JEFF BOLLINGER

linkedin.com/in/jeffb0llinger | *Esse Quam Videri*

SUMMARY

- 20+ years of experience in incident response, information security technology, security architecture, cloud security, threat research, risk and vulnerability management, and management of all aspects of security for large enterprises and academic networks
- Capable and accomplished executive with a practical vision for effective security and inspiring managers, engineers, and architects to deliver high quality results

SKILLS & ABILITIES

- Incident response and threat detection
- Cybersecurity threat intelligence
- Technical leader and people of large organizations
- Global enterprise security operations leadership and strategy
- Security investigations and security solutions architect for enterprise networks
- Cloud security and enterprise security
- Experienced international speaker and writer
- SANS Lecturer
- Author of O'Reilly Media's *Crafting the InfoSec Playbook* used in university Cybersecurity courses
- Able to articulate complex security issues appropriately for all levels of business
- Strong understanding of cybercriminal and adversarial techniques and methods

EXPERIENCE

DIRECTOR INCIDENT RESPONSE AND DETECTION ENGINEERING
LINKEDIN
FEBRUARY 2021 – PRESENT

Redesigned and overhauled the incident response program, creating three business functions and expanding to two theaters

Expanded incident response coverage from 10x5 to 24x7 monitoring, nearly doubling the time spent protecting the company from threats

Decreased time to detect and contain security incidents from days to under two hours on average

Designed and implemented a threat intelligence program, expanding coverage of known threats by more than 300%

Reduced risk of phishing from persistent threat actors by 70% through investigations and creative discovery and mitigation techniques

SENIOR MANAGER INFOSEC INCIDENT RESPONSE AND INVESTIGATIONS
CISCO SYSTEMS, INC.
SEPTEMBER 2015 – February 2021

Managed global teams of senior security investigators, managers, and two teams of analysts for US and Americas incident response operations at Cisco

Achieved 24x7 detection, investigation, mitigation, and Incident Response (IR) coordination of digital crimes, policy violations, or malicious activity across the global corporate landscape including private and public clouds like GCP, AWS, Azure, and Oracle

Authored and edited tactical, risk-specific, and data-driven updates within one hour on an incident to executive staff and senior leadership

Visualized incident data to identify key problem areas and drive changes to improve Cisco's security posture and response to threats improving average time to detect to under 24 hours

Developed a highly efficient framework for Monitoring, IR, and business intelligence as a service reducing time to detect incidents to under three hours on average

Streamlined and automated the internal security customer onboarding and solution development process saving 100+ hours and prevented 100s of data entry mistakes

Tailored more than 10 custom security monitoring plans and architects for engagements ranging from small, temporary networks, to FedRAMP compliant clouds and public IaaS, to global enterprise networks

Generated $1M in internal cross charges for services using the framework over the first 4 quarters use

Influenced Cisco's security product portfolio leading to enhanced features, bug fixes, capabilities, and new products along with increased revenue touching over $10M in sales

Consulted with hundreds of major Cisco clients, customer executives, and global companies, discussing CSIRT strategy, best practices, architecture, and success stories influencing $25M+ security sales revenue

TECHNICAL LEADER / INFO SECURITY INVESTIGATOR
CISCO SYSTEMS, INC.
MAY 2006 – SEPTEMBER 2015

Built a world-class team of over 40 people – delivering 24x7 coverage for attack detection and threat mitigation

Created and delivered 20+ security monitoring plans for acquisitions, Cloud (IaaS) environments, insider threats, supply chain partners

Improved network, data, and system visibility and control methods across the global enterprise and cloud platforms by 300%

Invented innovative approach for security monitoring and incident response widely known as the "Playbook" leading to 1000+ hours saved over two years

Led with technical direction, four diverse teams of developers, system/network administrators, and architects to design, build, and operationalize enterprise scale solutions for incident mitigation, investigations, and alerting

Designed and deployed global security monitoring solutions including 350+ intrusion detection sensors, user behavior analytics, honey tokens, NetFlow, transparent web proxies, and deception technology

Incident Handler with deep experience in security investigations and forensics across hundreds of security incidents and attacks against Cisco's global networks, subsidiaries, systems, personnel, and data

Experienced public speaker and lecturer, speaking at more than 10 international conferences

Executed as an organizer an annual international security conference focused on incidents, case studies, tools, and other issues related to incident response and information security for 10 years and over 150 presenters

CUSTOMER SUPPORT ENGINEER: SECURITY ESCALATIONS CISCO SYSTEMS, INC.
AUGUST 2004 – JANUARY 2006

INFORMATION SECURITY ANALYST UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL
AUGUST 2000 – DECEMBER 2003

Co-founded the original incident response team at UNC Chapel Hill investigating more than 20 incidents over three years

EDUCATION

UNVERSITY OF NORTH CAROLINA, CHAPEL HILL, NC
MASTERS OF SCIENCE IN INFORMATION SCIENCE (MSIS)

- Published in academic journal (ACM) and library archives
- Focused curriculum in IP networking, network security, Linux, and metadata

- Managed graduate school lab of 50+ servers and acted as departmental sysadmin

UNVERSITY OF NORTH CAROLINA, CHAPEL HILL, NC
BACHELOR OF ARTS IN ENGLISH WRITING AND LITERATURE (BA)

ETC | **CISSP 41372,** hacker, maker, tinkerer, beekeeper, homesteader, hunger for knowledge