Peter Dohr
1473 Allen Rd, Webster, NY 14580 | (585) 490-3052 | Pdohr33@gmail.com
www.linkedin.com/in/Peter-Dohr

TECHNICAL KNOWLEDGE

Systems:	Experience working in a Windows/Linux, database, server, and virtualized environments
Technologies:	Security Information and Event Management (SIEM), Advanced user of Threat Intelligence Platforms (TIP), Endpoint Detection and Response (EDR), Intrusion Detection/Prevention Systems (IDS/IPS), Data Loss Prevention (DLP), Vulnerability, Offensive, Forensic tools

PROFESSIONAL EXPERIENCE

Paychex, Inc, Rochester, New York
Cyber Threat Intelligence: Cyber Threat Hunt Lead: | March 2020 - Present

- Responsible for researching, assessing and prioritizing cyber threats based on internal and external relevance and impact.
- Participate in capturing historical threat activity, trends and common attack vectors to predict and prevent future threats.
- Developed a custom tool for using MITRE ATT&CK to map adversaries and detection capabilities to help focus threat hunt prioritization and tracking.
- Lead Purple team engagements utilizing offensive security and adversary emulation tools.
- Proactively search to detect and isolate advanced threats that are undetected in the network having evaded existing security solutions.
- Responsible for creating hunt hypotheses leveraging internal and external sources, private sources and trusted partners.
- Responsible for creating and writing custom detection rules.
- Partnering and participating in maintaining sources of data collection and analysis in order to facilitate the hypotheses supporting threat hunting.
- Evaluate new solutions and methodologies (machine-assisted techniques) and provides detailed reviews and recommendations to the Security Intelligence and Response Manager
- Provides research for next generation, traditional and non-traditional cyber threat methods, techniques and tactics specific to evolving IT infrastructures.
- Improve automated detection by prototyping new ways to detect malicious activity and then turning those prototypes into effective new automation.
- Prioritize and guide other team members on daily hunt tasks and responsibilities.

Vulnerability Assessment: Penetration Test Engineer II | June 2019 - March 2020

- Perform both manual and automated penetration tests of internal systems and web applications.
- Research the latest tactics, techniques and procedures (TTPs) of adversaries to test in our environment.
- Conduct assessments of proposed/existing systems and application architecture.
- Work closely with engineering and development teams to remediate findings.
- Triage of Bug Bounty, including validation and assisting with solutions.
- Participate in vulnerability management functions to triage and validate findings.
- Dynamic Application Security Testing (DAST) management, triage, and validations.

Security Investigation Unit: Specialist II | October 2017 – June 2019

- Reverse engineering of malware in a dynamic and static environment
- Manual removal of malware of systems and mobile devices.
- Forensic investigations of both computer and mobile devices using industry standard tools.
- Use of SIEM technologies to proactively identify anomalous behaviors.
- Analyze spoofed, malicious, and other anomalous emails.
- Conduct fraud investigations and create reports to be delivered to law enforcement.
- Conduct security posture examination of subsidiaries, mergers, and acquisitions.
- Conduct internal investigations for legal and HR.
- Project lead of the implementation of DMARC at Paychex.

Security Investigation Unit: Specialist I | October 2015 – October 2017

- Member of Computer Incident Response Team and Cyber Action Communication Team.
- Use of SIEM technologies to proactively identify anomalous behaviors.
- Information gathering from trusted partners to ingest and search within the environment

MIT Lincoln Laboratory, Lexington, Massachusetts
Information System Security Officer | June 2014 – Oct. 2015

- Department of Defense Top Secret Security Clearance
- Provide information system security support to MIT Lincoln Laboratory programs in a classified and unclassified environment.
- Conduct vulnerability assessments and distribution of software patches and antivirus updates.
- Log analysis with the use of SIEM technologies looking for anomalies in environment

- Develop and maintain System Security Plans.
- Ensure Information Technology systems are operated, maintained, and disposed of in accordance with System Security Plans.
- Conduct regular audits to ensure compliance with NISPOM regulations and assist in inspections and reviews.

BitSight Technologies, Cambridge, Massachusetts
Technical Researcher | Nov. 2013 – Apr. 2014

- Responsible for the reconnaissance of public entities using open source intelligence (OSINT).
- Conducted vulnerability scans of internal networks using QualysGuard.
- Reviewed vulnerability reports and made recommendations for securing systems.
- Built organizational profiles for companies across the globe that include mappings of their external IP ranges, addresses, and contacts.

EDUCATION SUMMARY

- **Northeastern University,** Boston, MA

Master of Science in Information Assurance (MSIA), May 2015

- **Niagara University,** Lewiston, NY

Bachelor of Science in Criminal Justice, Minor in Computer Science, Summa cum Laude, May 2013

CERTIFICATIONS AND AWARDS

- GIAC Certified Reverse Engineering Malware (GREM) – September 2018
- GIAC Certified Forensic Analyst (GCFA) - August 2017
- GIAC Certified Incident Handler (GCIH) - September 2016
- CompTIA Security+ - April 2015
- Boy Scouts of America, Eagle Scout - July 2009