

Brian Villanueva

CISSP, CISM, CASP+

Illinois • (309) 613-8943 • b.vill1@yahoo.com • [linkedin.com/in/brian-villanueva](https://www.linkedin.com/in/brian-villanueva)

Cybersecurity Specialist with 15+ years of experience driving measurable security improvements across diverse environments, including cybersecurity, physical security, and emergency services. Proven ability to lead strategic security initiatives, implement advanced threat detection systems, and reduce security incidents by up to 70% (as demonstrated at Alto Ingredients). Skilled in aligning security operations with business goals, fostering a security-first culture, and managing risk. Currently pursuing a PhD in Information Technology to further deepen expertise and strategic impact in AI and cybersecurity.

Skills

Security Strategy and Compliance

- Risk Management, Compliance & Regulatory Standards, Third Party Risk, Security Policy Development, Security Convergence

Technical Skills

- Incident Response, Threat Intelligence, Penetration Testing, Vulnerability Management, Security Automation
- Advanced Network Security, Ethical Hacking, Cloud Security

Leadership and Operations

- Crisis Management, Staff Training & Development, Business Continuity/Disaster Recovery

Experience

2021 – PRESENT

Cybersecurity Administrator | Alto Ingredients

- Led comprehensive security assessments aligned with federal standards, improving infrastructure protection across critical sectors.
- Collaborated with federal agencies and cross-functional teams, providing security insights that directly contribute to critical infrastructure protection.
- Drove a 70% reduction in security incidents by leading a cultural transformation to embed a security-first mindset.
- Engineered and deployed an advanced threat detection system, reducing response time and preventing an estimated \$2M in potential losses from cyber-attacks.
- Enhanced security measures, reducing downtime by 30%, directly improving operational efficiency.

2019 – 2021

Customer Engineer | NCR

- Developed security best practices for POS and ATM installations, adopted by 20+ field technicians, reducing unauthorized access attempts by 50%.

- Integrated advanced network security protocols for POS systems, resulting in a dramatic 40% reduction in incident response times and enhancing overall system security compliance by 30% within six months.

2010-2021

Physical Security | EMS | Fire Service

- Leveraged leadership and crisis response skills from emergency medical services and physical security roles to strengthen expertise in risk management and operational oversight.
- Conducted over 30 comprehensive threat assessments annually, resulting in a 40% reduction in physical security breaches and incidents.
- Directed cross-functional teams to respond effectively to emergencies and ensure organizational resilience.
- Enhanced physical security operations through streamlined protocols, benefiting compliance in regulated environments.

Education

EXPECTED 2026 - 2027

PhD in Information Technology (In Progress) | University of the Cumberlands
(Research Focus: Security Convergence & AI in Critical Infrastructure)

February 2024

Masters in Cybersecurity and Information Assurance | Western Governor's University

FEBRUARY 2022

Bachelors in Information Systems and Cybersecurity | Columbia Southern University

Certifications

ISC2 CISSP - Certified Information Systems Security Professional

ISACA CISM - Certified Information Security Manager

CompTIA CASP+ - Certified Advanced Security Practitioner

CompTIA CySA+ - Cybersecurity Analyst

CompTIA PenTest+ - Penetration Testing

Blue Team Level 1 (BTL1) - Defensive Cybersecurity Operations

CompTIA Security+ - Security Fundamentals

ISC2 CC - Certified in Cybersecurity

Tools and Platforms

Offensive Security: Cobalt Strike, Metasploit, BloodHound, Mimikatz, Burp Suite, Kali Linux

Defensive Security: Splunk, Wireshark, Sysmon, CrowdStrike Falcon, SentinelOne, Zeek, OSQuery

Vulnerability & Risk Management: Nessus, Qualys, OpenVAS, CVSS, Tenable

Cloud & Infrastructure: Azure AD, AWS IAM, Terraform, Docker, Kubernetes (basic)

Scripting & Automation: PowerShell, Bash, Python (automation, enumeration, parsing)