ROADMAP

Sysadmin to Security Engineer

A practical roadmap for system administrators moving into security engineering roles

You already manage infrastructure, troubleshoot incidents and understand how systems fail. This roadmap shows you how to reposition that experience into security engineering, what new skills you need, and how to build proof that employers recognise.

For	Sysadmin
Stage	Mid Career
Topic	System Administration To Security Engineering Transition

Where you are now

You manage servers, networks and cloud infrastructure. You handle user access, patch systems, troubleshoot outages and keep services running. You have dealt with compromised accounts, suspicious activity and the aftermath of security incidents. You understand how systems connect, where they break and what happens when something goes wrong. That operational knowledge is the foundation security engineering is built on.

Typical titles: System Administrator, Senior System Administrator, Infrastructure Administrator, Windows System Administrator, Linux System Administrator, Cloud Administrator, IT Administrator, Systems Engineer

What already transfers

— Incident response instinct: you already investigate suspicious behaviour, trace access patterns and recover from compromise. Security engineering formalises what you do under pressure.

— Infrastructure knowledge: you understand identity systems, network segmentation, logging, privilege escalation paths and where configuration drift creates risk.

— Automation capability: you write scripts to deploy, configure and audit systems. Security engineering uses the same skills to enforce controls and detect drift.

— Troubleshooting methodology: you know how to read logs, correlate events and work backwards from symptoms to root cause. That is how security investigations work.

— Vendor and tool experience: you have worked with Active Directory, firewalls, endpoint management, backup systems and monitoring tools. Security engineers secure and audit those same platforms.

— Change management discipline: you understand the risk of uncontrolled changes and the value of documentation. Security architecture depends on both.

— Communication across technical levels: you explain technical problems to non-technical stakeholders and translate business requirements into infrastructure decisions. Security engineers do the same with risk.

What is missing

- Threat modelling: understanding how attackers think, what they target and how defences fail under real-world conditions.
- Security architecture patterns: designing systems that are secure by default, applying defence in depth and understanding where controls belong in a stack.
- Compliance frameworks: mapping technical controls to SOC 2, ISO 27001, HIPAA, NIST or CIS requirements and producing evidence that auditors accept.
- Cloud-native security: securing identity in Azure Entra ID or AWS IAM, applying least privilege at scale, using policy-as-code and understanding shared responsibility boundaries.
- DevSecOps integration: embedding security into CI/CD pipelines, scanning infrastructure-as-code for misconfigurations and automating security testing.
- Offensive perspective: understanding common attack techniques, reading vulnerability reports and knowing what exploitation looks like in logs.

- Risk communication: translating technical vulnerabilities into business impact, prioritising remediation and presenting findings to executives and auditors.
- Security tooling depth: moving beyond basic familiarity with SIEM, EDR, vulnerability scanners and configuration management to designing detection rules, tuning alerts and interpreting results.

The pathway

PHASE 1 · 1–2 months

Phase 1: Reframe your existing work as security work

You are already doing security work. You lock down privileged accounts, investigate suspicious logins, harden configurations and respond to incidents. The gap is not capability — it is how you describe it. This phase is about repositioning your experience in security terms and filling the small knowledge gaps that make the difference in interviews.

— Audit your current environment using CIS Benchmarks or Microsoft Secure Score. Document what you find, prioritise fixes and implement the top ten. This is a security assessment.

— Review your last three incidents involving compromised accounts, malware or suspicious access. Write them up as incident response cases: timeline, indicators, containment actions, root cause and remediation.

— Take responsibility for one security improvement project: enforce MFA across your organisation, implement conditional access policies, deploy endpoint detection or harden your cloud identity configuration.

— Learn basic threat modelling. Pick one critical system you manage and map out how an attacker could compromise it: entry points, privilege escalation paths, lateral movement and data exfiltration routes.

— Study one compliance framework relevant to your industry. Read the control requirements, map them to your current infrastructure and identify gaps. Write a short remediation plan.

— Start reading security incident write-ups and breach reports. Understand what attackers did, what defences failed and what detection would have looked like.

> *Done when: A documented security assessment with prioritised findings, three incident write-ups in your portfolio and one completed security project you can discuss in detail.*

PHASE 2 · 3–4 months

Phase 2: Build cloud security and automation capability

Security engineering roles expect you to secure cloud infrastructure, automate controls and integrate security into deployment pipelines. If your current role is primarily on-premises or manual, this is where you close that gap. Focus on one cloud platform and go deep rather than surface-level familiarity with several.

- Pick Azure or AWS based on your current environment or local job market. Learn identity and access management in depth: roles, policies, conditional access, service principals and least privilege at scale.
- Deploy a secure reference architecture in your chosen cloud: network segmentation, logging to a SIEM, identity controls, encrypted storage and policy enforcement. Document every security decision.
- Learn infrastructure-as-code with Terraform or Bicep. Write modules that deploy secure-by-default configurations: no public access, encryption enabled, logging configured and least privilege applied.
- Set up a CI/CD pipeline that scans infrastructure code for security issues before deployment. Use tools like Checkov, tfsec or Microsoft Defender for Cloud to catch misconfigurations early.
- Automate a security control you currently manage manually: user access reviews, configuration drift detection, certificate expiry monitoring or security baseline enforcement.
- Work through real-world cloud security scenarios: investigate a compromised service principal, trace lateral movement through role assignments, analyse CloudTrail or Azure Activity logs and recover from a misconfigured public storage bucket.
- If your organisation uses Microsoft 365, run a Secure Score review, implement the top recommendations and document the security uplift. This is portfolio-ready evidence.

> *Done when: A working secure cloud environment you built and can demonstrate, infrastructure-as-code in a public GitHub repository and one automated security control you designed and deployed.*

PHASE 3 · 2–3 months

Phase 3: Develop security architecture and advisory skills

Security engineers are expected to design controls, advise on architecture decisions and communicate risk to non-security stakeholders. This phase is about moving from implementing security to designing it and explaining why it matters.

- Design a security architecture for a realistic scenario: a SaaS application moving to the cloud, a merger requiring identity integration or a compliance-driven infrastructure upgrade. Produce a diagram and a written design document.
- Learn to read and write threat models. Use STRIDE or PASTA to analyse a system you know well. Identify threats, map them to controls and document residual risk.
- Study one offensive security domain enough to think like an attacker: common web application vulnerabilities, Active Directory attack paths, cloud privilege escalation techniques or phishing and initial access methods.
- Practice explaining technical security issues in business terms. Take a vulnerability or misconfiguration you have found and write two versions: one for a technical team and one for an executive.
- Review a real security architecture from your current or a previous employer. Identify weaknesses, single points of failure and missing controls. Write a remediation roadmap with prioritised phases.
- Contribute to a security decision at work: advise on a vendor selection, review a proposed architecture change for security implications or help scope a compliance project.
- Understand one compliance framework in depth: read the controls, study real-world audit evidence and learn what assessors look for. If possible, support an audit or assessment.

> *Done when: A security architecture design document in your portfolio, a written threat model for a real system and evidence of advisory work or compliance involvement you can discuss in interviews.*

PHASE 4 · 1–2 months

Phase 4: Position yourself and start applying

You now have the skills, the proof and the experience. The final phase is about positioning your background effectively, targeting the right roles and performing well in security engineering interviews.

- Rewrite your CV and LinkedIn profile in security terms. Lead with security projects, incident response work and architecture contributions. Quantify impact where possible: systems secured, incidents resolved, compliance gaps closed.
- Build a portfolio site or GitHub repository showcasing your best work: security assessments, architecture diagrams, infrastructure-as-code, automation scripts and incident write-ups. Make it easy for hiring managers to see proof.
- Target roles that value your infrastructure background: cloud security engineer, Microsoft 365 security engineer, security architect, DevSecOps engineer or compliance-focused security roles.
- Prepare for security engineering interviews. Practice explaining your incident response process, walking through a security architecture you designed and discussing how you would secure a system from scratch.
- Study common interview scenarios: how would you investigate a compromised account, design secure access for a third-party vendor, respond to a ransomware incident or implement zero trust architecture.
- Network strategically: engage with security professionals on LinkedIn, contribute to relevant discussions and reach out to people in roles you are targeting. Many security positions are filled through referrals.
- Apply consistently. Expect initial rejections — hiring managers often overlook sysadmin backgrounds for security roles. Your portfolio and specific project examples will differentiate you.

> *Done when: An updated CV and LinkedIn profile positioned for security roles, a portfolio with at least three substantial projects and active applications to security engineering positions.*

Portfolio projects

- A documented security assessment of a real environment: findings, risk ratings, remediation recommendations and evidence of fixes implemented. Use CIS Benchmarks or a similar standard as your baseline.
- A secure cloud reference architecture you built: network design, identity controls, logging configuration and policy enforcement. Include infrastructure-as-code and a design document explaining your decisions.
- Three incident response write-ups from real cases you handled: compromised accounts, malware infections or suspicious access. Include timeline, investigation steps, containment actions and lessons learned.
- An automated security control: a script or pipeline that enforces a security policy, detects configuration drift or audits access. Show the code and explain the problem it solves.
- A threat model for a system you know well: identify attack paths, map threats to controls and document residual risk. Use STRIDE or another recognised framework.

— A security improvement project: MFA rollout, conditional access implementation, endpoint hardening or compliance remediation. Document the before state, what you changed and the measurable outcome.

— A written security architecture proposal: design a secure solution for a realistic scenario, produce a diagram and explain your control choices. This demonstrates advisory capability.

Certification options

Certification	When it makes sense
CompTIA Security+	Early in your transition, if you lack formal security credentials. Covers foundational security concepts and is widely recognised. Useful if you need to demonstrate baseline knowledge, but your practical experience may be more valuable.
Microsoft Certified: Security Operations Analyst Associate	If you work in a Microsoft environment and want to focus on threat detection and incident response. Covers Microsoft Defender, Sentinel and security operations. Directly applicable if you are moving into Microsoft 365 or Azure security roles.
Microsoft Certified: Azure Security Engineer Associate	If you are targeting cloud security roles in Azure environments. Demonstrates capability in securing Azure infrastructure, identity and data. Strong choice if your current work involves Azure.
AWS Certified Security – Specialty	If you are targeting cloud security roles in AWS environments. Covers AWS security services, identity management and compliance. Choose this if your organisation or target employers use AWS heavily.
Certified Information Systems Security Professional (CISSP)	Mid-transition or after landing your first security role, if you want to move toward senior or architecture positions. Requires five years of security experience, but sysadmin work can count toward some domains. Recognised globally and valuable for career progression.
GIAC Security Essentials (GSEC)	If you want a vendor-neutral security certification with more depth than Security+. Covers practical security skills and is respected in the industry. More expensive than CompTIA, but demonstrates hands-on capability.

Roles this opens

→ Cloud Security Engineer

→ Security Engineer

→ Microsoft 365 Security Engineer

→ Azure Security Engineer

→ DevSecOps Engineer

→ Security Architect (junior or mid-level)

→ Infrastructure Security Engineer

→ Compliance Security Engineer

Next steps

→ Audit your current environment this week using CIS Benchmarks or Microsoft Secure Score. Document findings and start fixing the highest-priority issues.

→ Write up your most recent security incident as a formal incident response case. Include timeline, investigation steps and remediation. Add it to your portfolio.

→ Pick one security improvement project you can own in your current role: MFA enforcement, conditional access, endpoint hardening or configuration baseline. Start it this month.

→ Choose Azure or AWS and deploy a secure reference architecture in your own subscription. Use infrastructure-as-code and document every security decision.

→ Rewrite your CV to lead with security work: incidents you handled, systems you hardened, compliance gaps you closed. Quantify impact where possible.

→ Build a portfolio site or GitHub repository. Add your security assessment, incident write-ups and any automation or infrastructure-as-code you have built.

→ Start applying to security engineering roles. Target positions that value infrastructure experience: cloud security, Microsoft 365 security, DevSecOps or compliance-focused roles.

> *Your infrastructure experience is the foundation security engineering is built on. The gap is smaller than you think — start building proof this week.*

More free resources and training at nandycybersuccess.com