STEVEN DEARSTYNE

Allentown, PA • 585-690-8330 • steven.dearstyne@gmail.com

SKILLS & QUALIFICATIONS

Active Directory & Entra ID • Identity Governance • Privileged Access Management •
SIEM & Log collection • Multi-factor authentication • Industrial control system security •
Security awareness training • Technical lead • Mentoring

Certification: Certified Information Systems Security Professional (CISSP)
Programming: PowerShell, .NET, Python, Bash, Perl, Java, C++, Azure DevOps
Publication: IEEE – Leveraging public posts and comments as covert channels – IWSSIP 2014 Proceedings

EXPERIENCE

Air Products and Chemicals Inc. *Allentown, PA*
IT Security Services **Jul 2017 – Present**

- Architected and supported identity and access management solution for managing credentials, security groups, file share access, and identity lifecycle processes.
- Designed strategy for organizational migration from federated authentication to cloud authentication.
- Onboarded four new team members in India and collaborated to establish roles and responsibilities.
- Partnered with HR to enhance new hire onboarding, eliminate legacy processes, and introduce automation.
- Coded and supported multiple .NET workflows for identity lifecycle management.
- Developed on-call rotation strategies for security incidents and user account provisioning & deprovisioning.

IT Security Engineering **Jul 2016 – Jul 2017**

- Developed custom solutions to integrate on-premises IIS logs, Azure IIS logs, and Azure SQL logs into SIEM.
- Implemented and configured a file activity monitoring solution for sensitive file shares, OneDrive, and SharePoint.
- Contributed to phishing response processes, phishing campaign design, and company-wide security awareness.
- Collaborated to develop a new plant cybersecurity architecture and ranked recommendations by consequence.

Plant Automation Cybersecurity **Jul 2015 – Jul 2016**

- Traveled to several high consequence facilities to redesign control system architecture into segmented zones. Infrastructure changes were completed at running plants with no impact to production.
- Designed and began implementation of multi-factor authentication solution for remote access to control systems.
- Tested and rolled out cybersecurity hardening policies for control systems at several remote plants.
- Collaborated with enterprise security teams to develop an incident response plan for industrial control systems.
- Developed custom parser and forwarder script to extract remote access logs and feed them into SIEM appliance.

IT Security Engineering **Jul 2014 – Jul 2015**

- Architected and implemented a solution to randomize local administrator passwords on 16,000 workstations. Post-deployment results provided the data necessary for a large cleanup of Active Directory objects.
- Migrated SIEM appliance to a new platform, and diagnosed migration issues for a variety of devices.
- Engineered a multi-factor authentication solution for externally available services and began pilot rollout.

Rochester Institute of Technology *Rochester, NY*
Graduate Assistant **Sep 2012 – May 2014**

- Managed and configured an air gapped security lab and a Mac/PC lab for student use in and outside of class.
- Performed imaging, modified network configurations, updated software/hardware, and monitored lab performance.
- Graded and assisted during lab sections for C++, Malware, and Network Services courses.

EDUCATION

Rochester Institute of Technology **Rochester, NY**
Bachelor of Science in Information Security and Forensics Graduated May 2012
Master of Science in Computing Security Graduated May 2014
BS GPA: 4.00/4.00, MS GPA 3.77/4.00