Jasen Crisp
Boise, ID

jasencrisp@gmail.com
https://www.crispsec.com
Phone: 208-703-1865

linkedin.com/in/jasencrisp
github.com/Jasen-C

Summary

Security Engineer with 20 years of hands-on technical experience in Information Security, Server and Endpoints, Virtualization, and Networking, with particular expertise in security automation and process optimization. Works well independently, or as part of a larger team of various skill levels, enjoys mentoring and working alongside junior team members. Able to work with different technology partners and business owners to communicate complex problems and solutions to varying levels of technical expertise. Actively pursuing advanced education in Cyber Operations and Resilience while maintaining multiple industry certifications to stay at the forefront of security practices.

Experience

Information Security Engineer

- Develop and implement security automation using PowerShell, Python and Azure Logic Apps to enforce security standards and remediate vulnerabilities at scale
- Design and implement Security Information and Event Management (SIEM) solutions including MS Sentinel, Splunk, and Graylog
- Container and cloud-native application security including Docker vulnerability scanning and reporting using Palo Alto Networks Prisma, collaborating with development teams to communicate findings and implement security best practices
- Identify, classify, research, prioritize, remediate, and report on vulnerabilities, and misconfigurations.
- Identify, document, and update security systems and processes for Attack Surface Management (ASM) and Cloud Security Posture Management (CSPM) tools.
- Assist with the evaluation, testing, design, and implementation of new security technologies.
- Monitor security logs and alerts to identify and respond to technical problems, anomalies, and suspicious activity.
- Build security dashboards to identify changes, anomalies, and trends quickly and accurately.
- Respond to security incidents and coordinate response, containment, forensics, and mitigation.
- Microsoft Advanced Threat Analytics, Entra ID, Exchange, and Office 365 Security configuration and incident response.
- Endpoint Security Administration - Sophos AV, Defender ATP, Intune, and CrowdStrike Falcon.

Work History

Compex Legal Services, Remote, Boise, ID   07/2024 to Present

Senior Systems Engineer

Design, implement, and maintain critical network and system infrastructure with a focus on security enhancement and process automation. Key accomplishments:

- Engineered and deployed an end-to-end automated user lifecycle management system utilizing Jira ticket automation, Azure Logic Apps, and API-driven user provisioning for Entra ID, delivering consistent and repeatable outcomes while reducing processing time by 70% and virtually eliminating human error
- Architect and maintain hybrid cloud infrastructure with emphasis on security compliance and performance optimization

- Lead cross-functional IT projects for system migrations and technology deployments, ensuring minimal disruption to business operations
- Develop comprehensive documentation for network architecture and system configurations to maintain regulatory compliance
- Implement robust security solutions protecting against unauthorized access and potential data breaches

Edgile, a Wipro Company, Remote, Boise, ID   12/2023 to 07/2024

Cybersecurity Architect & Engineer Consultant

Lead a team of security solution consultants in the delivery of major technology projects such as Endpoint Management, Microsoft cloud-centric security solutions. Hands-on configuring complex solutions alongside the delivery teams, providing leadership, and designing, demonstrating, piloting, and testing complex configurations for clients to support decision making.

- Led a team of 6 consultants migrating approximately 350 custom detection rules from SentinelOne to Defender for Endpoint (KQL) in just 2 months, under a tight timeline to support Client's migration off of SentinelOne. Successful delivery of high priority detection rules enabled client to begin EDR migration ahead of schedule.
- Led a team of 2 consultants implementing Azure Defender for Cloud CSPM policies, governance rules, RBAC Role migration, and vulnerability remediations.

Albertsons Companies Inc., Boise, ID   11/2022 to 12/2023

Staff Engineer Cyber Security

Vulnerability and Attack Surface Management

Worked closely with various security engineers, architects, and analysts to design, configure, and implement vulnerability and other product security controls for the Albertsons Companies business portfolios. Primary focus on infrastructure and container vulnerability management and reporting.

- Re-architected Tenable.io network-based vulnerability scans to match network architecture to support scanning 2200+ retail, manufacturing distribution, and office locations.
- Eliminated Major Critical Incidents caused by network-based vulnerability scans from several occurrences a month to 0 for the trailing 8+ months after implementation.
- Managed 70,000+ Tenable Nessus agents and 60 Tenable.io Nessus scanners.
- Remediated issues in Tenable Nessus agent configurations, scans, and deployments reducing 10,000 agents not performing monthly scans to less than 400 regularly. Agent scan coverage improved from 85% to 99% of deployed agents.
- Vulnerability Management SME working with Infrastructure, Developers, and DevOps team members.
- Configured, Deployed, and Managed Axonius - Cybersecurity Asset Attack Surface Management (CAASM) solution.
- Designed and Configured queries and dashboards in the Axonius CAASM tool identifying and reporting gaps in endpoint protection deployments, OS and Application patching.
- Provide Security Engineering Support for Information Security Incident Response on an as-needed basis.

Micron Technology Inc., Boise, ID   7/2022 to 11/2022

Information Security Engineer

Focused on various security technologies within the Technology Development (TD) Intellectual Property (IP) Security team. Participate as Technology Development's IP Security SME on critical initiatives and multi-functional project teams.

Agri Beef Co., Boise, ID   1/2019 to 3/2022
Network Administrator

Security, Systems, and Network Engineer. Primary lead resource on Information Security projects, administration, and incident response. Duties include overseeing all Hyper-V and Window Server Administration. Patch management and software deployments using Ivanti Security Controls and custom PowerShell deployment and automation scripts.

- Designed, configured, and implemented a complete overhaul of Identity and Access Management to transition to a passwordless user experience for all corporate users. Leveraging Azure AD SSO, Microsoft Authenticator App, Windows Hello for Business, and Citrix Cloud SSO with PKI user logon.
- Implemented and maintained internal vulnerability scanning process used to find and remediate vulnerabilities on the enterprise network as well as create hardened base images for rapid server and workstation deployment.
- Automated removing Sophos Anti-Virus and deploying CrowdStrike EDR Sensor via PowerShell. Completed automated no-touch full network deployment over a 2-week rollout.

Commercial Tire Inc, Meridian, ID   12/2017 to 1/2019
IT System Administrator

Supporting all aspects of System Administration, Network Administration, and VOIP Administration for 50 + sites and 600 employees.

Micronet Systems, Boise, ID   4/2015 to 12/2017
Network / System Administrator

Windows System and Network Administrator supporting local small businesses and all aspects of their IT needs.

Education

Boise State University, Boise, ID   2024 to Present
B.A.S., Cyber Operations and Resilience

Portland Community College, Portland, OR   2020 to 2024
A.A.S., Computer Information Systems - Cybersecurity
Graduated: March 2024

Certification

PenTest+, CompTIA, 10/2023 to 10/2026
Security, Compliance, and Identity Fundamentals, Microsoft, 5/2022
CompTIA Security Analytics Professional (CSAP), CompTIA, 10/2020 to 10/2026
Cybersecurity Analyst (CySA+), CompTIA, 10/2020 to 10/2026
Security+, CompTIA, 6/2020 to 6/2026
Azure Fundamentals, Microsoft, 2/2020
Security Fundamentals, Microsoft Technology Associate, 2/2015
Windows Server 2008 Active Directory, Configuring, Microsoft Certified, 11/2012