

Logan Ingram

INFORMATION SYSTEM SECURITY OFFICER

Security clearance; details available upon request.

logan@l-ingram.com | (719) 799-0617

PROFESSIONAL SUMMARY

Cybersecurity engineer with 15+ years of enterprise IT and security experience. Performs ISSO duties spanning RMF/ATO documentation, security control implementation, vulnerability remediation tracking, and incident response. Led compliance efforts that achieved CMMC Level 2 through a C3PAO assessment. Brings hands-on Windows, RHEL, cloud, and container infrastructure experience.

CORE EXPERTISE

Information assurance Risk Management Framework (RMF), Authorization to Operate (ATO), SSPs, POA&Ms, RARs, SCTMs, eMASS, XACTA, CMMC Level 2, NIST SP 800-171

Security operations DISA STIGs, vulnerability assessment and remediation tracking, incident response, security training, SIEM monitoring, access control, CUI protection

Platforms and infrastructure Microsoft Defender, Sentinel, Graylog, Entra ID, Intune, Azure, Windows, RHEL, Hyper-V, VMware, Docker, K3s/Kubernetes

PROFESSIONAL EXPERIENCE

Cyber Security Engineer II

Apr 2025 - Present

Caribou Thunder | Colorado Springs, CO

- Led cybersecurity operations and compliance efforts that achieved CMMC Level 2 through a C3PAO assessment, aligning systems with NIST SP 800-171 and enforcing CUI handling and data loss prevention policies.
- Develop and maintain RMF/ATO documentation, including System Security Plans (SSPs), Plans of Action and Milestones (POA&Ms), Risk Assessment Reports (RARs), and Security Control Traceability Matrices (SCTMs); work with eMASS and XACTA to support authorization activities.
- Use Microsoft Defender vulnerability scanning to identify findings and track remediation; apply DISA Security Technical Implementation Guides (STIGs) to system configuration and hardening.
- Support security incident response and provide security training to reinforce organizational security practices.
- Design Microsoft Sentinel detection and logging pipelines using KQL, Azure Monitor Agent, and data collection rules to improve visibility into user activity and security events.
- Implement and manage identity and endpoint controls across Microsoft 365, Entra ID, and Intune, including Conditional Access, endpoint hardening, and policy enforcement; automate user lifecycle workflows through Microsoft Graph.
- Develop deployment tooling and document procedures for connected and air-gapped Linux environments using Bash, Ansible, Docker, and K3s; troubleshoot RHEL certificate trust, container image access, and deployment issues.

PROFESSIONAL EXPERIENCE CONTINUED

Senior IT Systems Engineer

Nov 2015 - Jan 2025

Diamond Associates, Inc. | Dallas, TX

- Designed and managed cloud and on-premises infrastructure across Azure, Hyper-V, and VMware, implementing hardware VPNs, firewalls, Layer 3 switching, and enterprise Wi-Fi.
- Administered Active Directory, Group Policy, Windows Server, WSUS, Entra ID, and Google Workspace across managed client networks, supporting identity, endpoint, and application services.
- Maintained NIST-based security practices and supported PCI DSS and HIPAA compliance requirements across managed environments.
- Developed custom software and API integrations to streamline technical support and enable secure communication between third-party platforms; coordinated enterprise software and licensing with vendors.
- Led the transition from law firm cost-recovery systems to broader managed IT services, expanding the company's service offerings and business opportunities.

Tier 2 Help Desk Analyst

Jul 2015 - Nov 2015

TEKsystems | Irving, TX

- Delivered Tier 2 technical support and escalation assistance for Tier 1 analysts; coordinated with application support teams to investigate outages and resolve service issues.
- Administered Exchange users, distribution lists, shared mailboxes, and ActiveSync; managed Cisco IronPort web access and email quarantine controls.
- Supported virtual desktops for global clients through Cisco Desktop Director.

CERTIFICATIONS AND TECHNICAL CREDENTIALS

CompTIA Security+ (current) | Network+ | A+

Cisco CCNA | Network Security

TestOut Cyber Defense Pro | Ethical Hacker Pro | PC Pro

EDUCATION

Pikes Peak State College

Bachelor of Applied Science in Cyber Security | Expected Sep 2027

Associate of Applied Science in Cyber Security | Sep 2024

ADDITIONAL TECHNOLOGIES

PowerShell, Python, C#/.NET, Microsoft Graph, Active Directory, Group Policy, WSUS, Windows Autopilot, ThreatLocker, SentinelOne, CrowdStrike, Veeam, WatchGuard, Sophos, Cisco networking, Bash, Ansible, Helm, Atlassian tools