{Evan Nevermore} – InfiniteInsight@gmail.com

Nevermorelab.com – github.com/InfiniteInsight

Summary: Cybersecurity Engineer with Systems Administration roots. Heavy focus on self-improvement through self-education and mentoring others. I often use my test lab to explore concepts, protocols, programs and to sandbox things for analysis. Heavily engaged, naturally curious with a positive outlook. I'm not just a warm body in a seat. I wear many hats!

Xperi - *Enterprise Security Engineer* 7/2/21 to Current

- Management of Public Key Infrastructure and related processes
  - **Reduced expired Security Certificate Related outages by 100% year over year.**
- Digital Forensics and Incident Response
  - Reduced eradication and remediation time by half
  - Wireshark / Network Traffic Analysis
  - Memory Captures / Machine Images and analysis
  - Communications with management and stakeholders
  - Attribution and analysis
  - Write detailed and easy to understand reports
- Cloud Security
  - Reduced persistent overexposure alerts by 90% through education of technical teams. No new related alerts have been observed for a period of over 6 months.
- SOC Operations
  - Microsoft Sentinel / Exabeam (previous SIEM): Create alerts, review alerts, create workbooks and playbooks
  - Microsoft 365 E5 Security
- Network Security
  - Review firewall settings and make suggestions for improving posture through surface reduction
- Vulnerability Management
  - Ensuring every new server that is going on the internet has no severity 5 or 4 vulnerabilities
  - Regular scan cadence
- Threat Hunting
  - Identifying intrusions and or opportunities for improvement without triggered alerts
- Tooling setup and configuration audits
- Detailed and clear documentation
- Liase with other technical teams (light yellow teaming/DevSecOps)
- CTI / Track the pulse of the global threat landscape with OSINT

Xperi – *Systems Administrator* 9/10/2018 to 7/1/21

- Managed a Multi-forest Active Directory environment and related services; DHCP, DNS, DFS, Group Policy, etc. in a small team of 5 across the globe
- Microsoft Exchange

- Windows and Linux Administration
- Ansible
- vmWare, Nutanix
- NetApp/EMC
- PowerShell and Automation
- Machine Learning Support
- Tier 3 Support for Help Desk
- Commercial off the shelf software deployment, configuration and maintenance
- Documentation
- Backups
    - Schedule and test
- Monitoring of systems and services

Maryland Transportation Authority via Elegant Enterprise Wide Solutions - *IT Technical Systems Administrator* 7/24/17 to 9/9/2018

- Authority Operations Center subject matter expert
- Tier 3 for Help Desk
- Patch testing and deployment through SCCM
- Permissions audits
- Coordinate with service desk staff to configure, test, and support Active Directory, Group Policy, and all physical and virtual endpoints and infrastructure
- Complete lifecycle systems architecting, installation, configuration and maintenance of servers, corresponding settings and applications
- PowerShell

Eurofins E&E (prev. MET Labs) – *Systems Administrator* 2013 – 7/21/2017

- Monitor network and asset health
- Manage Helpdesk queue, research and provide solutions, and follow up on outstanding issues
- Active Directory and permissions auditing
- Microsoft Exchange 2013, Skype for Business and SharePoint 2013
- Standard image maintenance and deployment through Windows Deployment Services (WDS) and Microsoft Deployment Toolkit (MDT)
- Group Policy
- Order equipment and software
- Troubleshooting and modifying programs written in-house by departed employees
- Salesforce Administration
- Proactive preventative maintenance
- Running cable
- Quality Assurance (QA) testing for internally developed applications
- PowerShell and Scripting Automation
- Extensive and clear documentation that anyone can follow

Security+ COMP001020587498, 4/18 to 4/21