Cole Antognoni

Melbourne, FL | coleantognoni@gmail.com | 619-204-3606

Professional Summary

Cybersecurity professional with federal clearance and hands-on experience in vulnerability management, patching, and security operations. Skilled in remediation workflows, SIEM monitoring, and incident response using enterprise tools including BigFix, SCCM, Splunk, and IAM platforms (AWS IAM, Okta, Keycloak). Experienced in building security dashboards, automating remediation processes, and supporting compliance initiatives across enterprise environments. Currently advancing offensive security skills through labs and certifications (eJPT/PNPT) with the long-term goal of transitioning into penetration testing and red team roles.

Core Skills

Vulnerability Management: Nessus, Tenable, BigFix, SCCM, Risk Register

Security Operations & IR: Splunk, log analysis, escalation workflows, event triage

Threat Analysis & Reporting: Threat prioritization, remediation tracking, SOP documentation

Identity & Access Management: Okta, AWS IAM, Keycloak

Automation & Tools: Jira, Jenkins, GitHub, scripting for remediation automation

Systems & Networking: Windows Server, O365, Cloud Services, LAN/WAN fundamentals

Professional Experience

Vulnerability Management Analyst | Leidos (1901 Group) | Aug 2023 – Present

Contributed to vulnerability scanning and validation using Tenable/Nessus to support remediation across 500+ enterprise systems.

Designed and executed security patch deployments with BigFix/SCCM, driving a 40% reduction in critical vulnerabilities.

Partnered with penetration testing teams to review findings, validate exploitability, and communicate risks to stakeholders.

Produced security metrics and dashboards to brief leadership on remediation progress and compliance posture.

Tier 2 Security Solutions Analyst | Leidos | Oct 2022 – Aug 2023

Developed Splunk queries and detection logic to identify anomalous behavior and escalate confirmed threats.

Engineered monitoring dashboards and automated workflows in Jira, reducing incident response time for critical alerts.

Conducted log analysis across Windows and Linux systems to detect potential indicators of compromise.

Provided technical support for secure API integrations and incident escalations.

Service Desk Agent | Leidos | Jun 2021 – Oct 2022

Implemented and maintained secure IAM processes across AWS, Okta, Jenkins, and cloud services.

Monitored abnormal account activity and escalated incidents to SOC for investigation.

Tested and validated security tools prior to enterprise deployment to ensure operational readiness.

Desktop Support Technician | Constellium | Jul 2019 – Sep 2020

Applied endpoint hardening and patching with SCCM to ensure compliance with enterprise security standards.

Delivered technical support to executive staff, ensuring confidentiality and system uptime.

IT Technician (DOE Contracts) | ActioNet | Jan 2018 – Jun 2019

Provided secure IT support for Department of Energy systems and applications.

Maintained accurate reporting for telecom and network inventory audits using Excel and SCCM.

Education

B.S. in Computer Science – Cybersecurity (In Progress, Expected 2026) | Eastern Florida State College

A.A. Degree | Frederick Community College, 2017

Certifications

CompTIA Security+ (2024)

eJPT (in progress, expected 2026)

PNPT (planned, expected 2027)