Bowman Williams

Security Analyst- (SOC Operations, Penetration Testing, Vulnerability Management, Compliance Management)

SUMMARY

Certified Cybersecurity Analyst with **7+ years** of experience securing enterprise systems through vulnerability management, incident response, and governance, risk, and compliance (GRC). Skilled in planning, implementing, monitoring, and upgrading security measures to protect critical data and infrastructure across hybrid cloud and on-premise environments. Adept at identifying and mitigating risks, enabling compliance with NIST, ISO 27001, PCI-DSS, HIPAA, SOC 2, and GDPR frameworks. Strong background in SIEM, EDR, penetration testing, and risk reporting. Recognized for improving cybersecurity posture, reducing vulnerabilities, and strengthening regulatory compliance through policy development, audits, and proactive security strategies.

SKILLS

Security Operations & Incident Response: Incident Lifecycle Management, SOC Operations, Threat Hunting, Malware Analysis, Log Analysis, SIEM, Splunk, QRadar, Azure Sentinel, EDR, CrowdStrike, SentinelOne, Carbon Black
Vulnerability & Risk Management: Vulnerability Scanning & Penetration Testing, Nessus, Kali Linux, Burp Suite, Metasploit, Risk Identification, Assessment & Mitigation, Risk Reporting & Tracking, CVSS-based Prioritization, Vendor Risk Assessments
Governance, Risk & Compliance (GRC): Frameworks, NIST CSF, NIST 800-61, ISO 27001, SOC 2 Type II, PCI-DSS, HIPAA, GDPR, Risk Reporting & Quality Assurance, Audit Preparation, Policy & Standards Development, Change Management, Security Awareness & Phishing Campaigns
Network & Infrastructure Security: Security Controls, VPN, SSL/TLS, IPSec, MFA, Endpoint Hardening, DLP, Secure Configuration, Cloud Security (AWS, Azure), Network Traffic Monitoring (Wireshark, OpenVAS, Nmap)
Operating Systems & Tools: Windows, Linux (Ubuntu, CentOS, RedHat), PowerShell, Bash, Security Reporting, User Awareness Training

PROFESSIONAL EXPERIENCE

Senior Security Analyst **| Oct 2022 – Present**
Managed Security & IT Services Provider Houston, TX

- Planned, implemented, and monitored enterprise-wide security controls, reducing containment time by 30% through automated correlation rules.
- Conducted continuous vulnerability assessments and penetration tests, reporting findings and leading remediation aligned with NIST and ISO 27001.
- Coordinated risk assessments, prepared risk reports, and tracked remediation activities to closure.
- Designed and maintained incident response playbooks, reducing MTTR by 40%.
- Integrated SIEM (Splunk) and EDR (CrowdStrike) to enhance detection accuracy and reduce false positives.
- Participated in change management reviews to ensure secure implementation of system changes.
- Led phishing simulations and training for 500+ employees, improving risk awareness.
- Developed audit-ready security documentation and policies to maintain PCI-DSS, HIPAA, and GDPR compliance.
- Developed metrics dashboards for leadership to track incident response performance, vulnerability closure rates, and compliance status.
- Built automated scripts for log enrichment and risk correlation, reducing manual workload by 25%.
- Conducted forensic analysis of security breaches and produced executive-level post-incident reports.
- Engineered and deployed automated SOAR playbooks in Splunk/EDR to accelerate response workflows, cutting manual tasks by 30%.
- Designed and implemented secure IAM policies in Azure AD and AWS, aligning with Zero Trust principles.
- Configured and tuned IDS/IPS signatures and firewall rules to block advanced threats while minimizing false positives.
- Collaborated with vendors and third parties to conduct risk assessments and align controls with contractual obligations.

Cybersecurity Analyst **| Aug 2020 – Sep 2022**
Managed Security Services Provider (MSSP) Houston, TX

- Conducted penetration testing of applications and APIs using Burp Suite and OWASP Top 10, reducing exploitable flaws.
- Performed gap analyses against SOC 2 and HIPAA requirements; supported successful audits with zero critical findings.
- Tuned SIEM alerts and built dashboards for risk monitoring and compliance tracking.
- Monitored encryption, VPN, and access control configurations to ensure secure network practices.
- Partnered with GRC teams to design and maintain risk registers and remediation tracking systems.
- Collaborated with development and operations teams in the change management process, ensuring risks were addressed

prior to deployment.
- Conducted tabletop exercises to test incident readiness and updated escalation procedures based on results.
- Authored technical risk assessment reports and presented recommendations to executive stakeholders.
- Collaborated with DevOps teams to embed security testing into CI/CD pipelines, integrating SAST/DAST scans to eliminate vulnerabilities prior to release.
- Deployed and managed secure VPN, MFA, and access controls for a remote workforce, ensuring compliance with HIPAA and SOC 2.
- Conducted vendor security reviews, aligning third-party practices with organizational security requirements.
- Performed QA on risk assessments, ensuring accuracy of risk scoring and remediation planning.

Information Security Specialist **| Jun 2018 – Jul 2020**
Transportation Technology & Infrastructure Company, Houston, TX
- Conducted endpoint hardening and vulnerability remediation using Nessus scan results.
- Implemented network segmentation and endpoint hardening across 1,000+ devices, reducing lateral movement risks during red-team simulations.
- Deployed DLP policies and integrated monitoring tools that reduced data exfiltration risks by 20%.
- Performed vendor risk assessments and reviewed third-party security controls against organizational requirements.
- Designed phishing simulations that increased employee incident reporting by 45%.
- Authored GDPR and HIPAA awareness materials; delivered targeted training sessions across business units.
- Automated log analysis workflows with Bash/Python, improving detection efficiency.
- Participated in forensic investigations and prepared risk-based recommendations for leadership.
- Developed KPI dashboards tracking vulnerability closure, incident trends, and compliance readiness.
- Assisted in gap analysis against ISO 27001 and NIST CSF, contributing to remediation planning.
- Conducted change management security reviews for new applications and infrastructure deployments.
- Supported DLP policy audits and implemented improvements that reduced data exfiltration risks.
- Partnered with IT teams to improve access control policies and enforce least-privilege models.

EDUCATION

Bachelor of Business Administration (BBA)
Texas Wesleyan University - Fort Worth, TX

CERTIFICATIONS

CompTIA Security+