Bowman Williams

Cybersecurity Professional | CISSP | ISO 27001 Certified

Professional Summary

Cybersecurity Professional with 12+ years of experience defending corporate IT ecosystems. Proven expertise in threat intelligence, incident response, IAM cloud security (Azure, AWS), and penetration testing. Adept in tools like Splunk, Fortigate, CrowdStrike, Nessus, Imperva WAF and skilled in aligning security operations with ISO 27001. U.S. Permanent Resident open to onsite, hybrid, or remote technical roles.

Technical Skills

Security Operations & Incident Response: Splunk, MITRE ATT&CK, CrowdStrike, Threat Intelligence
Vulnerability Management & Penetration Testing: Qualys, Nessus, Burp Suite, Black/Grey Box Testing
Network & Endpoint Security: Firewalls (Fortigate, Forcepoint), Web Application Firewall (Imperva), IDS/IPS, MDR, EDR, DLP, Encryption
Governance & Compliance: ISO 27001, RBAC, Business Continuity, Disaster Recovery
Cloud Security: CSPM (Crowdstrike), IAM (AWS, Azure), Dome9

Certifications

- CISSP – Certified Information Systems Security Professional (ISC2) – 2024
- EXIN Information Security Foundation (ISO/IEC 27001) – 2021

Professional Experience

MSSP

Cybersecurity Operations Specialist | Mar 2022 – Present

- Conducted 50+ risk assessments using Qualys and Nessus to uncover critical vulnerabilities.
- Implemented Splunk, Fortigate, and CrowdStrike tools, cutting undetected incidents by 30%.
- Managed IAM and Change Management, improving ISO 27001 audit response times by 20%.
- Performed cloud security IAM assessment for compliance and risk mitigation.
- Improved and implemented Imperva WAF rules to enhance web application protection and reduce false positives.

IT Company

Security Risk Management & Incident Response | Mar 2018 – Dec 2021

- Automated threat detection with Splunk and Nessus, reducing false positives by 25%.
- Led incident response using MITRE ATT&CK, reducing containment time by 40%.
- Eliminated 80% of high-risk vulnerabilities through penetration testing.
- Oversaw MSP operations for threat intel, alert analysis, and incident response.
- Managed Imperva Web Application Firewall (WAF) policies and alerts to prevent web-based attacks and ensure application security.

Bank | Cybersecurity Identity Management & Incident Response | Oct 2012 – Feb 2018

- Reduced manual IAM workload by 20% through PowerShell automation.
- Managed 400+ RBAC identities to maintain ISO 27001 compliance.
- Configured enterprise firewalls (Fortigate, Forcepoint) for secure access control.

| RBAC Identity Management | Mar 2011 – Oct 2012

- Designed access strategies to improve identity governance and ISO 27001 adherence.
- Managed 100+ RBAC identities to maintain ISO 27001 compliance.

I | IT Security Support Engineer | Aug 2009 – Feb 2011

- Provided endpoint security support, focusing on user access lifecycle.

Education

- Associate Degree in Cybersecurity – Faculdade Impacta Tecnologia (Brazil) – 2018
- Associate Degree in System Analysis & Development – UNIP (Brazil) – 2013

Technical Training & Awards

- Microsoft Office 365: Security & Compliance – 2017
- Web Filtering & Content Protection (Forcepoint) – 2014
- High Performance Merit Award – SuperDigital Brazil – 2019

Languages

- Portuguese – Native
- English – Advanced
- Spanish – Advanced

Additional Info

- Seeking technical cybersecurity roles (not managerial).
- U.S. Permanent Resident – No sponsorship needed.
- Available for onsite, hybrid, or remote opportunities in the U.S.