IT Security Essentials

Technical security training for IT professionals

CosmicBytez Labs • Security Awareness Training • 2026

Notes: Welcome IT staff. This deck covers the 6 IT-focused modules that build on the end-user fundamentals.

Module 9: Incident Response Basics

- IR Lifecycle: Prepare → Detect → Contain → Eradicate → Recover → Review
- Containment is always the first priority — isolate to prevent spread
- Preserve evidence: disk images, logs, memory dumps before remediation
- Severity-based response: P1 Critical → 15 min, P2 High → 1 hour
- Post-incident review is mandatory for every incident

> Average time to identify a breach: 197 days. Faster detection = smaller impact.

Notes: Walk through a real-world incident timeline. Show the IR plan template.

Incident Response: Triage & Containment

- Triage: Assess scope, identify affected systems, determine severity
- Network isolation: disconnect compromised systems from the network
- Credential reset: force password changes for affected accounts
- Evidence collection: capture volatile data (RAM, network connections) first
- Communication: use out-of-band channels to avoid tipping off attackers

Notes: Demo the triage checklist. Discuss common mistakes during containment.

Module 10: Privileged Access & Least Privilege

- Separate daily-use accounts from admin accounts
- Implement just-in-time (JIT) access — elevate only when needed
- MFA required for ALL privileged access — no exceptions
- Quarterly access reviews: remove unused permissions proactively
- PAM tools: CyberArk, BeyondTrust, HashiCorp Vault, Azure PIM

> 80% of breaches involve compromised privileged credentials.

Notes: Show the Azure PIM workflow. Discuss the pain points of least privilege implementation.

Module 11: Patch Management Awareness

- Critical + exploited = patch within 24 hours
- Maintain accurate asset inventory — you cannot patch what you do not know about
- Test patches in staging before production deployment
- Automate: WSUS, SCCM, Intune, Ansible, or your platform's tooling
- Track and report patch compliance metrics monthly

> CISA KEV catalog: mandatory patching for known exploited vulnerabilities.

Notes: Show the CISA KEV catalog. Discuss patch management tooling options.

Patch Management: Risk Prioritization

- CVSS score + exploitability + asset criticality = patch priority
- Internet-facing systems always get priority over internal systems
- End-of-life software: migrate or isolate — patches will not come
- Have a documented rollback plan for every patch deployment
- Subscribe to vendor security advisories for proactive awareness

Notes: Walk through a real vulnerability prioritization exercise using CVSS.

Module 12: Secure Configuration Basics

- Default configurations are designed for usability, not security
- CIS Benchmarks: free, consensus-based hardening standards
- Disable unnecessary services, ports, and protocols
- Remove default accounts, sample apps, and test data from production
- Infrastructure as Code: codify and version-control your configurations

Notes: Show a CIS Benchmark scan result. Discuss common misconfigurations found in audits.

Secure Configuration: Hardening in Practice

- Golden images: build once, deploy consistently, update regularly
- Network segmentation: limit blast radius of any compromise
- Enable comprehensive logging: authentication, access, changes, errors
- Regular configuration audits against established baselines
- Document every deviation from baseline with a risk acceptance

> Misconfigured cloud storage is the #1 cause of cloud data breaches.

Notes: Show a hardening checklist for Windows Server and Linux.

Module 13: Email Security (SPF, DKIM, DMARC)

- SPF: authorize which servers can send email for your domain
- DKIM: cryptographically sign outbound emails to prevent tampering
- DMARC: policy enforcement — none → quarantine → reject progression
- Monitor DMARC aggregate reports to identify unauthorized senders
- Implement on ALL domains — including parked domains

Notes: Show how to check SPF/DKIM/DMARC with MXToolbox. Walk through DNS record examples.

Module 14: Cloud Security Fundamentals

- Shared responsibility: know exactly what you own vs. the provider
- Identity is the perimeter: IAM + MFA + conditional access policies
- Encrypt data at rest and in transit — no exceptions
- Enable cloud-native security tools: Security Hub, Defender, SCC
- CSPM for continuous posture monitoring and compliance

> IaaS: you manage OS up. PaaS: you manage apps up. SaaS: you manage data and access.

Notes: Draw the shared responsibility model on the whiteboard. Discuss real cloud breaches.

Cloud Security: IAM Deep Dive

- Root/Global Admin accounts: MFA + break-glass procedures only
- Service principals and managed identities over stored credentials
- Implement conditional access: location, device compliance, risk level
- Tag all resources for ownership, classification, and cost tracking
- Regular entitlement reviews using cloud-native tools

Notes: Show Azure Conditional Access policies. Discuss identity governance automation.

Key Takeaways for IT Professionals

- Incident response readiness: plan, practice, improve continuously
- Least privilege + PAM = minimize the blast radius of any compromise
- Patch management: automate, prioritize by risk, track compliance
- Secure configurations: harden defaults, use CIS Benchmarks, audit regularly
- Email authentication + cloud security: protect the expanding attack surface

> Complete all IT Essentials modules to earn your IT Security Essentials certificate at labs.cosmicbytez.ca/training

Notes: Summarize the IT professional's role as both defender and educator. Encourage certification completion.

Questions & Answers

Thank you for your commitment to security awareness.

Notes: Open for technical questions. Be prepared for questions about specific tools, vendor comparisons, and implementation timelines.