Manuel Moss

Security Engineer 5, Workforce Security

(512) 555-7318 | manuel.moss@example.com | linkedin.com/example/manuelmoss | Austin, TX 78704

STRENGTHS

Risk translation
Turned technical endpoint findings into clear business choices, helping partners act without losing sight of user needs.

Control delivery
Moved ambiguous security concerns from discovery through tested rollout, and kept stakeholders aligned during difficult decisions.

Exploit analysis
Validated public exploits in controlled settings and studied related variants, giving remediation teams sharper evidence.

Customer empathy
Listened closely to workforce needs during hardening work, which made safer controls easier for teams to adopt.

Cross functional trust
Worked with engineering, IT, identity, data, procurement, and vendors until security choices had shared ownership.

SKILLS

Endpoint Security

Workforce Security | Mac

Windows | Linux | Jamf | Kandji

Intune | CrowdStrike | Tenable

Host Hardening

Vulnerability Management

Patch Management

Threat Modeling

Threat Intelligence

SUMMARY

Senior workforce and **endpoint security** engineer with 14 years of progressive experience securing Mac, **Windows**, and Linux environments. Leads ambiguous security initiatives from risk discovery through validated control rollout, with hands on work across Jamf, Kandji, Intune, CrowdStrike, and Tenable. Builds host hardening baselines, patch and vulnerability strategies, **configuration drift prevention**, threat models, exploit validation methods, and variant analysis workflows. Connects endpoint, identity, data, SaaS, vendor, and emerging genAI risks with practical business decisions. Partners with engineering, IT, procurement, identity, data, and vendor teams through clear requirements, **cost benefit analysis**, development estimates, testing, and operational support. Brings customer empathy, sound judgment, measurable prioritization, and incident response experience to workforce security programs.

EXPERIENCE

Principal Endpoint Security Engineer

Redwood Collaboration Systems | January 2023 - Present | Austin, TX

Owns workforce endpoint security initiatives across Mac, Windows, and Linux. Leads risk discovery, control design, validation, delivery planning, stakeholder review, and **operational support** for endpoint, SaaS, vendor, and genAI enabled workflows.

- Turned ambiguous endpoint risk into sequenced initiatives using threat models and measurable control outcomes.
- Built Jamf, Kandji, and Intune baselines that reduced drift across **Mac**, Windows, and **Linux** fleets.
- Prioritized **OS**, application, and configuration remediation through CrowdStrike, Tenable, and **threat intelligence**.
- Validated public exploits in controlled environments, then mapped variants to related endpoint exposure.
- Compared build and buy options through requirements, **cost analysis**, estimates, testing, and stakeholder review.

Senior Security Engineer, Endpoint Protection

Blue Mesa Software | May 2019 - December 2022 | Denver, CO

Directed endpoint protection work across diverse workforce fleets, connecting vulnerability data, hardening standards, threat intelligence, and business risk. Guided delivery from early exposure analysis through testing, rollout, measurement, and production support.

- Reframed **workforce security** concerns into delivery plans with clear owners, milestones, and risk measures.
- Validated **host hardening** controls through Jamf, **Kandji**, and Intune across three operating systems.
- Used **CrowdStrike** detections and Tenable findings to shape patch priorities for business applications.
- Tested disclosed exploits and reviewed variants, giving engineering teams clearer remediation decisions.
- Applied **threat modeling** to SaaS, vendor, endpoint, and **genAI** workflows during control reviews.

Security Engineer

Lone Star Commerce Labs | July 2016 - April 2019 | Dallas, TX

Supported **endpoint security** architecture and vulnerability operations for workforce technology. Combined control testing, exploit research, scripting, **metrics**, and stakeholder communication to move security work from findings into practical remediation.

- Converted endpoint findings into actionable remediation plans through risk scoring and stakeholder workshops.
- Created hardening checks for Mac, Windows, and Linux, then reviewed drift during release cycles.
- Correlated **Tenable** exposure with **threat intelligence** to focus patch work on credible attack paths.

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Principal Endpoint Security Engineer at Redwood Collaboration Systems (3.7 Years)
- Senior Security Engineer, Endpoint Protection at Blue Mesa Software (3.6 Years)
- Security Engineer at Lone Star Commerce Labs (2.8 Years)
- Information Security Analyst at Prairie Cloud Services (3 Years)
- Systems Security Specialist at Heartland Network Solutions (11 Months)

- Reproduced public exploit behavior in isolated testing environments and documented affected variants.
- Used Python, **PowerShell**, and **shell scripting** to simplify recurring security validation tasks.

Information Security Analyst

Prairie Cloud Services June 2013 - June 2016 Omaha, NE

Analyzed workforce endpoint exposure, supported patch operations, and helped mature **security controls** across cloud connected business environments. Delivered evidence, **metrics**, and practical recommendations for engineering, IT, and vendor partners.

- Built vulnerability views that helped IT sequence operating system and application remediation work.
- Checked endpoint configuration against hardening expectations across Mac, **Windows**, and Linux systems.
- Used **threat intelligence** to add context around exposed software and prioritize investigation queues.
- Documented exploit validation results and variant observations for senior security review.
- Supported **incident response** investigations with endpoint evidence, clear notes, and timely escalation.

Systems Security Specialist

Heartland Network Solutions June 2012 - May 2013 Lincoln, NE

Provided foundational systems security support for endpoint operations, vulnerability review, configuration checks, and incident handling. Learned to connect technical findings with service continuity and user needs.

- Reviewed endpoint weaknesses and organized remediation tasks with systems and support teams.
- Applied baseline checks to **Windows** and Linux hosts during routine security assessments.
- Tracked patches, exceptions, and configuration changes for clearer operational follow through.
- Collected host evidence during incidents and prepared concise findings for escalation.
- Answered user security concerns with practical guidance that supported safer daily workflows.

PROJECTS

GenAI Workforce Risk Assessment 2025

Mapped genAI enabled workforce workflows, identified endpoint and data risks, and compared control options through threat modeling, requirements review, and measurable risk decisions.

Cross Platform Hardening Validation 2024

Validated host hardening controls across Mac, Windows, and Linux, using management platforms, drift checks, exploit research, and remediation evidence for operational review.

LEADERSHIP & AWARDS

- 2024, Earned GIAC Certified Incident Handler recognition after completing advanced incident response certification requirements.
- 2021, Earned Certified Information Systems Security Professional credential, reflecting sustained security leadership and technical practice.
- Selected by engineering and IT partners as a trusted reviewer for endpoint risk decisions and control trade offs.

EDUCATION

Bachelor's Degree in Information Systems

University of Nebraska-Lincoln GPA: 0 2012 Lincoln, NE

Coursework: *Information Security, Systems Analysis, Database Management, Network Administration*

CERTIFICATIONS

- GIAC Certified Incident Handler (GCIH) 2024
- Certified Information Systems Security Professional (CISSP) 2021

TECHNICAL SKILLS

- **Endpoint Management:** Jamf, Kandji, Intune
- **Endpoint Detection:** CrowdStrike, Tenable, endpoint telemetry
- **Operating Systems:** Mac, Windows, Linux
- **Host Hardening:** Security baselines, configuration checks, drift prevention
- **Vulnerability Management:** OS assessment, application assessment, remediation tracking
- **Patch Management:** OS patches, application patches, configuration updates
- **Threat Analysis:** Threat intelligence, exploit validation, variant analysis
- **Security Modeling:** Threat modeling, risk scoring, control sizing
- **Security Scripting:** Python, PowerShell, shell scripting
- **GenAI Security:** GenAI assisted scripting, genAI threat review, workflow analysis
- **Incident Response:** Incident handling, endpoint evidence, escalation
- **Security Planning:** Requirements gathering, cost benefit analysis, effort estimates

PROFESSIONAL AFFILIATIONS

- Professional security community participant focused on endpoint protection, vulnerability management, and incident response.
- Workforce technology partner supporting practical security conversations across engineering, IT, identity, data, and procurement teams.

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST