Hacktales

CYBERSECURITY FOUNDATION PROGRAM

Authors:
Chikodili Udeh & Jide Adebayo

Contents

Hacktales

01

Cyberdefense Controls

- Basic Controls
- Foundation Controls
- Organizational Controls

02

CIS Framework

- Implementation Groups CIS
- v8 Guide Review
- Use Cases

01
Cyberdefense Controls

Objectives

Hacktales

01

At the end of this section, students will understand cybersecurity controls at different layers.

02

Students will learn how to combine controls to acheive defense-in-depth within an organization.

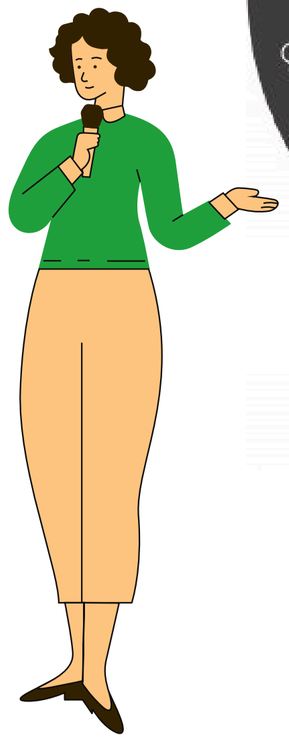
03

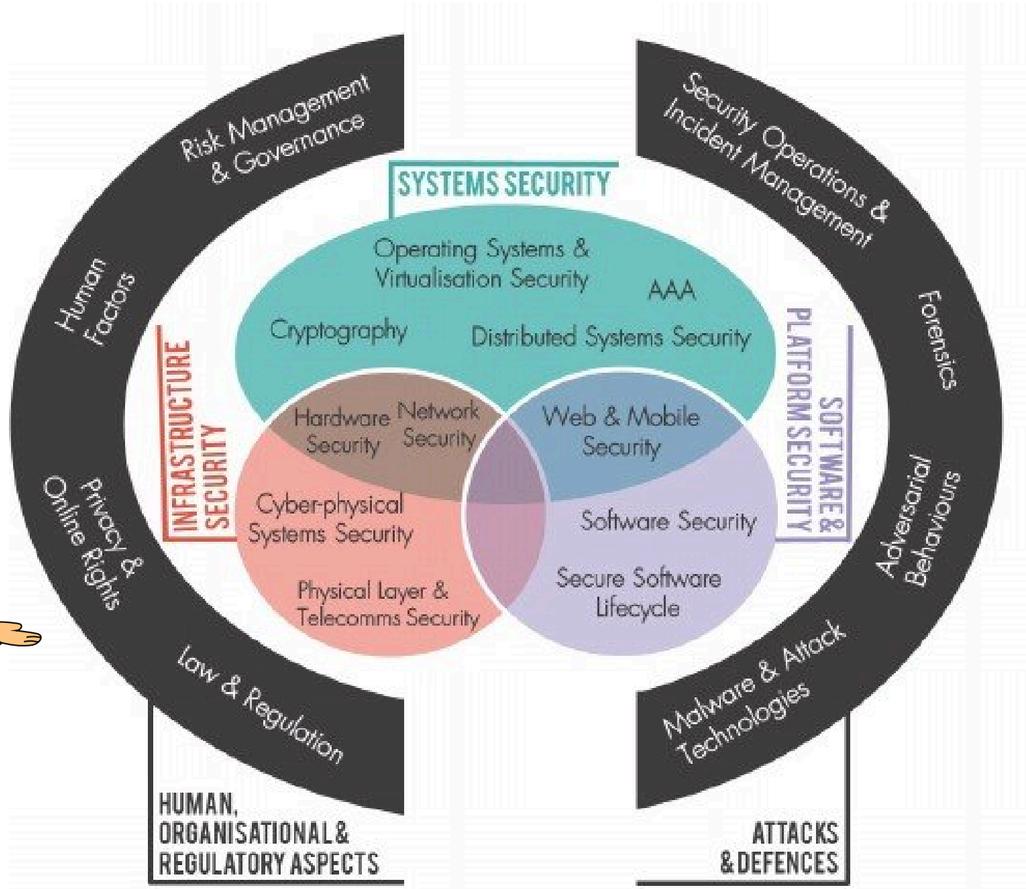
Students will review cyberdefense implementation approaches for small, medium and large organizations.

Recap

There are five major knowledge areas within cybersecurity which include:

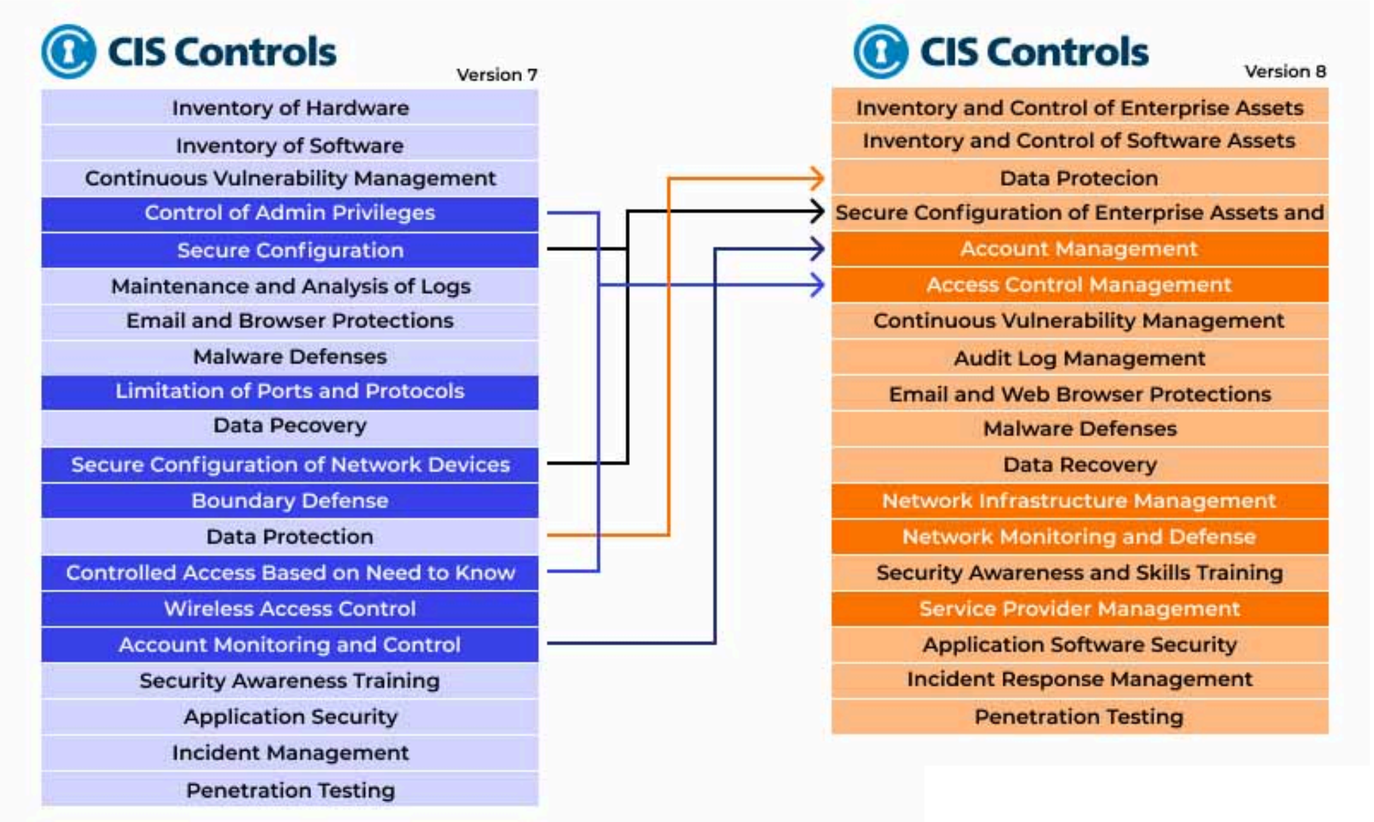
- Attacks and Defenses
- Human, Organizational and Regulatory aspects
- **Infrastructure Security**
- **System Security**
- **Software and Platform Security**





CIS v7 - v8

A set of finest practices for cybersecurity created by the Center for Internet Security (CIS). These controls Version 7 was released in 2018 and updated in 2020, while CIS Controls Version 8 was released in 2021.



CIS Security Controls

Hacktales

CIS Controls offer a comprehensive framework for effective threat and vulnerability management, ensuring robust end-to-end security.

It encompasses eighteen (18) controls that guide organizations in prioritizing and implementing best practices to protect against cyber threats.

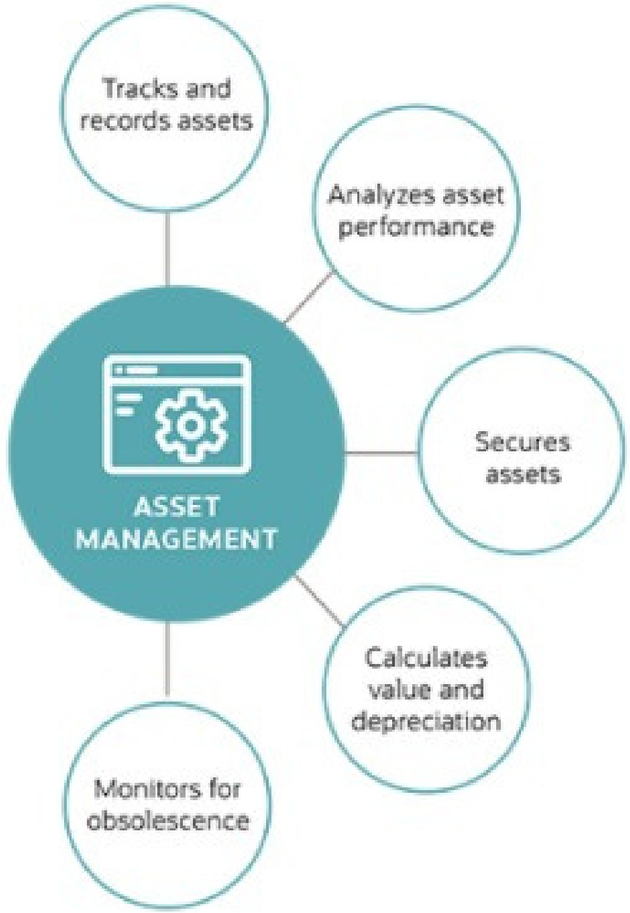
12

Hacktales

Inventory and Control of Enterprise Software and Hardware Assets

This involves maintaining a comprehensive database of software assets, including details such as licenses, versions, and usage to ensure that only authorized software is installed and used within the enterprise.

Additionally, this focus extends to hardware resources within the organization. It emphasizes tools capable of not only tracking and recording hardware assets but also analyzing their performance, calculating their value and depreciation, and securing them against unauthorized access or tampering.



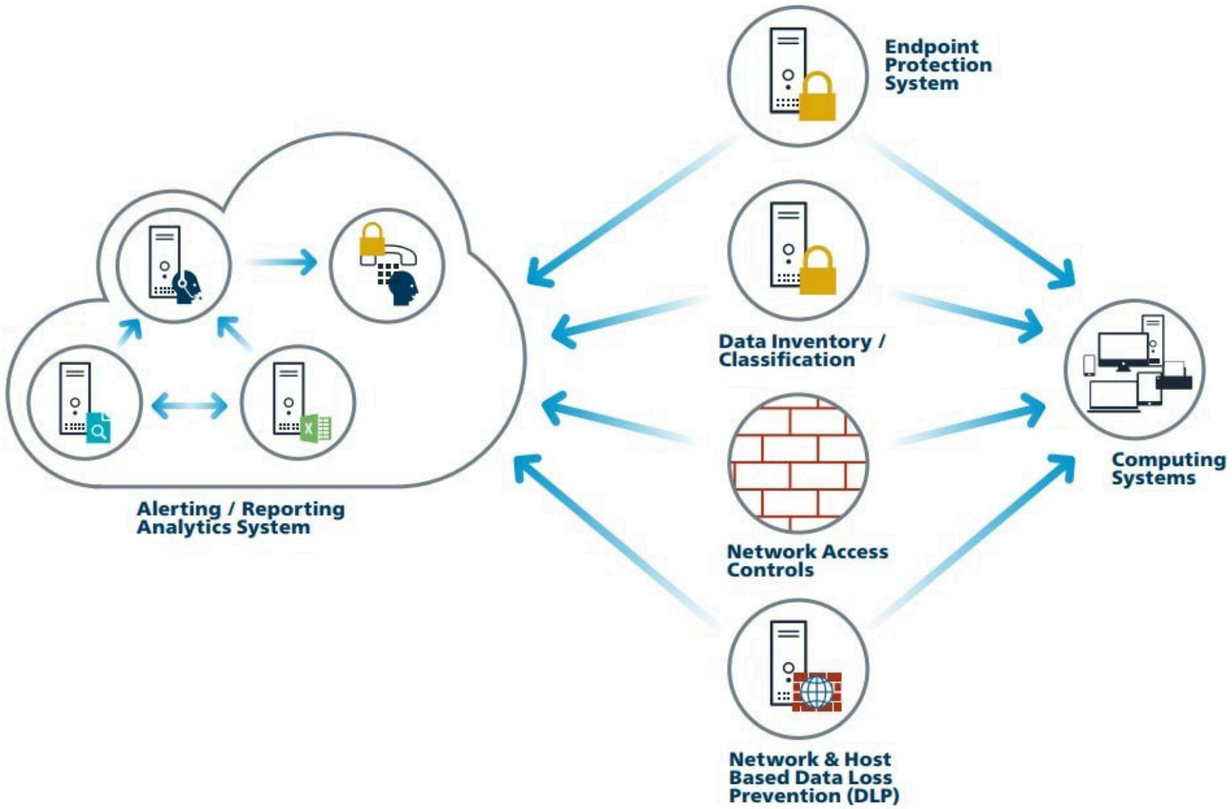
3

Hacktales

Data Protection

Data Protection emphasizes the implementation of tools capable of safeguarding data through various measures. This includes endpoint protection to secure devices, data classification to categorize information based on sensitivity, and Data Loss Prevention (DLP) to prevent unauthorized access or leakage.

Also, Network Access Control (NAC) and Security Information and Event Management (SIEM) are highlighted for controlling access and monitoring for potential threats, ensuring comprehensive data protection measures are in place.



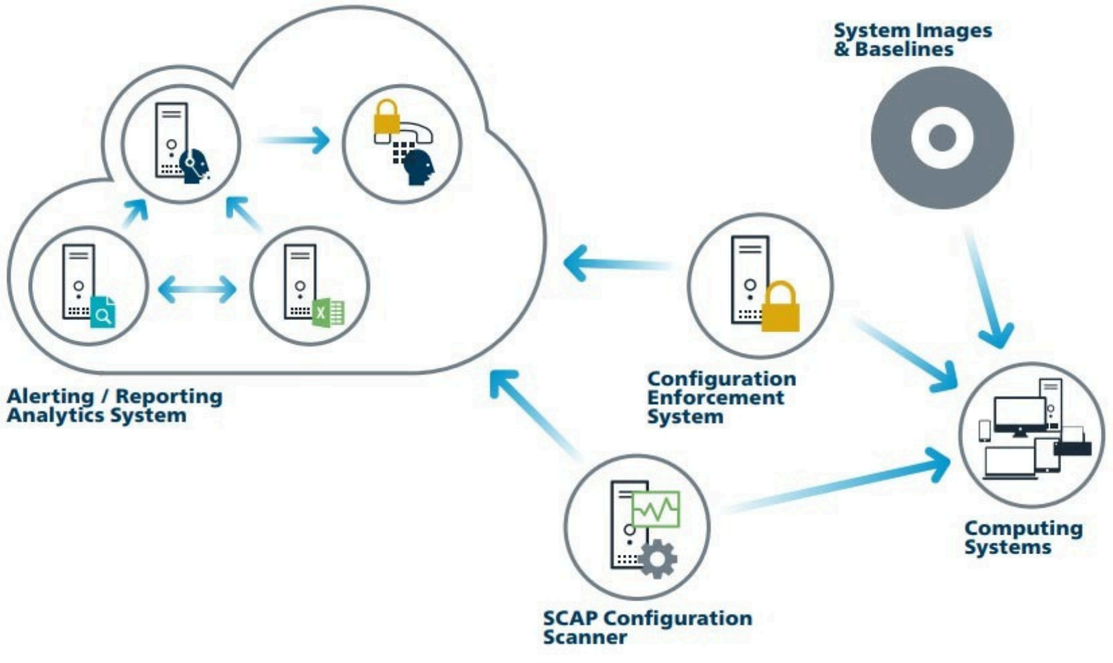
4

Hacktales

Secure Configuration

This underscores the importance of facilitating secure configurations across systems. This entails utilizing baseline system images to establish a secure starting point, employing Security Content Automation Protocol (SCAP) scanners to assess and validate system configurations, and implementing configuration enforcers to ensure compliance with security standards.

Furthermore, Security Information and Event Management (SIEM) solutions play a crucial role in monitoring and responding to configuration-related security events, enhancing the overall security posture of the organization.

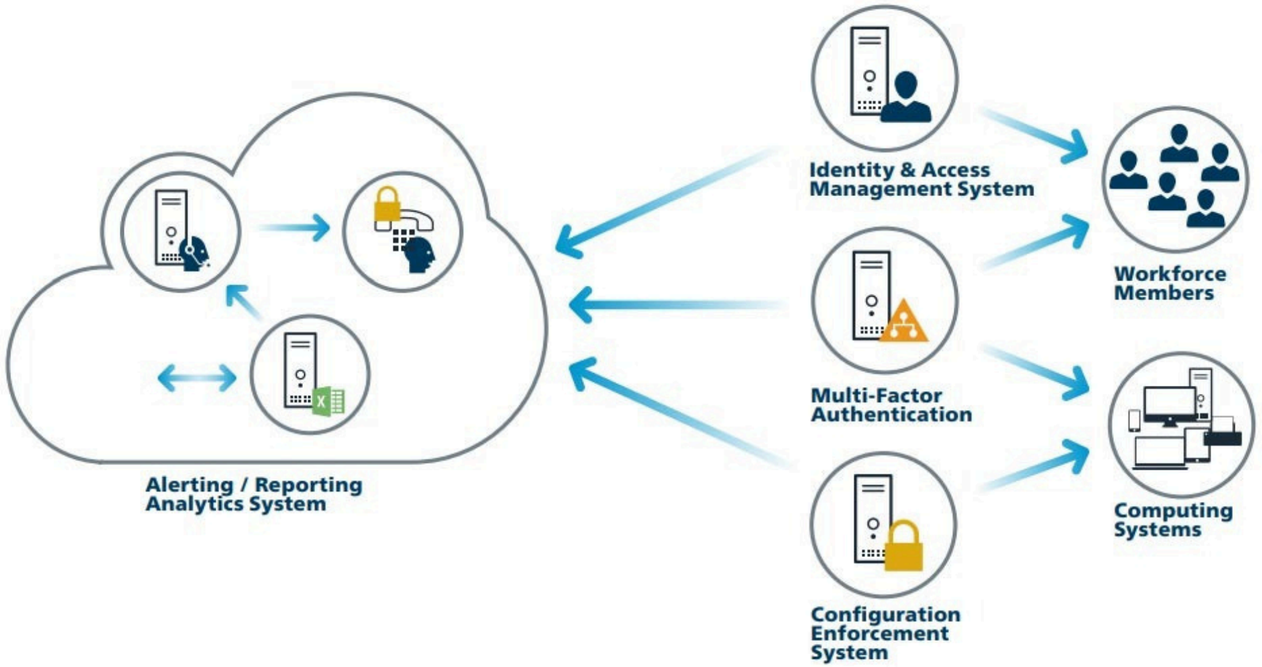


5

Hacktales

Account Management

This control focuses on strengthening cybersecurity through Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Configuration Enforcement, and Security Information and Event Management (SIEM), ensuring robust protection against unauthorized access, configuration vulnerabilities, and detection of security incidents.



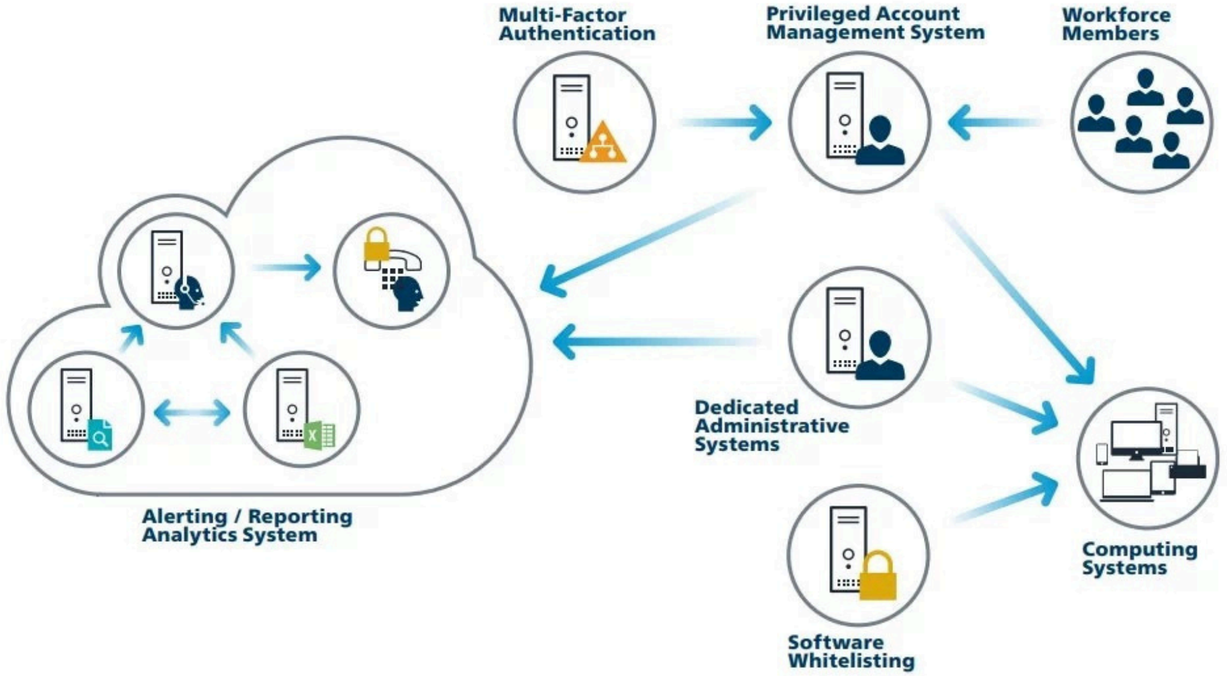
6

Hacktales

Access Control Management

Access control management is achieved through a holistic approach, integrating Multi-Factor Authentication (MFA), Privileged Access Management (PAM), Dedicated Administrative Systems, Software Whitelisting, and Security Information and Event Management (SIEM).

These components collectively enhance security, mitigate risks, and maintain a secure environment.



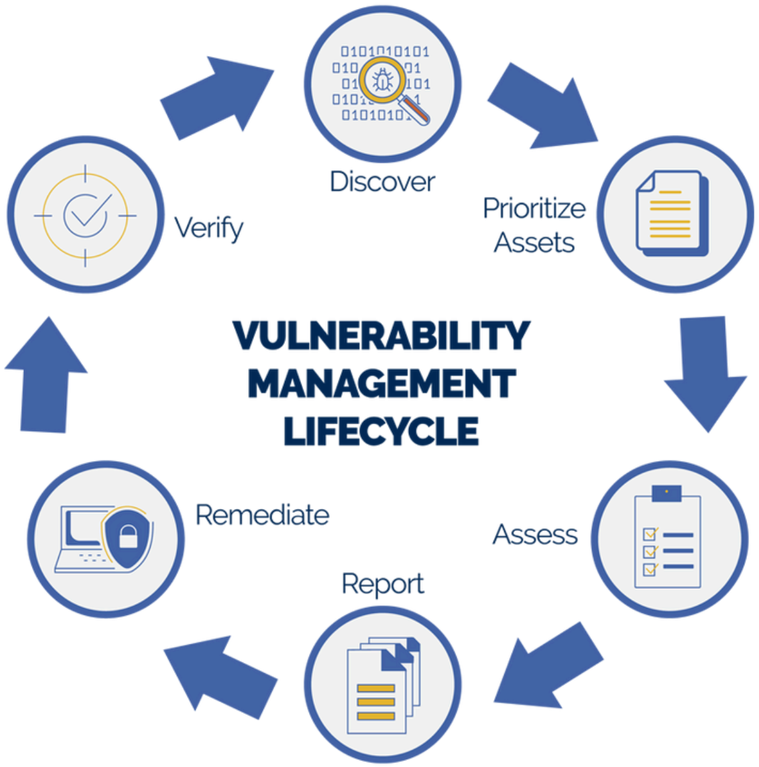
7

Hacktales

Continuous Vulnerability Management

The ongoing process of identifying, assessing, and mitigating security vulnerabilities within an organization's systems and networks. By regularly scanning for weaknesses, prioritizing patches, and implementing corrective actions, organizations can proactively strengthen their defenses against potential cyber threats.

This control underscores the importance of staying vigilant and responsive to emerging vulnerabilities to maintain a robust security posture.



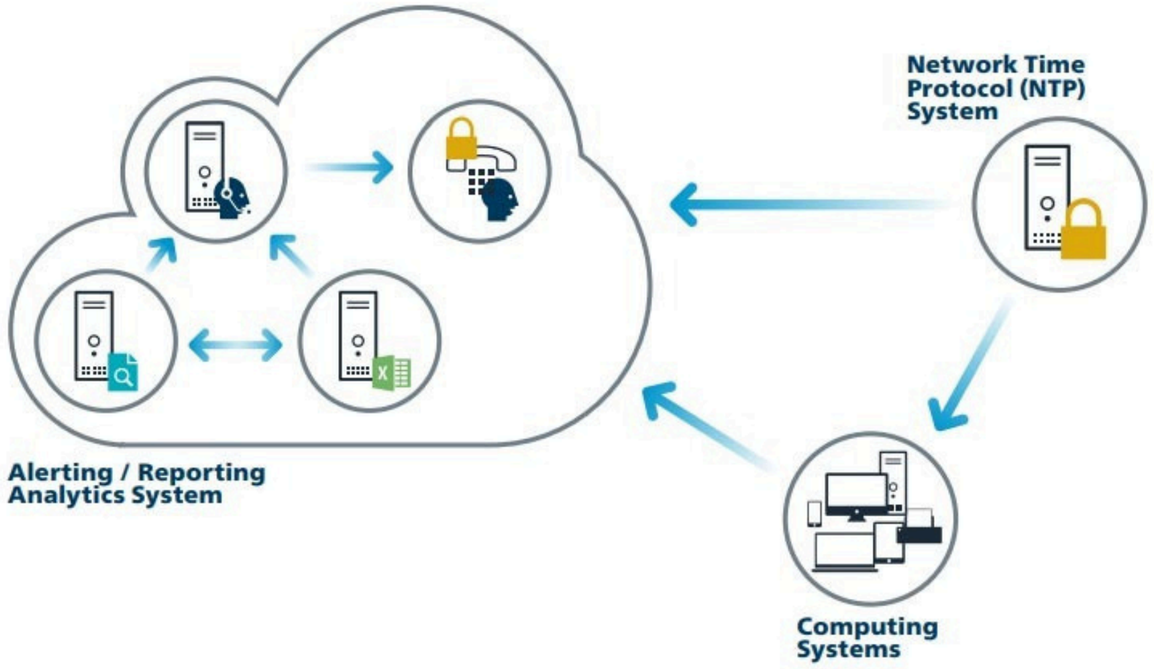
8

Hacktales

Log Management

Emphasizes the critical role of maintaining accurate and secure logs for monitoring and analysis. By synchronizing system time using Network Time Protocol (NTP) and leveraging Security Information and Event Management (SIEM) solutions, organizations can ensure the integrity and availability of logs.

This control enables effective detection, investigation, and response to security incidents, enhancing overall cybersecurity posture through comprehensive log management practices.



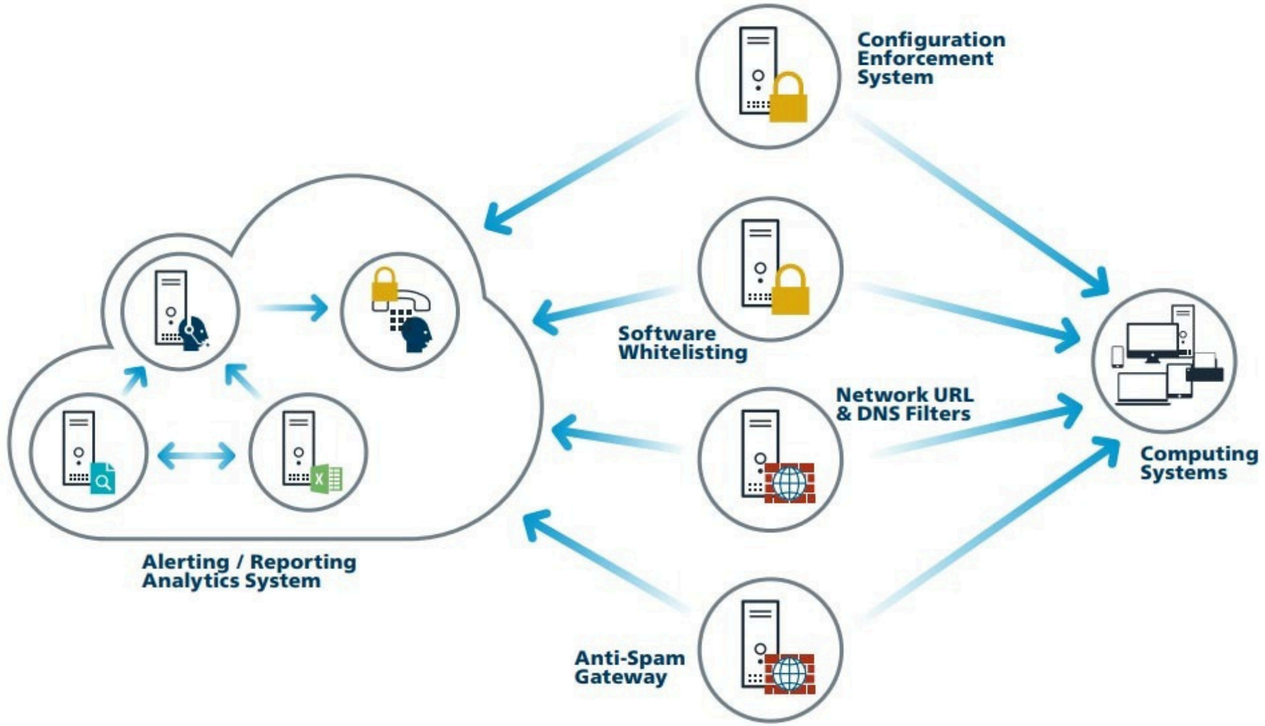
9

Hacktales

Email & Browser Protection

Here, our focus is on fortifying defenses against common attack vectors like phishing and malware through multiple layers of protection. Configuration enforcement and software whitelisting ensure that only authorized applications and settings are permitted, reducing the attack surface. Email gateways and anti-spam gateways filter incoming emails, detecting and blocking malicious content.

Network and URL DNS filters provide additional protection by blocking access to known malicious websites. Together, these measures bolster email and browser security, mitigating the risk of cyber threats and data breaches.



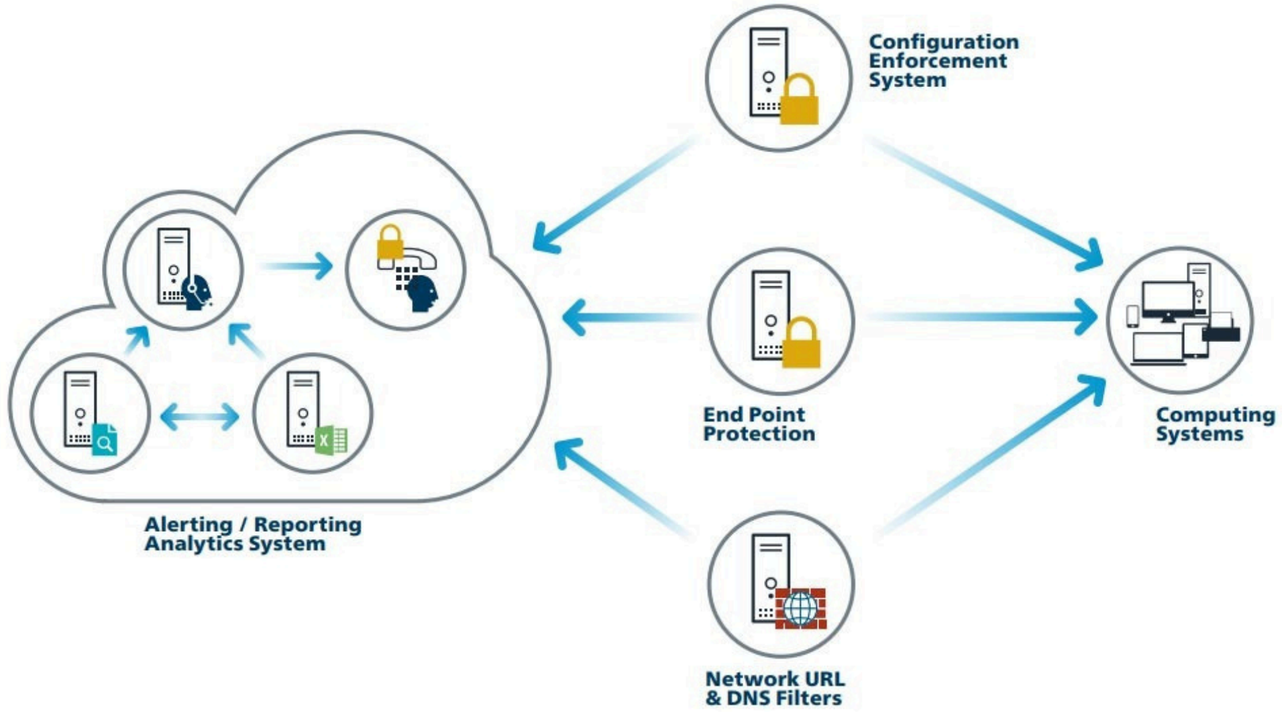
10

Hacktales

Malware Defenses

Implement robust measures to protect against malware infections. Configuration enforcement ensures systems adhere to secure settings, reducing vulnerability to malware attacks. Endpoint protection solutions, including antivirus software and endpoint detection and response (EDR) tools, safeguard individual devices from malware threats.

Network and URL DNS filters provide additional layers of defense by blocking access to malicious websites and filtering out malicious network traffic.

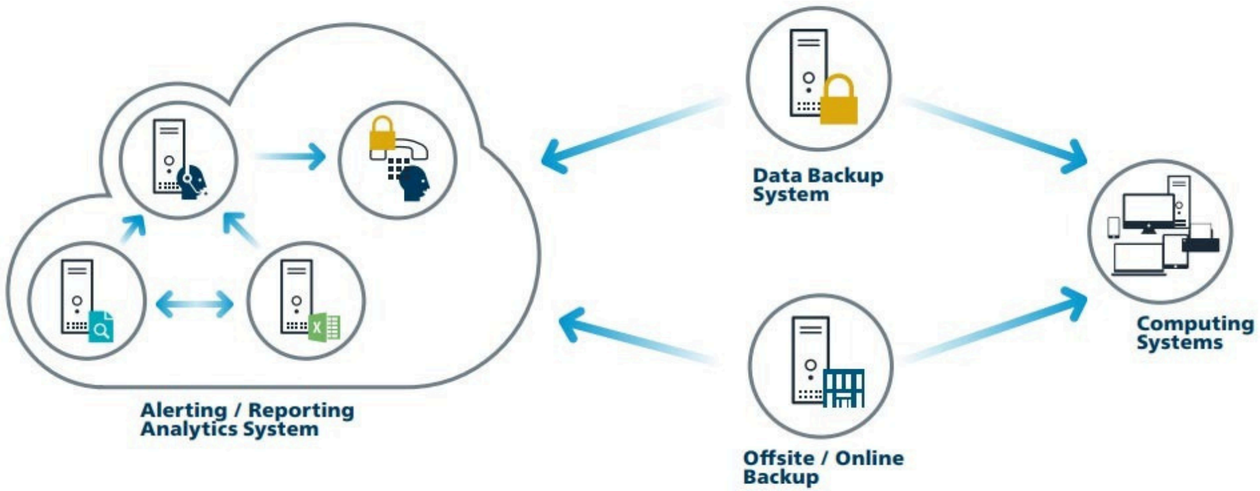


Hacktales

Data Backup & Recovery

This underscores the importance of safeguarding critical data through comprehensive backup and recovery strategies. Implementing a robust data backup system ensures regular and secure backups of essential information, reducing the risk of data loss due to cyber incidents or hardware failures.

Offsite and online backup solutions provide redundancy and resilience by storing backups in separate physical locations or cloud environments, ensuring data availability even in the event of on-premises disasters.

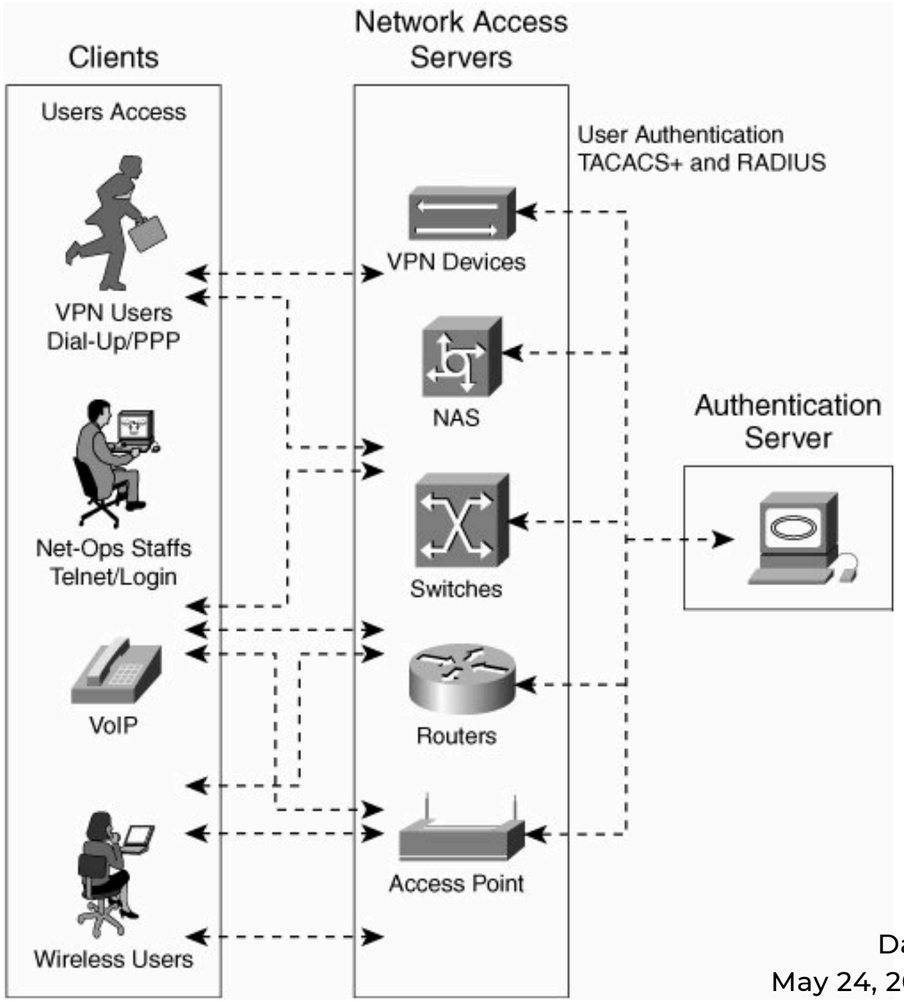


Hacktales

Network Infrastructure Management

Encompasses three key aspects: user access, network devices, and authentication servers. It involves implementing robust measures to ensure the security and integrity of these components.

This includes managing user access through strong authentication mechanisms and access controls, maintaining and securing network devices through regular updates and configuration management, and safeguarding authentication servers to prevent unauthorized access.



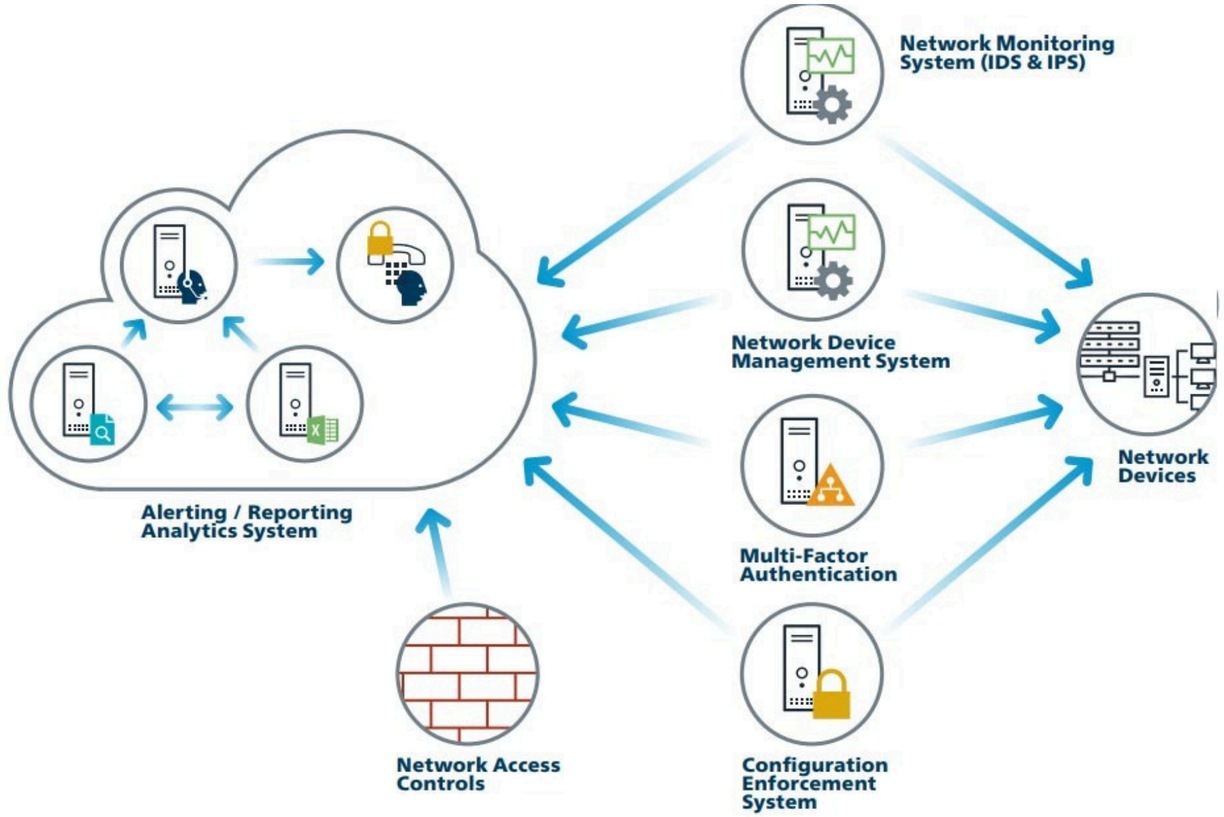
Date:
May 24, 2025

13

Hacktales

Network Monitoring & Defense

Proactively identify and respond to threats within the network environment. This involves deploying Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) to monitor network traffic for suspicious activities and potential security breaches. MFA adds an extra layer of security to access controls, reducing the risk of unauthorized access. Effective network device management ensures that network infrastructure remains secure and properly configured, while configuration enforcement ensures adherence to security policies and standards.



Date:
May 24, 2025

Hacktales

Security Awareness Training

Educate employees to recognize and respond to cybersecurity threats effectively. By providing regular training sessions and awareness programs, organizations can empower employees with the knowledge and skills needed to identify phishing emails, avoid social engineering attacks, and follow best practices for secure computing.

This proactive approach helps create a security-conscious culture within the organization, reducing the likelihood of human error leading to security incidents.

15

Hacktales

Service Provider Management

Managing relationships with third-party service providers to mitigate cybersecurity risks. This involves assessing and monitoring the security practices of service providers, ensuring they adhere to agreed-upon security standards and protocols. By establishing clear contractual agreements, conducting regular audits, and implementing oversight mechanisms, organizations can better protect their data and assets when outsourcing services.

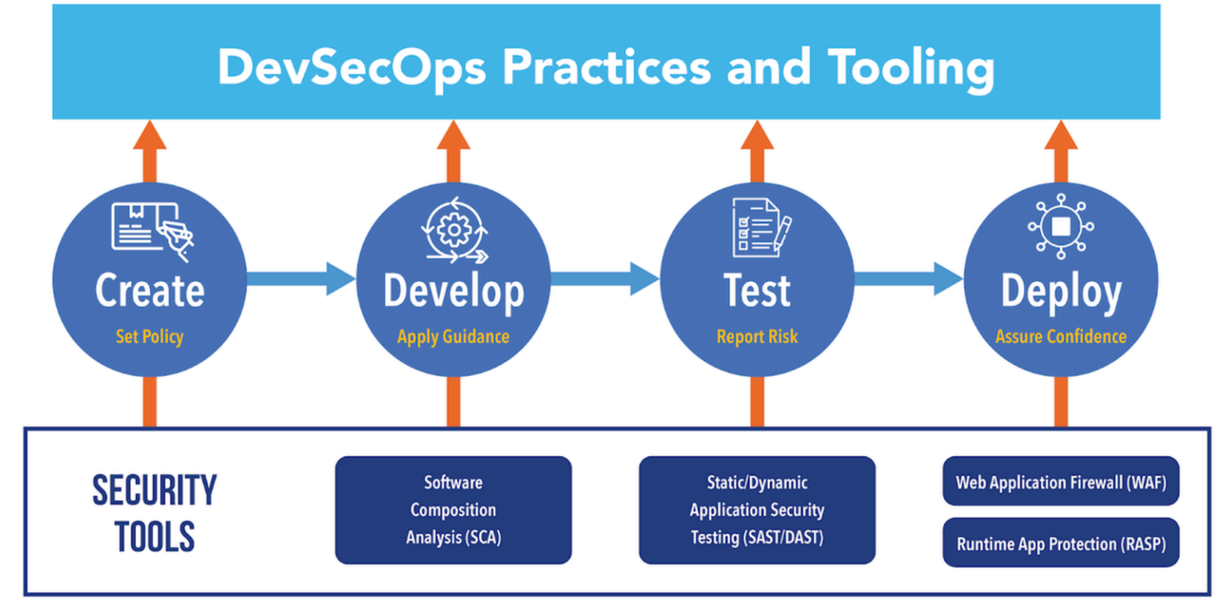
Module 5: Cyberdefense Controls
Cybersecurity Foundation Program

Date:
May 24, 2025

Hacktales

Application Security

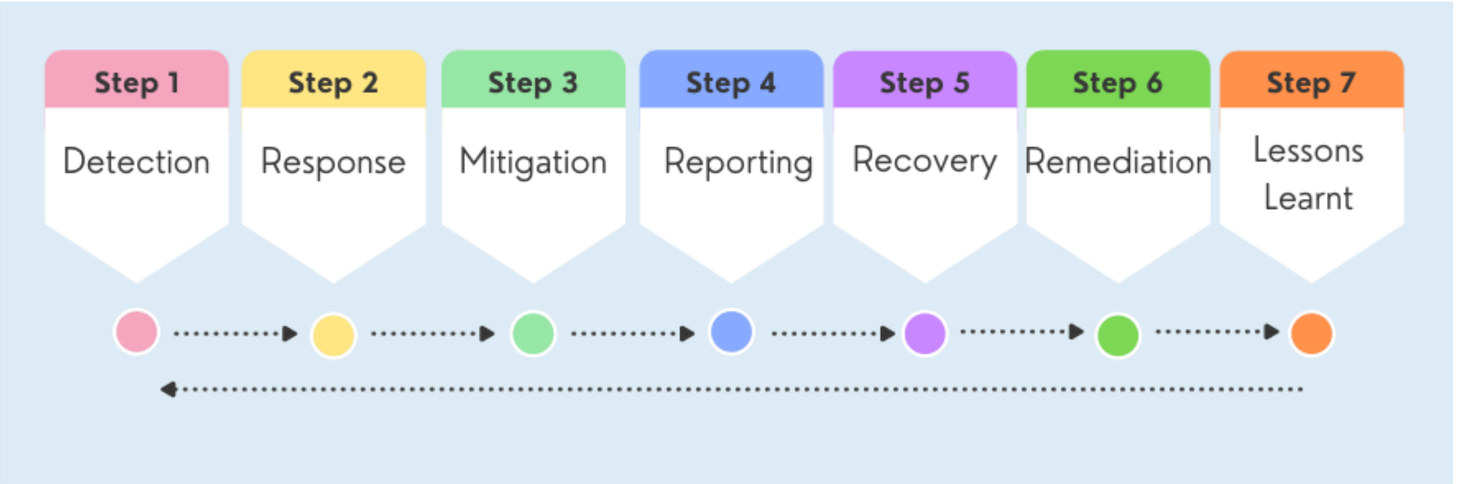
Emphasizes integrating security measures into the software development lifecycle. By implementing security best practices and automated security testing tools throughout the DevOps process, organizations can identify and address vulnerabilities early in the development cycle. This proactive approach reduces the risk of security flaws in applications and minimizes the potential impact of cyber threats. Additionally, fostering collaboration between development and security teams promotes a culture of shared responsibility for application security.



Source: GigaOm 2020

Hacktales

Incident Response



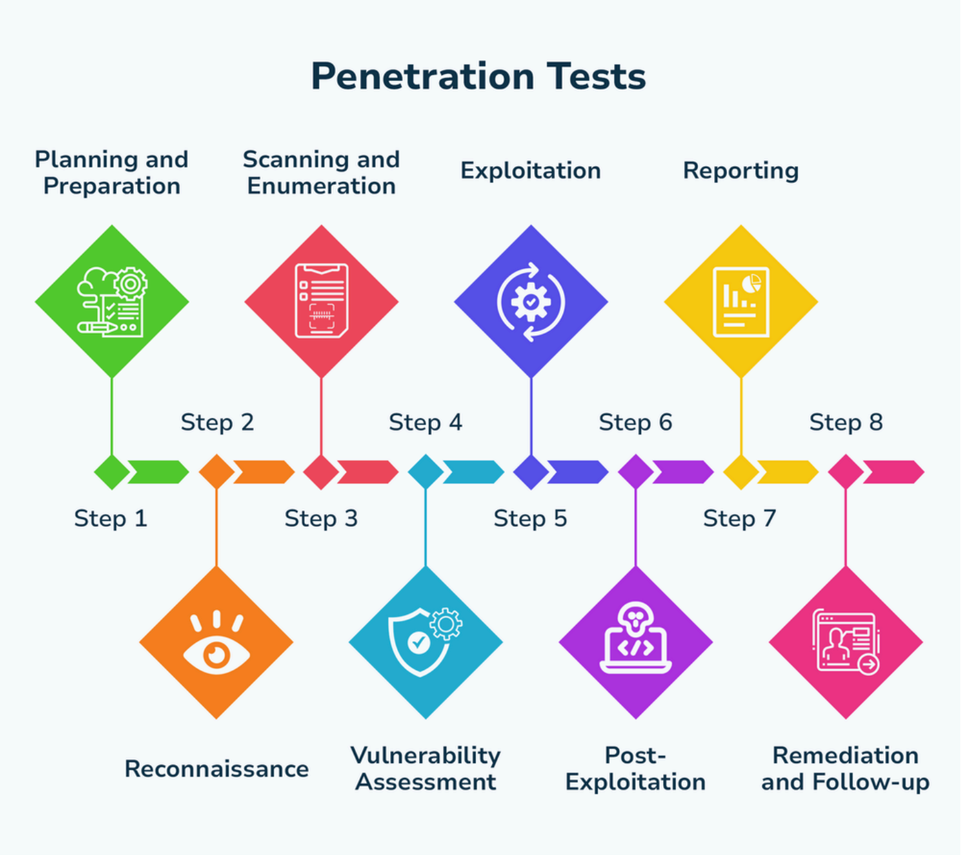
Incident response, is centered on establishing robust procedures and protocols for effectively detecting, responding to, and recovering from cybersecurity incidents. This involves creating an incident response plan that outlines roles, responsibilities, and escalation procedures for handling security breaches. Additionally, organizations must implement incident detection and monitoring systems to promptly identify and assess potential security incidents. By conducting regular incident response exercises and simulations, teams can refine their processes and improve their ability to mitigate the impact of cyber incidents.

Hacktales

Penetration Testing

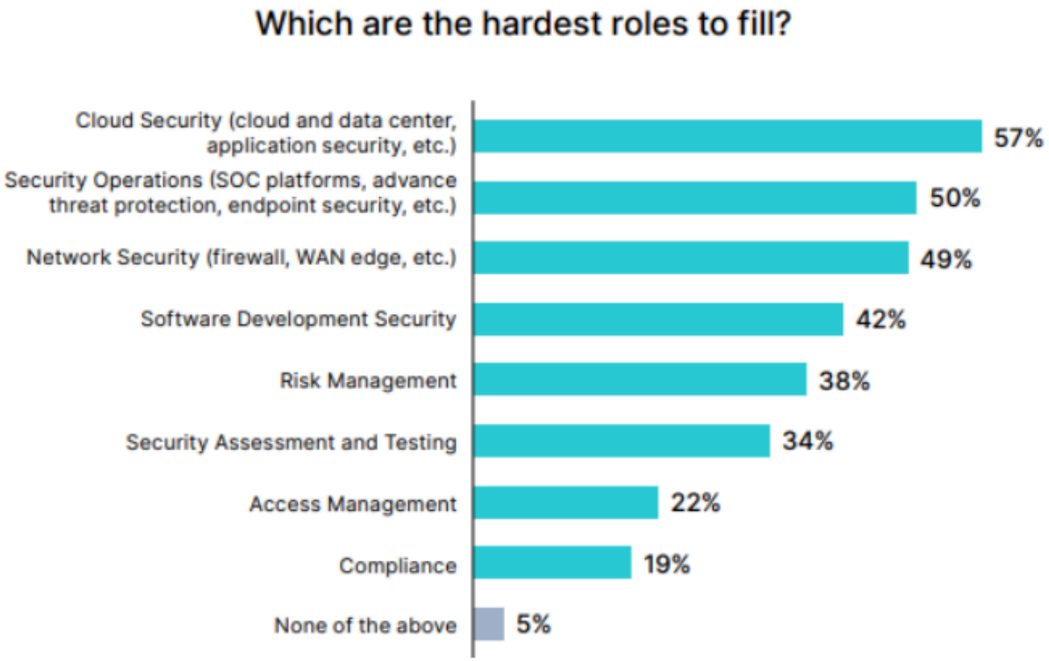
Focuses on proactively identifying and addressing security vulnerabilities within an organization's systems and networks. Penetration testing involves simulated cyber attacks conducted by ethical hackers to identify weaknesses that could be exploited by malicious actors. By conducting regular penetration tests, organizations can uncover potential security flaws and prioritize remediation efforts to strengthen their defenses.

This proactive approach helps organizations stay ahead of cyber threats, reduce the risk of breaches, and enhance overall cybersecurity resilience.

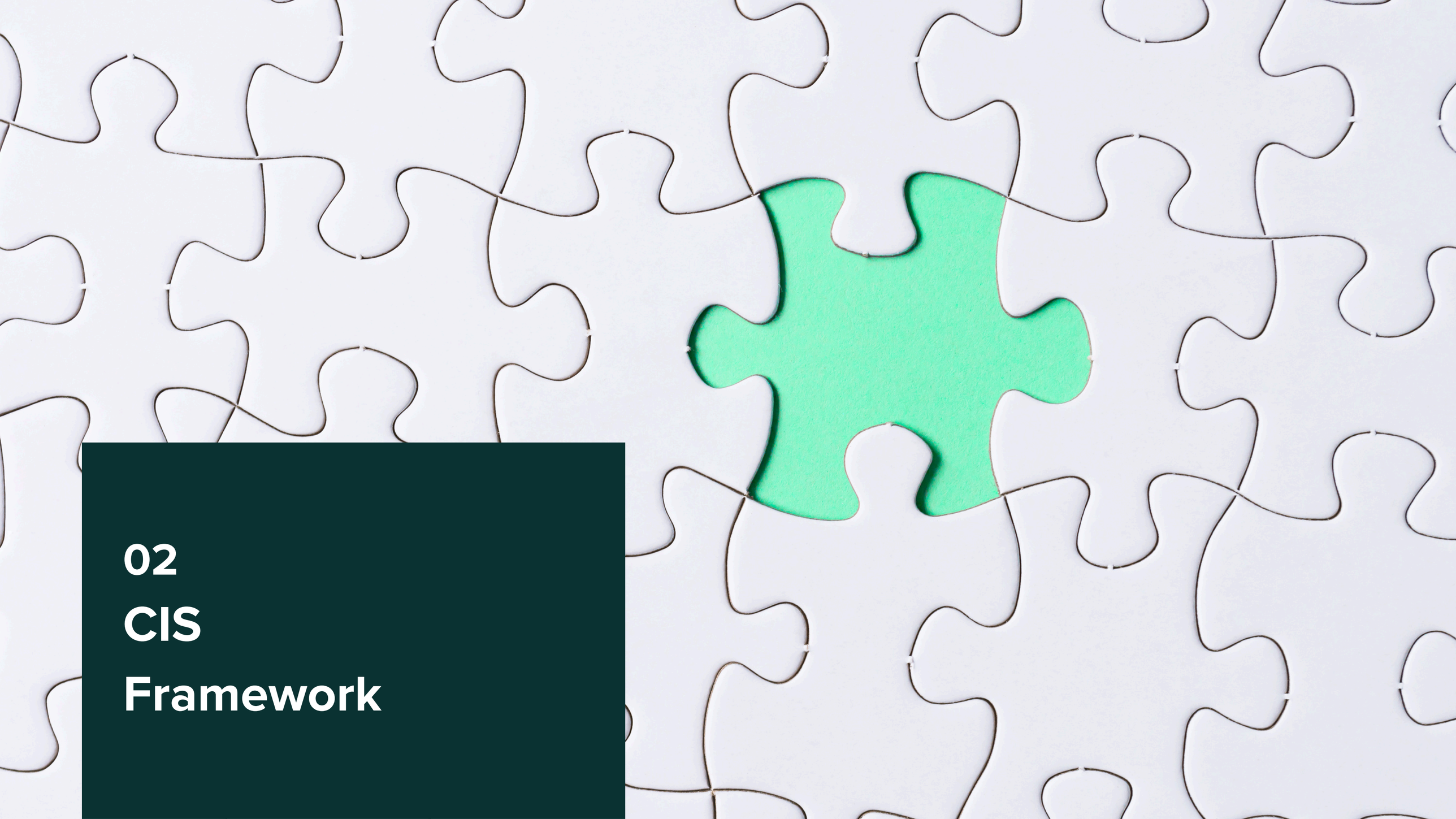


Career Outlook (2024 & Beyond)

Hacktales



Source: Fortinet



02
CIS
Framework

Hacktales

Cyberdefense Implementation

CIS Controls v8

Module 5: Cyberdefense Controls
Cybersecurity Foundation Program