

Avery Castillo

IT Specialist (INFOSEC)

Kansas City, MO · avery.castillo@example.com · (555) 555-0117 · U.S. citizen

SUMMARY

Information security specialist with more than eight years in IT, including four years at GS-11 running security authorization, vulnerability management and incident response for federal systems. CISSP certified, with a record of explaining risk in plain terms to system owners and managers. Seeking a GS-2210-12 IT Specialist (INFOSEC) position.

WORK EXPERIENCE

IT Specialist (INFOSEC)

03/2022 – Present

U.S. Department of Veterans Affairs, Office of Information and Technology, Kansas City, MO

GS-2210-11 · 40 hours per week

- Lead the Risk Management Framework process for 14 systems: categorize each system, tailor NIST SP 800-53 controls, assess them and assemble the authorization package; all 14 received a 3-year authorization to operate.
- Run weekly authenticated Tenable.sc scans of 2,300 servers and workstations; cut the average age of critical vulnerabilities from 41 to 12 days by agreeing remediation deadlines with 6 system owner teams.
- Built Splunk correlation searches and dashboards for privileged account activity; detected and contained 2 credential misuse incidents in FY2025, both reported within the 1-hour requirement.
- Serve as incident handler for the regional response team: triage alerts, preserve evidence, write incident reports and brief the ISSO and CIO staff on root cause and corrective actions.
- Manage 96 plan of action and milestones (POA&M) items across 14 systems; closed 71 in 18 months and keep the rest current in the agency GRC tool for quarterly FISMA reporting.
- Wrote the office's Windows Server 2022 security baseline from CIS Benchmarks; compliance rose from 68% to 94% across 410 servers in 9 months.
- Review proposed changes for security impact at the weekly change advisory board and advise project teams on encryption, logging and access control requirements.

Systems Administrator

06/2018 – 02/2022

Northgate Health Systems, Overland Park, KS

40 hours per week

- Administered 180 Windows and Linux servers and Active Directory for 2,400 users at 5 hospitals; clinical systems stayed at 99.95% availability for 3 years.
- Automated patching with WSUS and PowerShell, cutting the monthly patch cycle from 10 days to 3.
- Rolled out multifactor authentication for remote access to all 2,400 users and supplied evidence for the annual HIPAA security risk assessment.
- Sent logs from 180 servers to the hospital SIEM and wrote the alert runbook used by the 4-person operations team.
- Restored the patient scheduling system within its 4-hour recovery objective after a 2021 storage failure, using recovery steps I had documented.

IT Support Technician (part-time)

09/2016 – 05/2018

Brightwater Community Bank, Lee's Summit, MO

20 hours per week

- Resolved about 40 help desk tickets a week for 3 branches and imaged and deployed 120 workstations.
- Set up accounts, permissions and laptop encryption for new staff under the bank's access control policy.

EDUCATION

Bachelor of Science, Cybersecurity

05/2018

University of Central Missouri · GPA 3.5/4.0

- Capstone: built a network intrusion detection lab with Security Onion

CERTIFICATIONS AND TRAINING

Certified Information Systems Security Professional (CISSP), ISC2	06/2023
CompTIA Security+, CompTIA	08/2018
Splunk Core Certified Power User, Splunk	02/2024
Hacker Tools, Techniques, and Incident Handling (SEC504), SANS Institute	10/2023

SKILLS

Security frameworks: NIST Risk Management Framework, NIST SP 800-53 Rev. 5, FISMA reporting, CIS Benchmarks

Tools: Tenable.sc and Nessus, Splunk, Microsoft Defender for Endpoint, PowerShell, Python

Systems: Windows Server, Red Hat Enterprise Linux, Active Directory, VMware vSphere

ADDITIONAL INFORMATION

- Background investigation: Tier 4 public trust, favorably adjudicated 2022
- Awards: Special Contribution Award, 2024, for the Windows Server security baseline
- Languages: Spanish (professional working proficiency)
- Professional organizations: ISC2 member