Leo Pitts

Senior Cyber Security Engineer

(719) 555-0148 | leo.pitts@protonmail.com | linkedin.com/example/leopitts | Colorado Springs, CO 80903

STRENGTHS

Zero Trust Integration
Connected Microsoft visibility and automation signals across enclaves; customer teams gained clearer paths from detection through action.

RMF Leadership
When authorization reviews became demanding, organized artifacts and evidence so ISSOs could answer assessors with confidence.

Security Automation
Built Python, PowerShell, and Bash utilities for recurring checks; engineers gained repeatable reviews instead of manual rework.

Technical Communication
Translated workflow health and residual risk into practical briefings, helping government stakeholders make timely decisions.

Team Development
Mentored four engineers through testing, documentation, and customer communication; peers became more consistent during compliance reviews.

SKILLS

Microsoft Sentinel

Microsoft Defender

Microsoft Purview | Microsoft Entra

Logic Apps | UEBA | SOAR

Behavior Analytics | Splunk | RMF

ATO Lifecycle | DISA STIG

Zero Trust Guidance | Windows

Unix

SUMMARY

Senior Cyber Security Engineer with 14+ years supporting enterprise security engineering, Microsoft environments, **Zero Trust** programs, and Department of Defense compliance. Leads **Microsoft Sentinel**, Defender, Purview, Entra, Logic Apps, UEBA, SOAR, and **behavior analytics** initiatives across Windows and Unix infrastructure. Delivers Tier 3 and Tier 4 support, telemetry integration, workflow tuning, RMF artifacts, ATO lifecycle execution, DISA STIG assessments, control evidence, and assessor coordination. Works closely with ISSOs, **cybersecurity assessors**, system owners, customer representatives, and engineering teams to turn guidance into practical controls and reliable operations. Python, PowerShell, and Bash automation improves recurring reviews and evidence collection. Active DoD TS/SCI clearance and CISSP certification support mission-focused work. Ready to help advance Zero Trust integration, automation, visibility, and product quality for Northstar Defense Analytics.

EXPERIENCE

Principal Cyber Security Engineer

Red Mesa Federal Systems | March 2023 - Present | Colorado Springs, CO

Directs **Microsoft security engineering** across a multi-enclave defense environment, connecting visibility, analytics, automation, identity, data protection, and Zero Trust objectives. Leads RMF and ATO delivery, technical assessments, engineering automation, stakeholder briefings, and Tier 3 and Tier 4 support.

- Connected Sentinel, Defender, Entra, Purview, and **Logic Apps** telemetry across multi-enclave Zero Trust operations.
- Tuned **UEBA** and **SOAR** workflows with analysts, preserving high-risk account detections during alert refinement.
- Governed RMF artifacts and ATO milestones through evidence reviews with ISSOs and cybersecurity assessors.
- Assessed **Windows**, Unix, network appliances, and enclave services against **DISA STIG** requirements and documented remediation.
- Built Python and PowerShell utilities for telemetry validation, evidence collection, and recurring configuration checks.
- Presented workflow health, open findings, and delivery trends to government stakeholders and support contracts.

Senior Cybersecurity Engineer

Blue Canyon Mission Technologies | January 2020 - February 2023 | Aurora, CO

Managed Microsoft security operations for sensitive mission applications and distributed users. Built analytics and automation, coordinated **RMF** evidence, supported platform transition work, applied DISA STIG guidance, and mentored engineers through recurring compliance and customer reviews.

- Managed Sentinel, Defender, Entra, and Windows security operations supporting sensitive mission applications and distributed users.
- Built Sentinel rules, workbooks, and **Logic Apps** playbooks for credential misuse and privilege anomalies.
- Mapped security requirements to RMF controls, assembled **ATO evidence**, and maintained traceable **POA&M** updates.
- Converted **DISA STIG** findings into prioritized remediation tickets with validation steps for administrators.
- Integrated **Splunk** use cases with Microsoft telemetry, preserving visibility during a platform transition.
- Mentored four engineers on workflow testing, evidence quality, incident documentation, and customer communications.

Cyber Security Engineer

Ironwood Secure Networks | June 2017 - December 2019 | Albuquerque, NM

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Principal Cyber Security Engineer at Red Mesa Federal Systems (3.5 Years)
- Senior Cybersecurity Engineer at Blue Canyon Mission Technologies (3.1 Years)
- Cyber Security Engineer at Ironwood Secure Networks (2.5 Years)
- Information Systems Security Engineer at Cobalt Ridge Defense Services (2.8 Years)
- Cybersecurity Analyst at Pioneer Mission Support (2 Years)

Administered Microsoft enterprise security services across Windows and hybrid identity environments. Supported endpoint protection, access governance, centralized monitoring, telemetry validation, scripting, STIG reviews, RMF evidence, **behavior analytics**, and technical risk reporting.

- Administered Microsoft security services across Windows and hybrid identity environments supporting access governance.
- Configured Sentinel connectors and Defender policies, then validated telemetry through controlled test events.
- Created **Bash** and **Python** scripts comparing hardened configurations with DISA STIG expectations for infrastructure owners.
- Maintained RMF documentation and evidence packages for cybersecurity assessor review and authorization milestones.
- Correlated Entra, endpoint, and network data during privileged-account behavior investigations before containment recommendations.
- Presented monthly security trends and technical risks to system managers with practical remediation priorities.

Information Systems Security Engineer

Cobalt Ridge Defense Services | August 2014 - May 2017 | San Antonio, TX

Supported ISSOs and system administrators across Windows and Unix enclaves subject to DoD controls, configuration baselines, and authorization reviews. Maintained RMF packages, performed host and network assessments, defined monitoring use cases, and prepared teams for assessors.

- Supported **ISSOs** and administrators across Windows and **Unix** enclaves subject to DoD security controls.
- Performed host and network assessments using STIG checklists, vulnerability reports, and configuration evidence.
- Maintained security plans, control narratives, risk registers, and POA&M records through ATO milestones.
- Normalized Windows event data and defined monitoring use cases for authentication, malware, and privilege activity.
- Coordinated assessor requests with system owners, database administrators, and network teams before formal reviews.
- Drafted account review and configuration-change procedures, giving junior staff repeatable compliance guidance.

Cybersecurity Analyst

Pioneer Mission Support | July 2012 - July 2014 | San Antonio, TX

Monitored enterprise security events across Windows and Unix systems while supporting vulnerability reviews, RMF evidence collection, Microsoft security administration, scripting, and operational reporting. Built an early foundation in incident procedures, STIG validation, and customer-facing security communication.

- Monitored Windows and Unix security events, escalating suspicious authentication and malware activity under procedures.
- Performed vulnerability and configuration reviews against **DISA STIG** requirements for senior engineering review.
- Collected RMF evidence from administrators and organized artifacts by control family for authorization packages.
- Used **PowerShell** and Bash to validate service status, security settings, and log forwarding.
- Reviewed access groups, endpoint policies, and event collection health with Microsoft system owners.
- Prepared weekly summaries showing open findings, aging tickets, and upcoming assessment activities.

PROJECTS

Zero Trust Visibility Integration | 2025

Integrated Microsoft Sentinel, Defender, Entra, Purview, and Logic Apps signals into a multi-enclave visibility and automation model. Refined UEBA and SOAR workflows with analysts, giving customer teams clearer risk signals and more consistent response paths.

RMF Authorization Modernization 2023

Standardized RMF artifacts, control evidence, assessor responses, and ATO milestone tracking across infrastructure changes. The work gave ISSOs and system owners a clearer review rhythm and stronger traceability from requirements through residual risk.

Microsoft-Splunk Operations Transition 2022

Connected selected Splunk security use cases with Microsoft telemetry during a platform transition. Preserved operational visibility, clarified triage ownership, and gave analysts a practical path for consistent escalation.

LEADERSHIP & AWARDS

- Mission Support Excellence Award, 2024
- Customer Technical Impact Award, 2021
- Security Operations Innovation Recognition, 2018

EDUCATION

Bachelor's Degree in Cybersecurity

University of Texas at San Antonio GPA: 3.5 2012 San Antonio, TX

Coursework: *Information Assurance, Network Security, Digital Forensics, Risk Management*

CERTIFICATIONS

- CISSP, (ISC)² 2018
- Microsoft Certified: Security Operations Analyst Associate, SC-200 2022
- Microsoft Certified: Cybersecurity Architect Expert, SC-100 2024
- DoD 8570 IAT Level III / DoW 8140 Advanced Certification Alignment 2024

TECHNICAL SKILLS

- **Microsoft Security:** Microsoft Sentinel, Microsoft Defender, Microsoft Purview
- **Identity Platforms:** Microsoft Entra, hybrid identity, access governance
- **Automation Platforms:** Logic Apps, SOAR, workflow orchestration
- **Analytics Engineering:** UEBA, behavior analytics, Sentinel workbooks
- **Compliance Frameworks:** RMF, ATO lifecycle, control evidence
- **DoD Standards:** DISA STIG, DoD 8570, DoW 8140
- **Zero Trust Guidance:** DoW guidance, NSA guidance, USSOCOM SOFNET
- **Operating Systems:** Windows, Unix, Windows Server
- **Programming Languages:** Python, Bash, PowerShell
- **Security Operations:** Tier 3 support, Tier 4 support, incident triage
- **SIEM Use Cases:** Splunk, analytics rules, security use cases
- **Infrastructure Assessment:** Vulnerability assessment, network assessment, host assessment

PROFESSIONAL AFFILIATIONS

- Cybersecurity Mentor, Colorado Springs Security Professionals Network, March 2023 - Present
- RMF Knowledge-Sharing Facilitator, Federal Security Engineering Community, January 2020 - December 2023
- Volunteer Presenter, Rocky Mountain Cyber Defense Forum, 2019 - 2022

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST