E-MAIL: RESUME@DFIR.NINJA PHONE: UPON APPLICATION

PETER PILARSKI

EXPERIENCE

Sabbatical — Feb 2025 - Present

Individual

- Resigned to personal matters focused on projects, hobbies, and recreation

AWS Security Operations - Operational Research & Development — Nov 2023 – Feb 2025

Security Engineer II

- Assisted complex and emergent investigations by providing technical capability, expertise, and escalations to support AWS Security response efforts
- Automated large-scale log retrieval into ad-hoc deploy-able query instances, allowing engineers to instantiate complex log dive infrastructure via a single interface
- Implemented personalized golden images for an internally developed malware sandbox, providing engineers with their own customized analysis environments including each individual's tooling, configuration, and licenses
- Automated FedRAMP compliance assessment to identify in-scope entities during an investigation, ensuring legal counsel and other parties are engaged in a timely manner to meet incident notification requirements

Amazon Information Security – Security Incident Response Team (SIRT) — Jul 2018 – Nov 2023

Security Engineer I & II

- Provided security incident response for issues impacting Amazon and their 30+ subsidiaries, coordinating among partner teams, legal, and public relations to address critical security events company-wide and manage external communications surrounding those issues
- Developed a scalable and automated digital forensics pipeline to analyze and timeline cross-platform evidence of various formats, enabling rapid parallel investigations with minimal hands-on effort
- Defined responsibilities, capabilities, and escalation paths between partner security teams across the company to support coordinated incident response efforts, adapting processes to global business developments, acquisitions, and new market segments (e.g. healthcare, aerospace)
- Partnered with various business units to increase detection and monitoring coverage, document unique risks and compliance requirements, and develop org-specific incident response run-books
- Managed large-scale incident response campaign efforts to systematically address critical risks company-wide, automating the creation, monitoring, and escalation of issues across thousands of simultaneous service team engagements
- Handled researcher engagement and remediation of vulnerability reports via the security@ mailbox along with private and public bug bounty programs, leading to the creation of a dedicated bounty team
- Guided the transition of corporate network security response to a dedicated team, delivering tooling, training, and documentation to support their operations

Amazon Information Security – Threat Response — Jun 2017 – Jul 2018

Security Engineer

- Triaged, assessed, and remediated security events and vulnerability reports impacting Amazon
- Developed a service to provide rapid triage of artifacts and indicators of compromise, correlating data from various third-party APIs to drive risk-based decision making through easily pivot-able investigations
- Defined incident response telemetry requirements for an in-house endpoint detection and response agent
- Developed internal training and exercises for the broader security organization
- Guided development of a company-wide phishing reporting service to de-duplicate internal reports, provide artifact extraction, and enable rapid triage

Amazon Information Security – SIRT — May 2016 – Aug 2016

Security Engineer Intern

- Developed tooling to collect forensic images from physical endpoints, with output to centralized AWS infrastructure (S3)
- Developed automation to perform forensic analysis tasks on encrypted disk images stored in S3, triggered upon evidence upload

EDUCATION

Eastern Michigan University – Ypsilanti, MI 2014 – 2017

- BAS Information Assurance and Cyber Defense – NSA CAE-CD (3.98 GPA)
- Security club: member, competitor, mentor

Henry Ford College – Dearborn, MI 2012 - 2015

- AAS Information Assurance (3.63 GPA)
- Programming club: founding member, VP

TRAINING

- AWS Associate Architect
- AWS Security Specialist
- SANS FOR498: Battlefield Forensics & Data Acquisition
- SANS FOR518: Mac and iOS Forensic Analysis and Incident Response
- SANS FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
- CrowdStrike Falcon Administration, Response, and Hunting

HOMELAB