Douglas M. Schauer

MSCSIA, CISSP, CISA, SSCP, CySA+, CEH, CHFI

Middleburg, FL 32068 ▪ 352-316-6154 ▪ schauer6797@gmail.com ▪ www.linkedin.com/in/douglas-schauer-b508a485/

Cybersecurity Engineer

Goal-driven, dynamic **Certified Information Systems Security Professional (CISSP)** with extensive experience intensifying cybersecurity measures across network management software industries and government sectors. **Certified Information Systems Auditor (CISA)** with unmatched competencies in information security management, system administration, vulnerability assessment, and incident response. Excel at developing cutting-edge IT solutions to resolve complex technical issues and bolster security system capabilities. Exemplify leadership, accountability, and integrity to nurture productive collaborations and drive team effectiveness.

Core Competencies

Information Security Governance
Threat & Vulnerability Assessment
Security Policy Development
IT Security Operations
Analytical Problem-Solving

Cyber Defense
Risk Mitigation
Cloud Computing
Business Continuity
Issue Resolution

Identity & Access Management (IAM)
Log Analysis
Systems Engineering
Audit & Compliance
Leadership & Collaboration

Career Highlights

- ✓ Strengthened IT infrastructure by employing Sentinel One to optimize threat detection, facilitate prompt incident response, streamline communication channels, and escalate security incidents per established protocols.
- ✓ Instituted vigorous cybersecurity defense mechanisms in authoring Snort rules, enhancing detection capabilities in Barracuda Web Application Firewall incidents, safeguarding critical assets, and preserving data integrity.
- ✓ Averted potential data breaches and system compromises by identifying, assessing, and resolving unauthorized access incidents from Ukraine, mitigating financial losses while preserving organizational integrity.
- ✓ Mobilized business continuity by deploying IDS and IPS technologies to pinpoint and mitigate threats, decreasing downtime through unauthorized access and data infiltration prevention mechanisms.

Professional Experience

Security Engineer | CITY OF JACKSONVILLE▪ Jacksonville, FL 06/2024 - Present

The professional is responsible for managing the Rapid7 Insight IDR platform and providing support for Microsoft's Intune Mobile Device Management software. He demonstrates proficiency in Microsoft Defender and Azure Intra, contributing to cybersecurity efforts. Additionally, he conducted load testing on the city's emergency preparedness website using Opentext's Loadrunner and implemented the OpenVAS vulnerability scanner for effective vulnerability management.

Senior Threat Analyst | QUADRANT INFORMATION SECURITY ▪ Jacksonville, FL 03/2022 – 03/2024

Fortified defense systems by navigating cutting-edge technologies to mitigate potential threats and safeguard digital infrastructure.

- Conducted comprehensive, real-time analysis of security events from multiple sources, including complex security information monitoring tools, intrusion detection systems, and diverse log data, reducing incident response time.
- Ascertained 100% service level agreement compliance by executing network and log-centric analysis while utilizing IDS, IPS, and signature matching technologies to assess, troubleshoot, and resolve technical issues.
- Led first response team in regulating critical breach incidents, minimizing impact and escalation through robust multi-factor authentication protocol administration to reinforce access controls.
- Mitigated potential threats by performing in-depth log analysis, spanning Windows servers, CrowdStrike, Carbon Black, Sentinel One, Microsoft Azure, Linux, and various firewalls, improving system reliability and resilience by.

Security Analyst | QUADRANT INFORMATION SECURITY ▪ Jacksonville, FL 02/2021 – 03/2022

Optimized IT security system against malicious intrusions through real-time monitoring, network analysis, and risk mitigation.

- Galvanized organizational defenses by facilitating continuous surveillance across multiple sources, encompassing security information monitoring tools, intrusion detection systems, and system logs across Unix and Windows platforms.

- Benchmarked best practices on solution integration, technological breakthroughs, incident response, threat hunting, monitoring, and vulnerability management by attending several training programs.
- Augmented first-line troubleshooting support for low-level engineering issues and process documentation while serving as the primary liaison for escalating security issues or incidents per established protocols and management directives.
- Secured critical print server infrastructure by identifying and mitigating sophisticated Log4j vulnerability exploits through black box penetration test implementation, preventing potential data breaches and system infiltrations.

Desktop / Help Desk Support Technician | VISTA DEFENSE TECHNOLOGIES, LLC ▪ Jacksonville, FL 05/2017 – 02/2021

Bolstered optimal network performance and top-notch technical support among 3K+ users at Naval Hospital and 5 branch clinics.

- Boosted IT systems' optimum functionality by overseeing nightly data backups of confidential medical records on Microsoft Windows 2012 R2 Server, upholding the highest standards of data accuracy and 100% regulatory compliance.
- Systematized user account management, encompassing credential renewal, confidential agreement signing, security access processing, security PIN code reset, and PIV certificate verification for CAC cards.
- Resolved 75% of hardware and software issues through systematic troubleshooting while collaborating with several military personnel and various hospital staff to provide immediate technical support in high-pressure environments.
- Reduced vulnerabilities by conducting periodic data center inspections to heighten physical security standards, enhancing network integrity by 50 through proficient application of network topology and connectivity.

Distributed Computer Systems Analyst | FLORIDA DEPARTMENT OF CORRECTIONS ▪ Lake Butler, FL 01/2008 – 02/2015

Elevated security standards in network administration of 1K+ users at 7 correctional facilities, encompassing desktop support, troubleshooting, domain controller management, VoIP implementation, as well as data backup and recovery.

- Intensified risk mitigation mechanisms in executing annual security audits, strong password policy implementation, malware eradication, inactive user removal, and inventory database maintenance of physical assets for 5 sites.
- Amplified optimal performance by utilizing diagnostic and testing tools, updating servers with security patches, and configuring host and server hardware in compliance with written procedures and standardized images.
- Enhanced user experience by simplifying complex computer details for non-technical personnel to facilitate open communication on emerging issues, foster collaboration, and increase productivity.

Additional Work Experience

Network Specialist ▪ FLORIDA DEPARTMENT OF Transportation ▪ Deland, FL
Independent IT Contractor ▪ Lake Butler, FL
Lieutenant ▪ UNITED STATES NAVY
Nuclear-Trained Submarine Officer

Education & Professional Development

Graduate Student pursuing PhD Information Systems Security
UNIVERSITY OF THE CUMBERLANDS ▪ Williamsburg, KY
Estimated Graduation 2028

Master of Science in Cybersecurity & Information Assurance
WESTERN GOVERNORS UNIVERSITY ▪ Salt Lake City, UT ▪ 2020

Bachelor of Science in Information Systems Security, Minor in Digital Forensics
AMERICAN MILITARY UNIVERSITY ▪ Charles Towne, WV ▪ 2016
Distinction: Cum Laude

Associate of Science in Computer Network Engineering Technology
KEISER UNIVERSITY ▪ Melbourne, FL ▪ 2005
Distinction: Phi Beta Kappa

CERTIFICATIONS

ISACA Certified Information Systems Auditor (CISA)	Valid until 01/2027
EC-COUNCIL Computer Hacking Forensic Investigator (CHFI)	Valid until 10/2026
EC-COUNCIL Certified Ethical Hacker (CEH)	Valid until 06/2026
(ISC)^2 Systems Security Certified Practitioner (SSCP)	Valid until 02/2026
CompTIA Cybersecurity Analyst Plus (CySA+)	Valid until 08/2025
CompTIA Security+, A+, Network+	Valid until 08/2025
(ISC)^2 Certified Information Systems Security Professional (CISSP)	Valid until 06/2025
Axelos ITIL 4 Foundations	No Expiry
LPI Linux Foundations	No Expiry

TECHNICAL SKILLS

Security Solutions: Sentinel One, Suricata, Sagan, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Rapid7 InsightIDR, Microsoft Defender, Microsoft Intune MDM

Cloud Computing: Microsoft Azure

Network & Communication: Voice over IP (VoIP), Cisco, Baystack, HP

Operating Systems: Microsoft Windows 10/11, Microsoft Server 2012, 2016, 2019, Ubuntu LTS 20, 22, 24