Peter Merola

STRATEGIC LEADER IN CYBERSECURITY ENGINEERING & MANAGEMENT

📞 (315) 427 2737   ✉ merola.peter@gmail.com   🌐 Linkedin

Dynamic cybersecurity professional with over 8 years of comprehensive experience in leading cybersecurity initiatives across diverse sectors. Expert in crafting robust security architectures, leading cross-functional teams, and driving the implementation of battle-tested security solutions. Proven track record of enhancing system security, reducing vulnerabilities by up to 25%, and delivering substantial improvements in operational efficiency. Leadership acumen demonstrated in roles requiring the orchestration of complex cybersecurity projects and initiatives. Holds a Master's degree in Cybersecurity with advanced certifications including SANS GIAC, Palo Alto Networks, CompTIA, and EC-Council's Associate C|CISO Grandfathering Program, positioning well for roles as Cybersecurity Engineering Manager or Chief Information Security Officer (CISO).

Work Experience

Cyber Security Consultant

Self-Employed Freelancer, Remote. April 2023- Current

- Implemented customized security solutions for clients' projects, resulting in a potential 30% decrease in cyber-attacks and a potential 20% increase in overall system efficiency.
- Provided support after hours as needed for clients.
- Collaborated with cross-functional teams to identify vulnerabilities in client systems, ultimately reducing potential cyber threats by 50% and increasing client potential satisfaction ratings by 25%.

Cyber Security Manager

Enact Mortgage Insurance, Raleigh, NC, March 2023 - April 2023

- Developed and executed a comprehensive cybersecurity risk assessment strategy, identifying and mitigating vulnerabilities across IT systems.
- Fostered strong collaborative relationships with IT and business units to align cybersecurity initiatives with organizational goals.
- Enhanced the organization's security posture by integrating advanced threat detection and response systems.
- Delivered insightful security analysis and recommendations to executive leadership, driving informed decision-making on cybersecurity investments.

Cyber Security Engineer

WakeMed Health & Hospitals, Raleigh, NC, May 2022- March 2023

- Improved network, application, and cloud security through the implementation of secure frameworks, resulting in 25%
- reduction in potential vulnerabilities.
- Acted as Subject Matter Expert (SME) for Proofpoint Email Security Platform and Palo Alto Next Generation Firewalls
- resulting in at least 50% improvement in efficiency and reduction in operating costs.
- Evaluated existing security architecture and protocols for risk of vulnerability and recommended improved tools and
- protocols to management.
- Performed security audits to bring awareness about security problems and issues.

Key Expertise

- ✓ Leadership & Project Management
- ✓ Cybersecurity Program Development
- ✓ Email Security
- ✓ Advanced Threat Detection & Response
- ✓ Network Security
- ✓ Cloud Security Architectures
- ✓ Firewall/IPS
- ✓ Stakeholder Engagement & Communication
- ✓ Advanced Security Frameworks & Technologies

- Directed the overhaul of network, application, and cloud security frameworks, achieving a **25% reduction in vulnerabilities** and significantly mitigating potential risks.
- Served as the Subject Matter Expert for Proofpoint Email Security and Palo Alto Firewalls, enhancing security measures while **reducing operating costs by 50%.**
- **Led a 30-person team** in achieving a critical F35 Project Milestone, enhancing project efficiency by 25% through strategic leadership and innovative cybersecurity solutions.

Education

Master of Science in Cybersecurity

Saint Leo University, St. Leo, FL

Bachelor of Science in Computer Information Systems

Saint Leo University, St. Leo, FL

Principal Systems Administrator

Northrop Grumman Corporation, Patuxent River, MD, September 2020- July 2021

- Identified IT service delivery enhancements, leading to improved system performance and user satisfaction.
- Managed and optimized Tenable Nessus Security scans, ensuring comprehensive network and system security.
- Conducted preventive maintenance and system upgrades, enhancing data availability and system integrity.
- Ensured robust system support by managing, troubleshooting, and restoring critical data and system functionalities.
- Streamlined system management processes, improving network and data security while ensuring efficient system operations.

Certifications

- ⊘ Associate C|CISO Grandfathering Program, EC-Council
- ⊘ GIAC Certified Enterprise Defender (GCED)
- ⊘ Palo Alto Networks Certified Network Security Administrator (PCNSA)
- ⊘ CompTIA Security+
- ⊘ CompTIA A+
- ⊘ CompTIA Network+

Information Security Administrator IV

Texas Christian University, Fort Worth, TX, August 2019- May 2020

- Designed and delivered effective security training programs, significantly elevating the security culture among employees.
- Established stringent user access controls, bolstering the security of sensitive academic and personal data.
- Conducted forensic investigations to address and remediate security breaches, minimizing impact and recovery time.
- Analyzed and mitigated malware threats, securing the university's IT infrastructure against sophisticated cyber attacks.
- Implemented and managed robust access and identity management solutions, ensuring secure and compliant access to IT resources.

Systems Engineer, Computer System Analyst

Lockheed Martin Corporation, Orlando, FL & Fort Worth, TX, January 2016- August 2019

- Directed a team of 30 to achieve an essential milestone in the F35 project, boosting project efficiency by 25%.
- Oversaw the organization-wide migration to ordinated comprehensive inventory management and cybersecurity measures, including patching and remediation efforts, to safeguard critical systems.
- Developed and implemented New Hire Documentation processes, leading to a 50% improvement in onboarding efficiency and employee readiness.
- Played a crucial role in enhancing cybersecurity posture through meticulous management of Tenable Nessus Scans and system updates, ensuring high levels of system security and compliance.

Technical Skills & Additional Work Experience

- **Analytics & Monitoring Tools:** Expertise in utilizing Elasticsearch and Kibana for advanced data analysis and visualization, enabling effective security monitoring and incident response. Skilled in the deployment and management of OSSEC Wazuh for comprehensive threat detection and analysis.
- **Cloud Services & Security:** Proficient in securing cloud environments across platforms such as AWS, Azure, OCI, and Akamai Linode. Demonstrated capability in implementing robust cloud security measures, ensuring data protection and compliance in multi-cloud environments.
- **Cybersecurity Technologies:** Deep understanding of Endpoint Security solutions including Trend Micro, CrowdStrike, and SentinelOne, ensuring endpoint resilience against cyber threats. Advanced knowledge in Email Security with Proofpoint, and expertise in Network Security technologies from Palo Alto Networks, Juniper Networks, Cisco, and Fortinet.
- **Identity & Access Management (IAM):** Extensive experience with IAM solutions including SailPoint, CyberArk, Cisco Duo, and Okta. Skilled in the design and implementation of IAM frameworks to enhance security posture and ensure compliance with regulatory requirements.
- **Scripting & Automation:** Proficient in scripting languages such as PowerShell, Bash, and Python for automating security tasks, enhancing operational efficiency, and customizing security solutions to meet organizational needs.
- **Security Frameworks & Compliance:** In-depth knowledge of security frameworks including ISO 27001 Series, NIST SP 800-53, GDPR, CIS Controls, MITRE ATT&CK, SOC2, PCI DSS, and HIPAA. Expertise in aligning security practices with regulatory requirements and industry standards.
- **Systems & Virtualization:** Comprehensive experience in managing and securing Windows, macOS, and Linux systems. Skilled in virtualization technologies like VMWare, Hyper-V, and Citrix, optimizing IT infrastructure for security and efficiency.

References are available upon request