DigitalAcademy

Cyber Security for Systems Administrators - OUTILNE

Description:

System Administrators - Welcome to the Newest Front in Modern Warfare

I. Introduction
A. Welcome and Course Overview
B. Understanding the Role of System Administrators as Warriors

II. The Five Domains of Battle
A. Land
B. Sea
C. Air
D. Space
E. Information

III. Cyber as a Battleground
A. Importance of Cybersecurity in Modern Warfare
B. Consequences of Information Technology Attacks
C. Case Study: August 2022 Attack in Montenegro

IV. The Human Factor: People as Risk and Asset
A. Recognizing the Role of People in Attacks
B. Investing in Education and System User Awareness
C. Security Dependence on Human Control

V. Establishing Security Foundations
A. Defining Functions and Well-Documented Designs
B. Importance of Logging for Detection and Troubleshooting
C. Trained Personnel for System Monitoring
D. Inventory Management as a Countermeasure to Theft

VI. Ensuring System Reliability
A. Understanding Coupling and Complexity
B. Mitigating Segmentation Failures
C. Learning from Historical Examples (e.g., Titanic)

VII. Anatomy of a Strong Design
A. Addressing Segmentation Failures
B. Avoiding Shared Platforms and Credentials
C. Importance of Accurate Documentation and Logging

VIII. The Three Activities of Cybersecurity
A. Prevention: Defining Necessary Permissions

DigitalAcademy

B. Detection: Utilizing Automated Tools and Overcoming Limitations
C. Correction: Planning for Attacks and Accidents

IX. Importance of Prompt Patching
A. Understanding the Role of Patching in Security
B. Time Sensitivity and Counteracting Malicious Exploits
C. Addressing Software Vulnerabilities

X. Firewall Basics
A. Access Controls
B. Stateful Inspection
C. Deep Packet Inspection

XI. Detection Challenges and Rumor Control
A. Automated Tools and Their Limitations
B. Alert Fatigue and False Alarms
C. Evaluating "Reputation-Based" Systems

XII. Correction Strategies
A. Preparing for Attacks and Accidents
B. Backup Systems as the Last Line of Defense

Goals:

- ⇨ Raise Awareness: The course aims to make system administrators aware of the evolving nature of modern warfare and the significance of cybersecurity in this context. It emphasizes the role of system administrators as warriors in protecting vital information.
- ⇨ Comprehensive Understanding: By covering the five domains of battle (land, sea, air, space, information) and highlighting why cyber is a battleground, the outline provides a holistic view of the cybersecurity landscape and its importance in the modern world.
- ⇨ Risk Management: The outline emphasizes the role of people as both the greatest risk and the best asset in cybersecurity. It encourages system administrators to invest in education, recognize system users, and address the human-controlled dependencies that impact security.
- ⇨ Foundational Knowledge: The outline covers essential aspects of system administration, including careful documentation, observation of logging, trained personnel, and inventory management. These fundamentals form the basis for building a secure and reliable system.
- ⇨ Identifying Vulnerabilities: The outline discusses common weaknesses in system design, such as segmentation failures, shared platforms, inadequate logging, and undocumented architecture. It helps system administrators identify these vulnerabilities and develop strategies to address them effectively.
- ⇨ Cybersecurity Activities: The outline introduces the three key activities of cybersecurity—prevention, detection, and correction. It emphasizes the importance of prevention through explicit permissions and prompt patching, while also recognizing the need for detection tools and correction strategies when prevention fails.

DigitalAcademy

- ⇨ Backup and Recovery: The outline emphasizes the critical role of backups as the last line of defense. It highlights the need for planning and preparing for attacks and accidents, ensuring system administrators prioritize reliable backup systems.

Recommended Experience and Knowledge:

- ⇒ System Administration Experience
- ⇒ Fundamental IT Knowledge
- ⇒ Cybersecurity Awareness
- ⇒ Networking Proficiency
- ⇒ System Architecture Understanding
- ⇒ Documentation and Logging Skills
- ⇒ Patch Management Knowledge
- ⇒ Backup and Recovery Proficiency
- ⇒ Incident Response Understanding
- ⇒ Continuous Learning Mindset

15.06.2023 – Cyber Security for Systems Administrators

Overview

In this course we will explore the challenges in cybersecurity across the five domains of battle and focus on the significance of cyberspace as a battleground. By examining real-world events, such as the August 2022 incident in Montenegro, we'll understand the consequences of information technology attacks. The course emphasizes the role of people as both the greatest risk and asset in cybersecurity. Education, careful design, logging, trained personnel, and inventory management are crucial. We'll discuss the enemies of reliability (coupling and complexity) and the anatomy of weak designs. The three core activities of cybersecurity (prevention, detection, and correction) will be covered, highlighting the importance of permissions, patching, and backups. This course will provide system administrators with the knowledge and tools to navigate the cybersecurity landscape effectively.

Time	Agenda Items
10:00-10:15	Introduction to Cyber Security and its challenges
10:15-10:20	Questions and answers
10:20 – 10:45	Cyber security structures and countermeasures
10:45 – 11:00	Questions and answers. Break
11:00 – 11:45	The three activities: Prevention, Detection, and Correction

DigitalAcademy

Course Lecturer Biography:

Patrick Bryant, M.Sc., CISSP, ISSAP, ISSMP, CISA

Patrick Bryant has been a Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA) for twenty years. Patrick worked as a Cyber Security Subject Matter Expert at the Montenegro Ministry of Defense from 2020 to 2022 under a U.S. Department of Defense contract. He joined eGA as a consultant at the Ministry of Public Administration in 2023. Prior to his work in Montenegro, he was a Senior Information Security Advisor at NASA Ames Research Center where he was lead researcher of the Security Innovation Lab, as well as a countermeasures architect and incident responder. He also worked as a Licensed Private Investigator in California specializing in cyber-crime investigations where he was engaged by The Boeing Company, ExxonMobil, and Wells Fargo Bank as well as many other Silicon Valley enterprises. Patrick has extensive experience in incident detection and response, countermeasures development, technical risk minimization and security process development.