureBat
  - Experience with FireEye, LastLine, Cuckoo Sandbox, and other malware appliances
- Reverse Engineering
  - Comfortable in Radare 2
  - Basic skills using Binary Ninja
  - Used in CTF competitions at conferences and online
  - Built automated functions to do static reversing of obfuscation methods such as DOSfuscation
  - Comfortable using a variety of dynamic analysis engines

Work Experience

VP, Sys/Data Security, Bank of America - Malware Prevention - Research, Analysis, and Tooling Team
Charlotte, NC (June 2018 - Present)

- Built automation and tooling to improve team effeciency and efficacy.
- Built an automated system (backend and frontend) for automatically tracking and proactively blocking callbacks for documents distributed by Emotet.
- Rapidly designed and built data collection and correlation tools during incidents to assist with incident response.
- Helped design and automate metrics reported to senior leadership and the Bank of America board.

VP, Information Security Engineer, Bank of America - Real-time Security Event Correlation Team
Simi Valley, CA (June 2013 - June 2018)

- Integrated ArcSight with many products that do not have official ArcSight integration, without support from HP.
- Created accurate parsers for new data feeds within 24 hours when necessary during incidents to close a gap.
- Discovered undocumented features and tricks to accomplish goals which the vendor advertised were not possible.
- Integrated a significant number of program and application logs into ArcSight, building custom parsers and connectors.
- Designed and implemented new lab setups for repeatable physical malware analysis (US Patent US9185128).

Extracurricular Experience

Black Team, Western Region Collegiate Cyber Defense Competitions (2017-Present)

- Part of the team who built the environment for the competitors.
- Built a custom web application that worked as a dashboard for a black-box SCADA style device. The competitors were expected to secure.
- Built deployment and configuration scripts for the custom National CCDC Scoring system, Mantis Bug Tracker, and Apache Guacamole to do large scale competition deployments quickly.

Competitions and Awards

- LayerOne CTF (2016 - 2nd, 2017 - 5th)
- LayerOne DeObfuscation (2015 -2nd, 2016 - 1st)
- Boy Scouts (Eagle Scout - 2011, Vigil Honor - 2010)
- DEFCON Capture The Packet (Finalist)
- Western Region CCDC (2013 - 1st, 2014 - 2nd)
- National CCDC (2013 - 4th)