SANS SECURITY AWARENESS

Security Essentials for IT Administrators

IT administrators play a crucial role in defending your organization's IT infrastructure against the ever-evolving landscape of cyber threats. From exploiting vulnerabilities to misusing privileges and launching ransomware attacks, cyber adversaries are becoming increasingly sophisticated. With their advanced technical knowledge and privileged access, IT administrators are often prime targets for these malicious actors.

To combat these threats, IT administrators need more than just basic training - **they require comprehensive, role-based instruction tailored to their unique challenges.**

Security Essentials for IT Administrators (SEITA) training delivers exactly that. Our modules provide IT administrators with the specialized knowledge and skills necessary to implement secure configurations, ensure timely patching, and effectively respond to incidents.

By empowering IT administrators with these critical capabilities, SEITA enhances your organization's overall security posture and resilience against breaches.

How is our training different, and how will it benefit your organization?

Specialized Role-Based Training:

SEITA provides advanced-level training tailored to the unique challenges faced by IT administrators. This ensures that those with privileged access and critical system knowledge are well-prepared to counter cyber threats.

Bridging Training Gaps:

Historically, IT administrators have been overlooked in cybersecurity training efforts. SEITA fills this gap, ensuring that those with privileged access and critical system knowledge are well-prepared to counter cyber threats.

Focus on Preventive Measures:

Beyond reactive measures, SEITA emphasizes proactive security practices, such as threat hunting and active defense strategies. This proactive focus helps in identifying and mitigating threats before they can impact the organization.

Enhanced Organizational Security:

By equipping IT administrators with the latest security practices and tools, SEITA helps to fortify your organization's defenses against sophisticated cyber threats.

Learn through real-world scenarios

The 12 modules included in Security Essentials for IT Administrators feature real-world attack and mitigation scenarios while progressing learners along an increasingly complex training path.

Overview:

Examining common beliefs vs realities of cyber-attacks with an introduction to specific responsibilities of cybersecurity practitioners.

Security Maintenance:

Covers security hygiene practices that include practicing change control and configuration management; integrating security into SDLC; patch management; active threat hunting; and more.

Sample Attacks:

Examines the characteristics of attacks like Social Engineering, Spear Phishing, Malware, Denial of Service, and Distributed Denial of Service. It also covers Machine-in-the-Middle, Drive-by-Download, and Watering Hole attacks, highlighting QR Code Attacks, Teams Phishing, and the role of AI in adding complexity and credibility. Emphasizes the critical role of humans as the last line of defense.

Cloud Computing Environments:

Explore cloud environments, their respective security concerns, and best practices for secure deployments while examining the security advantages to cloud environments.

Core Principles:

Focusing on three core principles of cybersecurity. The Principle of Least Privilege, The CIA Triad, and the principle of Prevent, Detect, Respond.

Authentication and Authorization:

Explores the use of passphrases, password managers, and 2FA as authentication mechanisms. It includes best practices for passphrase use, such as the use of 'space' functionality, setting proper permissions according to the Principle of Least Privilege, and an examination of the Zero Trust Model.

Attack Scenario:

An attack scenario is followed from start to finish, the training focuses on the need for changing our methods of detection and response as attack methods change.

Securing Web Servers:

Reviews each of the Open Web Application Security Project (OWASP) top vulnerabilities and how security practitioners can prevent and/or mitigate issues in each category.

Security Program Management:

Learn how threats, vulnerabilities, countermeasures, laws, and compliance requirements inform Risk Management Programs.

Data Protection:

Covering the effective deployment of encryption methods such as the Advanced Encryption Standard algorithm, Transport Layer Security, Internet Protocol Security, Virtual Private Networks, key management fundamentals, and Zero-Knowledge implementations.

Attack Mitigation:

Learn what happens if a cyber-attack cannot be prevented, including deploying mitigation technologies to return to normal operation and repair the root causes of attacks. Emphasizes the use of AI tools for scaling threat detection, malware analysis, incident response, and vulnerability detection and prevention.

Supply Chain Attacks:

Analyzes real-world examples of supply chain attacks to understand why they occur and how to prevent or mitigate them. Stresses the timelessness of the attack examples and illustrates how administrators can prevent attacks through reflection on past incidents and lessons learned.

Technical Training from the Leader in Information Security

Security Essentials for IT Administrators modules from SANS Security Awareness provide crucial reinforcement of the security fundamentals required of technical employees to better protect your organization through the proper configuration of critical IT infrastructure.

Cybersecurity risk is a people problem.
Empower your people to be its solution.

www.sans.org/awareness

SANS SECURITY AWARENESS