BILL WEBER

1290 E. Ireland Road V100-249, South Bend, IN 46614 • (571) 833-3000 • bill@cyberfoundrty.io
HTTPS://WWW.LINKEDIN.COM/IN/BILLRWEBER/

CAREER HIGHLIGHTS

LEADERSHIP	Chief Information Security Officer, Detection Response & Forensics Lead, Executive Briefings, and Training, Enterprise & Security Architecture, Program & Project Management
SECURITY	Vulnerability Management, Network Protection (Intrusion Detection, 802.1x, Firewalls, Micro-Segmentation, Zero Trust), Threat Hunting, Security Audit Reviews, Incident Response Planning, EDR/XDR Desktop Support, MITRE ATT&CK, and D3FEND Assessments
COMPLIANCE	OneTrust Governance, Risk Management, and Compliance, NIST Risk Management Framework, GDPR, NIST SP800-53, NIST SP800-171, Cybersecurity Maturity Model Certification (CMMC), FISMA, ISO 27001, FedRAMP, DISA Security Technical Implementation Guide (STIG)
CLOUD	Amazon Web Services, Microsoft Azure
PREMISE INFRASTRUCTURE	VMware, Kubernetes, K8S, Rancher, Docker, L2/L3 Networking, Service Edge Networking

PROFESSIONAL EXPERIENCE

Cyber Foundry, South Bend, Indiana USA 01/2017 to present
CyberSecurity Consultant
Consulting Practice: A boutique cyber security consulting firm offering enterprise-level strategy and implementation services for small and medium businesses. Consulting services include pragmatic and understandable cyber security strategy and operational capabilities and Incident Response Training for Executives and Incident Responders.

- Implement CyberSecurity strategy and operational projects for mid/large enterprise customers.
- Assess and manage CyberSecurity risks; develop post-audit strategy and tactics; develop performance metrics.
- Implement Risk Management programs, GRC tools, policies, procedures, and run books to improve operational maturity. Bring focus to the larger picture, implement, and improve on the basics, and drive organizational capability.

New York University, New York, New York USA 01/2021 to 10/2021
Director of Detection, Response, and Forensics Teams
NYU is a top global research university with an annual academic and research revenue of $3.7bn. As director of the Detection, Response, and Forensics department, I led global efforts to implement and manage a Security Operations Center (SOC) and managed internal, matrix, and multi-national teams to implement security services for 13 global sites.

- Rebuilt SOC detection and response capabilities by rearchitecting the Splunk SIEM and implementing Palo Alto Cortex SIEM.
- Deployed Palo Alto Cortex XDR (Extended Detection and Response) capability across 13 countries.
- Rearchitected the network into an 'Open Campus' and protected networks using Micro-Segmentation and ZTNA concepts.
- Prepared the organization for IT Outsourcing by standardizing operational procedures, negotiating contracts, and performing risk assessments.
- Developed Incident Response Procedures and led multiple Incident Response Activities. Trained leadership on risk and response.
- Conducted listening tours to understand stakeholder needs and adapt the program to the culture of the organization.

Massachusetts Institute of Technology (MIT) Lincoln Laboratory, Lexington, Massachusetts USA 11/2018 to 10/2020
Cyber Security Sector Manager
MIT Lincoln Labs is a Federally Funded, Research and Development Center with an annual research revenue of $1bn. As the team leader for cyber security operations within the Information Technology division, my responsibilities include the development, implementation, and operation of all cyber security operations within DoD classified and unclassified environments. This role extended into protecting unique and threat adverse environments under a high degree of external interest and sensitivity and potential security threats.

- Developed, managed, and operated DoD classified and unclassified security operations centers (SOC) in compliance with CMMC, FISMA, NIST Risk Management Framework, NIST SP800-53, and NIST SP800-171 standards.
- Implemented ACAS and related vulnerability management technologies for the support of DoD classified systems.
- Partnered with researchers to leverage the unique skills of the lab to detect and deter cyber security threats using ahead-of-market insights and technologies.
- Built collaborative, strategic relationships with stakeholders within the lab to advance the cyber security capability and culture.
- Analyzed SOC tooling and procedures allowing a reduction of duplicate capabilities, and provided normalized operating procedures, which were then automated through a Security Orchestration Automation and Response (SOAR) platform.
- Created and monitored performance analytics to measure effectiveness.
- Developed MITRE ATT&CK and CMMC Performance Metrics to improve SOC capabilities.

eSentire, Waterloo Ontario Canada 09/2016 to 09/2018
Principal Security Strategist (Virtual CISO)
Served as a consultant and virtual CISO to clients in the FinTech and Legal industries who were procuring security services from the team.

- Client Advocate performing comprehensive risk assessments and business impact analysis with remediations.
- Partnered with clients to define their risk and map out long-term strategies for their operations.
- Created MDR offerings portfolio while supporting sales and marketing. Managed pricing and profitability of the portfolio.

Hewlett-Packard Enterprise (Electronic Data Systems - EDS), Plano, Texas USA 05/2003 to 05/2016
Chief Information Security Officer (CISO) / Enterprise Architect

- Team leader to implement security services for the Navy-Marine Corps Intranet (NMCI) program with 400,000 users and 1m+ assets globally. Functioned in DoD classified and unclassified environments.
- Developed and implemented a team-based DHS Continuous Diagnostics and Monitoring (CDM) program winning a position on a $6bn contract.
- Team leader to develop and pitch FedRAMP cloud solution offerings to the US Government.
- Provided services as a Virtual Chief Information Security Officer (CISO) to commercial clients.
- Served as a HIPAA Compliance Officer and Lead Security Architect for CMS-focused software development efforts.
- Managed complex projects requiring strong analytical skills and creative cultural adaptation with government clients.

Microsoft, San Diego, California USA 10/1999 to 05/2003
Consultant / Engineer

- Provided deep technical diagnostics for kernel debugging and active directory operations.
- Consulted with and helped clients implement key Microsoft technologies.
- Performed sales, marketing, and consulting activities while embedded with clients.

Winchester Hospital, Boston, Massachusetts USA 01/1998 to 10/1999
Manager, Information Technology

- Managed a team responsible for all aspects of networking, server, and desktop support for a community healthcare provider.

New England Medical Center / Tufts, Boston, Massachusetts USA 01/1996 to 01/1998
Senior Consultant

- Managed networking and server technologies for a regional healthcare provider.

St. Mary's Health Services / Mercy Health Systems, Grand Rapids, Michigan USA 01/1992 to 01/1996
Senior Consultant

- Managed networking and server technologies for a community healthcare provider.

Data Link Systems, South Bend, Indiana USA 01/1990 to 01/1992
Production Coordinator

- Managed the Software Development Lifecycle (SDLC) and go-to-market (GTM) operations for a software development company.

Education

Master of Business Administration (MBA)
The University of Texas at Dallas, Graduated 2011

Master of Science (MS)
Information Technology specializing in Security
Capella University, Graduated 2008

Bachelor of Science (BS)
Computer Information Systems
Excelsior College, Graduated 2006

Publications

Topics including Cyber Security and Crypto Economics can be found on billweber.io.
Professional Profile can be found on LinkedIn.

Certifications

$(ISC)^2$ Certified Information Systems Security Professional (CISSP) #29867
ISACA Certified Information Security Manager (CISM) #1014442
ISACA Certified in Risk and Information Systems Controls (CRISC) #1004569
Microsoft Certified Systems Engineer (MCSE) #1793697
Microsoft Certified Information Technology Professional (MCITP) #1793697
Amazon Web Services Certified Cloud Practitioner (CCP) #01783372
OneTrust Certified Privacy Professional (OCMP) #C68858
OneTrust Cookie Consent #C69390
DoD 8570 IAT 3, IAM 3, IASE 2, CSSP Manager

Honors & Volunteer Activities

Mensa International High IQ Society
Security Special Interest Group Coordinator

Clearances

US Department of Defense TS SSBI (last active 2022)
US Department of Homeland Security (last active 2022)