Brent Eskridge | PhD

Cybersecurity · Threat Intelligence · Data Analysis · Software Engineering

resume@brenteskridge.com www.brenteskridge.com

Skills Summary

Threat intelligence	Data analysis & visualization	Python, Bash, C/C++, R, SQL
Research & investigation	Technical storytelling	TryHackMe Top 0.5%
Machine learning & AI	Written & oral communication	Mentoring & teaching

Employment Experience Highlights

Threat Intelligence Analyst - IronNet 2021 - 2022

· Tracked both established and emerging APT actors and their TTPs using open source intelligence (OSINT). Monitored geopolitical developments to anticipate future threat actor actions and trends. Combined this information with data gathered through internal sensors to produce strategic, operational and tactical threat intelligence, including IoCs and TTPs mapped to MITRE ATT&CK. Areas of specialty included cybercrime, data analysis, and communicating technical concepts.

· Co-led internal briefings to peer and CXO level audiences and external briefings to customers. Participated in weekly CXO level planning sessions for threat intelligence updates sent to customer CEOs.

· Collaborated with proactive threat hunters to produce actionable intelligence from large data sets on threat actor command and control (C2) servers such as Cobalt Strike using ElasticSearch and Kibana.

· Collaborated with network threat hunters to: identify potential threats and attack vectors; track threat actor actions using PCAPs, netflow, and metadata; and create after action reports and articles.

· Led the creation of IronNet's first annual threat report with responsibilities that included: identifying and organizing content, analyzing data and creating visualizations, coordinating with graphic designers, and creating content. The report resulted in IronNet's largest media engagements to date.

· Authored articles and infographics discussing technical details of observed cyber attacks and high-level trends in cybersecurity. Topics covered included: Log4j, Cobalt Strike, and critical infrastructure. The articles were in the top 10 most read IronNet publications to date.

· Developed Python scripts to automate: the extraction, analysis, and visualization of threat intelligence; the import and export of research data between platforms; and the generation of weekly threat reports.

Professor & Dept. Chair, Dept. of CSNE - Southern Nazarene University 2004 - 2021

· Proposed, secured, and managed three interdisciplinary research projects that applied machine learning to biologically-inspired models of collective behavior. Projects had funding in excess of $380,000 and consisted of two National Science Foundation (NSF) research grants and a sabbatical at the Max Planck Department of Collective Behaviour in Konstanz, Germany.

· Led six research projects with responsibilities including: building collaborative teams; defining and managing scope; identifying and assessing potential techniques; managing and analyzing data; drawing insights and implications from results; and communicating and contextualizing findings.

· Designed, implemented, and maintained software for eight different research projects using concepts that included neural networks, reinforcement learning, fuzzy logic, autonomous agents, and multi-agent systems. Software used technologies such as Python, Java, R, Bash scripts, Ant, YAML, and GitHub.

· Designed, taught, and assessed over 20 different Computer Science courses covering topics that included: software development, operating system concepts, computer architecture, Linux, algorithms, data structures, database systems, network programming, and ethics in technology.

· Performed manual static and dynamic code analysis on student code to assist in debugging and ensure requirements compliance. Languages included Python, Java, C/C++, MIPS assembly, Bash, and SQL.

Software Engineer II - Raytheon Systems Company 1997 - 2000

· Designed and implemented a Solaris (Unix) TCP/IP network server, with a custom message format, and logging subsystem in C++ that communicated with programmable logic controller (PLC) machinery.

· Initiated, designed, and implemented a GUI tool in Perl/Tk that simplified QA testing of software-based device simulators. Due to its success, a second version was developed for use in subsequent projects.

· Represented the software team for six months in initial offsite integration efforts with a subcontractor. This included troubleshooting network communications at the packet level, determining specification compliance, and serving as the software point-of-contact for the subcontractor.

Other Experience Highlights

· Developed and taught an online Introduction to Linux course for TCM Security.

· Operate a home cybersecurity learning lab using various tools including: Kali Linux, pfSense, FLARE VM, REMnux, Trace Labs OSINT, ThreatPursuit VM, Linux Mint, CentOS, and VirtualBox.

· Implemented and ran machine learning experiments on the supercomputing cluster at the University of Oklahoma, totaling over 415,000 core hours (47 core years) of processing time.

· Developed tools using Python, Bash, Perl, R, and regular expressions to automatically parse, process, and analyze large experimental data sets, including the generation of statistics and visualizations.

· Completed numerous TryHackMe and RangeForce training rooms, including topics such as: VirusTotal, Splunk, Yara Rules, Suricata, Wireshark, PCAP analysis, OSINT, Malware Analysis, and Ghidra.

· Earned and maintained a security clearance at a previous employer *(currently inactive)*.

Education

Ph.D. Computer Science - University of Oklahoma 2009

M.S. Computer Science - University of Oklahoma 2004

B.S. Physics and Mathematics - Southern Nazarene University 1995

Relevant Certifications & Accomplishments

· eLearnSecurity Junior Penetration Tester (eJPT)
· CompTia Security+
· INE: Cloud Fundamentals
· TryHackMe: Top 0.5% *(as of 2022.06.23)*
· RangeForce: SOC Analyst 1 Elite, SOC Analyst 2
· AttackIQ: Operationalizing MITRE ATT&CK

Relevant Training

· Black Hills Information Security: Active Defense & Cyber Deception *(June 2021)*, Getting Started in Security with BHIS and MITRE ATT&CK *(May 2021)*, Network Forensics and Incident Response (May 2022)

· Active Countermeasures: Cyber Threat Hunting *(May 2021)*

· INE: Cloud Foundations *August 2021*, Reverse Engineering Professional *(July 2021)*, Malware Analysis Professional *(July 2021)*, Penetration Testing Student *(May 2021)*

· TCM Security: Open-Source Intelligence Fundamentals *(July 2021)*, Practical Ethical Hacking *(June 2021)*

Volunteer Experience

· Developed and led a free 13-week YouTube series introducing Python to non-programmers.

· Served as a peer reviewer for 3 research journals and 5 research conferences and as a grant proposal reviewer for the National Science Foundation.

· Mentored Bethany High School and Elementary robotics teams from 2015 to 2019.

Brent Eskridge, PhD · resume@brenteskridge.com