Alex Hegyi

949.677.6418 | hegyia2@hotmail.com | www.linkedin.com/in/hegyia

Work Experience

Blackberry Cylance

Senior Threat Analyst, Hunting & Intel 01/2017 – Present

- Utilize knowledge of offensive techniques and strategies in order to hunt for new and novel malware campaigns; improving detection capabilities and contributing to technical blogs.
- Design an automated python utility to validate EDR rules via known sample back-test as well as customer soak for integration in to live hunting systems.
- Research solutions strategies for MITRE ATT&CK techniques and delivered documentation to sales and support teams for implementation in to customer environments.
- Reverse engineer malware to design mitigation strategies in collaboration with both offensive and defensive teams to ensure the best effective detection solution utilizing Cylances' product offerings for external and internal customers.
- Participate in high-value deals as a subject matter expert providing best practice recommendations and custom product implementations. Managed and executed cross-functional projects that had a direct impact on over 10 million dollars of revenue.
- Write strategic assessments of product bypass reports and develop strategies to improve product security.
- Analyze threat trend data across large data sets, both structured and unstructured, to provide internal and external stakeholders guidance on impact and implementation solutions.
- Architect and deliver an EDR training course around OPTICS to enhance customer utilization and user experience.

Cylance, Inc

Malware Analyst 02/2016 – 1/2017

- Analyzed files from multiple OS and types in order to characterize and label malware from legitimate software.
- Studied generic and contextually based malware to develop automated tools to efficiently scale with the increased alerts from Cylance's next-generation malware detection engine.
- Conducted in-depth static and dynamic analysis of malware to understand adversarial trade-craft to improve detection, prevention, and response capabilities.
- Created and maintained a VM lab network environment for evaluation of new and novel attack strategies, as well as malware and attack campaign analysis.

Alex Hegyi, Inc

Computer and Networking Consultant 05/2015 – 02/2016

- Self-employed building networking solutions for homes and small businesses including those in the real estate and legal services industries.

Virtium Technology

Senior Systems Engineer, Design 02/2014 – 04/2015

- Designed schematics and PCBs for 10 SSD products and form factors including, USB 3.0, SATA 2.5", NGFF m.8, and CFAST, all approved for production and in-market.
- Performed failure analysis engineering work and circuit design validation on more than 20 SSD products, and provided certification reports for customer assurance of future quality.
- Developed and executed testing framework using industry standard tools, including power cycle testing, temperature and electrical 4 corner, and workload-specific write amplification, in order to deliver pre-market reports to potential customers.

Western Digital

Senior Systems Engineer, Design 04/2011 – 11/2013

- Created prototype SSD products in multiple form factors for preliminary firmware development and testing.
- Constructed custom designs for customer driven needs such as low clearance enclosures, one-sided placement layouts, and forced air cooling solutions.

CERTIFICATIONS

eLearnSecurity Junior Penetration Tester (eJPT)	2019
CompTIA Cybersecurity Analyst+ (CySA)	2018
Global Information Assurance Certification (GIAC) Reverse Engineering Malware (GREM)	2017
CompTIA Security+	2015

EDUCATION

Rensselaer Polytechnic Institute

B.S. Electrical Engineering, Hardware Design 2009

SKILLS AND TOOLS

- Portable Executable (PE) file structure
- Malware Analysis Tools (ProcMon, CFF Explorer, PE Studio, peepdf, etc.)
- Anti-Virus and EDR Solutions technology
- Disassemblers & Debuggers (IDAPro, Ghidra, Immunity)
- Wireshark PCAP analysis
- YARA
- Windows and Linux/Mac internals and hardening
- C and Python familiarity
- Contributing author, BlackBerry Research & Intelligence Team (https://blogs.blackberry.com/en/author/the-blackberry-research-and-intelligence-team)
- CTF: Antisyphon ACE-T level 8