

Joey Crysel

CYBERSECURITY ANALYST

Wetumpka, AL | 334-430-8950 | joey.crysel@protonmail.com
linkedin.com/in/joey-crysel-11b17b219

PROFESSIONAL SUMMARY

Cybersecurity Analyst with more than six years of experience supporting security operations in healthcare and state government environments. Background includes threat detection, incident response, threat hunting, SIEM administration, digital forensics, vulnerability management, and security engineering. Hands-on experience with Microsoft Defender XDR and CrowdStrike Falcon, including EDR, NG-SIEM, Fusion SOAR, Identity Protection, and endpoint security.

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst

Alabama Medicaid Agency

Sep 2026 - Present

- Monitor, triage, and investigate security alerts using Microsoft Defender XDR and CrowdStrike Falcon.
- Analyze security telemetry to validate potential threats, determine scope, and support containment and response activities.

Information Security Engineer II

Baptist Health

Dec 2024 - Aug 2026

- Served as the CrowdStrike subject-matter expert for NG-SIEM, Fusion SOAR, Identity Protection, Firewall Management, and Endpoint Protection.
- Led Tenable Vulnerability Management scanning, prioritization, and remediation coordination.
- Managed ExtraHop NDR detections and escalation workflows using network telemetry and behavioral data.
- Supported Zscaler ZIA/ZPA policy tuning, Cisco ISE secure access controls, and Proofpoint email security monitoring.
- Built the organization's threat intelligence program and produced reporting on healthcare-sector threats and risks.
- Designed digital forensic workflows using Magnet AXIOM, FTK Imager, Autopsy, and Eric Zimmerman tools while maintaining chain of custody.

Systems Analyst I

Oracle Health

Mar 2020 - Dec 2024

- Supported Baptist Health IT Works and CSIRT in enterprise security operations.
- Performed Nessus vulnerability scanning and coordinated remediation using scan results, asset inventories, and vulnerability data.
- Conducted CrowdStrike EDR monitoring, threat triage, and incident response.
- Managed ADFS and Imprivata single sign-on integrations for clinical workflows.
- Administered the PKI/ADCS environment, including certificate enrollment, lifecycle tracking, and supporting records.
- Maintained SCCM patching and endpoint configurations and built VMware vSphere virtual servers.

Network Field Technician

Information Transport Solutions

Oct 2014 - Mar 2020

- Implemented and troubleshot Cisco wireless, routing, switching, and VoIP systems.
- Supported Windows workstations and small-business IT environments.

CORE SKILLS AND TECHNOLOGIES

Security Platforms: Microsoft Defender XDR; CrowdStrike Falcon (EDR, NG-SIEM, Fusion SOAR, Identity Protection); ExtraHop Reveal(x); Zscaler ZIA/ZPA; Proofpoint Email Security

Threat Detection and Response: Alert triage, threat hunting, incident response, security telemetry analysis, detection tuning, threat intelligence enrichment, MITRE ATT&CK

Digital Forensics: Magnet AXIOM, FTK Imager, Autopsy, Eric Zimmerman tools, evidence collection, chain of custody

Vulnerability and Access Management: Tenable, Nessus, Cisco ISE, BeyondTrust PAM/PRA, 802.1X

Infrastructure and Scripting: Active Directory, PKI/ADCS, SCCM, VMware vSphere, PowerShell, Linux CLI, Cisco networking

SELECTED PROJECTS

Enterprise SIEM Migration

Led the migration from AlienVault to CrowdStrike NG-SIEM, consolidating and normalizing log ingestion to improve visibility and detection fidelity.

Security Data Integrations

Onboarded Cisco FTD, Exchange Online, Azure Activity, and Proofpoint CASB telemetry into CrowdStrike NG-SIEM.

Security Automation

Created CrowdStrike Fusion SOAR workflows to automate alert handling and deduplicate recurring ExtraHop alerts.

Network Access Control

Designed and implemented Cisco ISE, including medical-device profiling and secure wired and wireless 802.1X deployment.

Privileged Access Management

Implemented BeyondTrust PAM for administrative access and BeyondTrust PRA for monitored vendor access.

Certificate Authority Upgrade

Designed and deployed a SHA-256 Active Directory Certificate Services infrastructure to replace legacy SHA-1 services.

CERTIFICATIONS

GCTI	GIAC Cyber Threat Intelligence
GCIH	GIAC Certified Incident Handler
GCFA	GIAC Certified Forensic Analyst
GCFE	GIAC Certified Forensic Examiner
BTL1	Security Blue Team Level 1
Security+	CompTIA

EDUCATION

Associate Degree in Computer Information Systems

May 2014

Trenholm State Community College

Related coursework: Cisco Networking Academy