SANS SECURITY AWARENESS

Security Essentials for IT Administrators

Until recently, IT Administrators responsible for system or network configuration have represented a unique challenge when it comes to cybersecurity preparedness. With the advanced technical knowledge and skill set required for these roles, traditional end-user awareness training can be inadequate. While conventional wisdom may be that technical users will not benefit from routine awareness training, the reality is that the exclusive knowledge and privileged access that come with these roles is precisely what makes IT Administrators a prime target for cyber-attacks.

It is for this reason, that SANS Security Awareness is delivering a computer-based awareness course to provide advanced-level training to better communicate the unique threats and mitigation techniques required in Information Technology roles.

How Organizations Benefit from IT Administrator Training

Training for the whole organization:

Traditionally, Security Awareness and Training efforts have been focused almost entirely on end-users, leaving a training gap for employees in advanced or technical roles. Security Essentials for IT Administrators ensures your entire organization has the awareness training relevant to the roles and responsibilities unique to each employee.

Upskill your technical team:

Protecting your organization from cyber threats requires continuous investment in skills development to stay ahead of any emerging threats. Provide your technical teams with a deep understanding of evolving security concepts with a learning progression suited to their skillset.

Remove Operational Siloes:

Once one and the same, recent years have seen security job functions and IT job functions becoming increasingly specialized. As such, while their privileged access makes them an increased target for cyber-attacks, IT Admins don't always receive the baseline security training available in this targeted and specialized collection.

A progressive learning path with real-world use cases

The 12 learning 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 cyber security practitioners.

Core Principles:

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

Security Program Management:

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

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.

Authentication and Authorization:

The use of passphrases, password managers, and 2FA are explored as authentication mechanisms. Setting proper permissions according to the Principle of Least Privilege and an examination of the Zero Trust Model is included.

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.

Sample Attacks:

Explores the characteristics of attacks such as Social Engineering, Spear Phishing, Malware, Denial of Service and Distributed Denial of Service, Machine-in-the-Middle, Drive-by-Download, and Watering Hole.

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.

Attack Mitigation Technologies:

Learn what happens if a cyber-attack cannot be prevented and deploying mitigation technologies to return to normal operation and repair the root cause(s) that led to the attack.

Cloud Computing Environments:

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

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.

Supply Chain Attacks:

The final module in the series analyzes real-world examples of supply chain attacks to understand why they occur and how to prevent or mitigate them.

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