JEREMIAH PEGUES

New York, NY ▪ jeremiah@pegues.io ▪ (917) 690-5011 ▪ LinkedIn

TECHNICAL PROGRAM MANAGER, DATA SECURITY

Cybersecurity and IT Security Specialist with 10+ years of experience in endpoint security, data loss prevention, threat detection, and risk mitigation across enterprise environments. Skilled in security policy enforcement, authentication solutions, and system migrations, enhancing data protection for 100K+ endpoints. A strategic problem solver and leader, adept at optimizing security frameworks, reducing vulnerabilities, and driving operational efficiency in complex infrastructures.

CORE COMPETENCIES

Endpoint Security ▪ Data Protection ▪ Threat Detection ▪ IT Infrastructure ▪ System Migration ▪ Cybersecurity Strategy
Machine Learning ▪ Automation ▪ Incident Response ▪ Risk Mitigation ▪ Security Information & Even Management (SIEM)
Team Collaboration ▪ Security Policy Development & Enforcement ▪ Network Security ▪ Policy Optimization ▪ Compliance

EDUCATION & CERTIFICATIONS

Bachelor of Science, Computer Science ▪ St. John's University
Symantec Data Loss Prevention 15.5 ▪ Certified Information Systems Security Professional
AWS Certified Solutions Architect Associate ▪ Certified Cloud Security Professional (CCSP)

PROFESSIONAL EXPERIENCE

MANAGER, DATA SECURITY ▪ Capital One Financial Corporation   Feb 2024 to Feb 2025

Operations:

- Implemented advanced Data Loss Prevention (DLP) controls across SaaS and IaaS environments, strengthening security post-incident and reducing unauthorized data access, enhancing compliance, and mitigating risks to protect sensitive information.
- Directed an Agile team to execute a strategic plan, conduct risk assessments, and implement advanced DLP tools, reducing unauthorized data access incidents and strengthening cybersecurity posture across enterprise environments.
- Spearheaded the onboarding of 24/7 support for DLP Engineering services on the Symantec DLP platform, creating runbooks and triage instructions, increasing engineering resource availability by 30% through streamlined processes and stakeholder alignment.

Achievements:

- Enhanced GDPR and HIPAA compliance by 30% and improved system scalability by 25% by conducting technical analysis, rectifying vulnerabilities, and implementing secure, scalable DLP solutions using DevOps practices.
- Optimized DLP infrastructure post-security audit using ITIL best practices, implementing strategic upgrades that improved operational efficiency, reduced response times by 15%, and accelerated incident processing speed by 4x.
- Boosted stakeholder engagement and technical proficiency by 30% through leading Symantec DLP upgrades, optimizing platform performance, and delivering comprehensive training programs to enhance adoption and security best practices.
- Reduced data handling errors by 43% in six months by launching a DLP awareness initiative, designing workshops, and implementing change management strategies to strengthen data security and organizational best practices.

SENIOR SECURITY CONSULTANT ▪ Amazon Web Services   Aug 2022 to Sep 2023
Professional Services (AWS ProServe)

Operations:

- Enhanced clients' security posture by implementing AWS security best practices, leveraging AWS WAF, Shield, and Inspector, ensuring GDPR, HIPAA, and PCI DSS compliance, and mitigating vulnerabilities to strengthen cloud resilience.
- Led Fortune 1000 companies in AWS migration, implementing a well-architected framework and secure-by-design principles, resulting in scalable, secure, and compliant cloud architectures that enhanced performance and regulatory adherence.
- Modernized and refactored legacy applications using AWS Lambda, ECS, and API Gateway, boosting performance, increasing scalability, and reducing operational costs, enabling clients to achieve greater efficiency and cloud optimization.

Achievements:

- Increased endpoint compliance to 97% for workstations and 100% for servers by managing business transformation projects and implementing security solutions, enhancing overall security posture and regulatory adherence.
- Achieved significant cost savings and optimized resource utilization by developing and executing application modernization strategies, analyzing workloads, right-sizing resources, and leveraging EC2 Reserved Instances and Savings Plans for efficiency.
- Ensured full compliance with security frameworks by integrating AWS security services, eliminating compliance gaps, and strengthening clients' security posture to meet regulatory standards and mitigate risks.

SENIOR SECURITY ENGINEER ▪ Country Financial   Aug 2017 to Aug 2022
Endpoint Security Team Lead

Operations:

- Led, mentored, and developed a 12-member team, setting clear security metrics, enhancing accountability, and driving cross-division efforts to complete security engineering deliverables ahead of schedule through hands-on guidance and coaching.
- Developed high-quality security engineering documentation and knowledgebase articles, collaborating with SMEs to create installation, remediation, and incident response workflows, enhancing user understanding of architecture and technical solution dynamics.
- Improved security architecture understanding by developing technical documentation and workflows and collaborating with SMEs to create installation, remediation, and incident response guides for enhanced solution adoption.

Achievements:

- Reduced budget needs by $320K in eight months by developing cloud security strategies, optimizing Azure interoperability, collaborating with network security/IAM teams, and designing a capability matrix to assess business-aligned solutions.
- Achieved 97% workstation and 100% server compliance, increasing data loss incident response efficacy by 400% in three years by managing security transformation projects, analyzing risks, and leading cross-functional solution execution.
- Resolved an audit finding nine months early by identifying high-risk areas, devising a data security framework, conducting risk audits, refining policies, and enhancing the visibility of structured and unstructured data flows.

SECURITY ENGINEER I , Security Operations Center ▪ Ciphertechs Inc   Apr 2015 to May 2017

Operations:

- Led managed service implementations and security upgrades, enforcing security policies via ePO to drive encryption and prevent data loss, securing over 100K endpoints, and ensuring compliance with industry standards.
- Developed agent-less authentication and asset classification, enabling secure multi-domain user access within shared workspaces, reducing security risks, and implementing policies to approve, deny, or limit network access for enhanced corporate security.

Achievements:

- Upgraded 17K+ endpoints from McAfee OVSEQ to Endpoint Security 10.5, designing a seamless migration path, optimizing policy compatibility, eliminating inactive policies, and enabling advanced machine learning and containment capabilities for enhanced security.
- Reduced false positives by >80% by identifying false negatives in security applications, fine-tuning ESM parsers, and integrating custom parsers to enhance UEBA accuracy and deliver highly correlated security event detection.

PRODUCT LEAD, Wercflow App ▪ Werc FTP (*formerly Treauu Inc*.)   Apr 2015 to May 2017

Operations:

- Transformed development priorities into a market-aligned MVP by analyzing the competitive landscape and target audience, ensuring the product met end-user needs and preferences.
- Defined user stories and acceptance criteria, reducing technical debt during MVP to v1 transition, ensuring design consistency and efficient feature implementation.

Achievements:

- Revamped iOS-web integrations, migrating key mobile components from Unity to Swift and Swift UI, enhancing native compatibility, optimizing large media handling, and boosting mobile response time for a seamless user experience.
- Managed and coordinated SDLC for MVP and Beta releases, leveraging agile methodologies to mitigate risks, ensure on-time delivery, and improve functional testing coverage to approximately 90% per sprint.
- Provided technical leadership to a globally distributed team of 9-12 developers, establishing best practices and a collaborative culture that increased efficiency, strengthened commitment, and enhanced overall team performance.