Jay Hayward

github.com/JayHayward
jay@jayhayward.com

(970) 215-7103
Westminster, CO 80020

Cybersecurity Engineer

Languages - C, C++, Python, Bash, Git, Linux/Unix CLI, PowerShell, SPL. KQL

Tools - Windows Active Directory, Microsoft Defender for Endpoint, Microsoft Azure, Splunk, ServiceNow

Professional Experience

Staples – SOC Analyst Tier II (February 28, 2022 – January 26, 2024)

- Use ServiceNow to receive and manage security incidents that have been reported via Staples internal services or submitted from endpoint users in a timely fashion.
- Handle security incidents such as potential malware, suspicious processes, account modification, among others, leveraging Splunk for event details and log analysis.
- Analyze escalated security incidents and supported efforts to reduce false positives.
- Create and develop tools and scripts to support triaging and managing security incidents across endpoints.
- Work with team to handle real-time active incidents that occur within the company.
- Analyze and review emails that have been marked as phishing automatically or reported by users.
- Leverage Windows Defender for Endpoint to remediate, terminate, and remove malicious files, registry keys, and processes from endpoints in real-time using Windows Live Response.
- Work with users across the company to notify and validate suspicious activity, as well as revoking user sessions and resetting passwords as necessary.
- Leverage Windows Active Directory for analyzing activity involving users and security-enabled groups.
- Participate in training and activities revolving around detection, real-time response, remediation strategy, and further security measures.
- Remaining up-to-date with current and prominent threats in the evolving threat landscape.

Opentext | Webroot – Threat Research Analyst (February 22, 2021 – February 24, 2022)

- Analyzing potentially malicious scripts picked up by Webroot antivirus in the form of PowerShell, Javascript, Visual Basic, and Batch scripts.
- Conduct analysis, de-obfuscation, and reverse engineering on malicious samples to determine their function and evasion techniques.
- Writing PowerShell scripts for automation across industry-standard Windows systems.
- Utilizing Linux and Windows virtual machines to develop and execute my own malware to test Webroot antivirus detections and reports on certain edge cases.
- Working with my own and other teams to update and publish live patches to Webroot antivirus in a timely fashion.

Staples – SOC Engineering Intern (June 29, 2020 - August 21, 2020)

- Conducting Purple Team exercises to test the functionality of our threat detection systems, including DNS tunneling, SMB remote command execution, and Man-in-the-Middle, among others.
- Utilizing Windows Active Directory architecture and PowerShell scripting to identify and exploit vulnerabilities in various systems including Windows servers and clients in our enterprise network.
- Conducting penetration testing leveraging the MITRE ATT&CK Framework, focusing on Discovery, Lateral Movement, and Defense Evasion.

Events and Competitions

- **Collegiate Cyber Defense Competition** - Won 3rd place, Rocky Mountain Regional competition.
- **HackCU IV** - Developed an algorithm that tracks and recognizes varying heart rate patterns.
- **HackCU V-** Developed a program that introduces CS students to capture-the-flag challenges.
- **Facebook Hackathon 2018** - Won 2nd place for a system that reroutes traffic through a network.

Education

University of Colorado Boulder
Bachelor of Arts, Computer Science

Graduation Date: May 7, 2020
Major Specific GPA: 3.860

Academic Achievements

- Society of Telecom Fellowship (2020)
- National Technical Honor Society (2014)

Extracurricular Activities

- CU Cyber Club: Executive Board (January 2017 – May 2020)
- Collegiate Cyber Defense Team (September 2017 – March 2020)
- Science Bowl (2011-2014)

Major Specific Courses

- Advanced Penetration Testing
- Digital Forensics
- Linux System Administration
- Cybersecurity for a Converged World
- Algorithms
- Operating Systems
- Data Science
- Software Development

Relevant Skills and Experience

- **Collegiate Cyber Defense Competition** - CU Blue Team Strategic Defense Coordinator
  The Blue Team is responsible for keeping numerous web services running against a team of professional penetration testers. I would run constant monitoring and keep a detailed record of any breaches to our system. I was responsible for effectively communicating my reports to a non-technical administration.
- **CU Cybersecurity Club** - Social Media and Marketing Executive
  I was responsible for maintaining a social presence for CU's Cybersecurity Club, which involves giving presentations and generating interest for cybersecurity among students. In the club environment I would help less technically oriented students develop useful skills in a friendly and accommodating setting.
- **Advanced Penetration Testing –** Developing an understanding of vulnerabilities and exploits
  In weekly assignments I would be presented with one or more machines in a private network, where I used tools and scripting to identify and exploit various vulnerabilities to gain user and root access. I analyzed malicious scripts and used reverse-engineering to determine their purpose and function, as well as how to detect them in various forms and systems.