Quick Collective Guide to MITRE ATT&CK® and ISO 27001 Frameworks

Introduction

In today's dynamic cybersecurity landscape, robust frameworks are essential for effectively assessing and mitigating security risks. Among the most influential frameworks, MITRE ATT&CK® and ISO 27001 offer complementary approaches that help organizations establish and maintain comprehensive security postures.

Delinea's Advanced Solutions: PCCE and CID

Delinea enhances identity security with Privilege Control for Cloud Entitlements (PCCE) and Cloud Identity Discovery (CID), two solutions designed to secure cloud identities and manage entitlements efficiently.

For more content like and follow me: @bertblevins

Privilege Control for Cloud Entitlements

PCCE helps enforce the principle of least privilege across multi-cloud environments by continuously discovering and managing entitlements. Key features include:

Continuous Discovery:

Automatically identifies entitlements across public clouds and identity providers, ensuring visibility into all access rights.

Risk Identification:

Detects over-privileged identities and misconfigurations, such as accounts lacking multi-factor authentication (MFA), to mitigate potential security risks.

Enforcement of Least Privilege:

Streamlines the process of right-sizing entitlements, limiting access to necessary resources while maintaining operational efficiency.

Unified Administration:

Provides a centralized platform for managing privileges, reducing administrative overhead and enhancing compliance.

For more content like and follow me: @bertblevins

Cloud Identity Discovery (CID):

CID extends Delinea's Secret Server Cloud capabilities to encompass cloud identities, including privileged accounts, service accounts, admins, and shadow admins. Key features include:

Automated Monitoring:

Continuously scans for sensitive accounts, enabling prompt identification and management of privileged credentials

Integration with Secret Server:

Facilitates the secure storage and management of discovered credentials within Secret Server, reducing the risk of unauthorized access.

Customizable Definitions:

SAllows organizations to tailor definitions of admin and privileged accounts to align with specific security policies and requirements.

By implementing PCCE and CID, organizations can proactively manage cloud entitlements and identities, bolstering their security posture within complex cloud environments.

For more content like and follow me: @bertblevins

Core Components (as of October 2022)

Tactics:
14 stages representing the adversary's goals.

Techniques:
193 ways adversaries achieve their goals.

Sub-techniques:
401 specific variations of techniques.

Software:
718 documented tools and malware.

Threat Actor Groups:
135 recognized adversarial groups.

Documented Campaigns:
14 instances detailing real-world adversary operations.

Key Elements

The MITRE ATT&CK® framework organizes cyberattack tactics, techniques, and procedures (TTPs) to help organizations analyze, prioritize, and strengthen their defenses systematically. By understanding the common strategies attackers use, security teams can anticipate, detect, and thwart malicious activities more effectively.

ISO 27001 Framework: An Overview

ISO 27001 is an internationally recognized standard for managing information security, developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This framework provides a structured approach to managing sensitive company data, with a focus on maintaining confidentiality, integrity, and availability.

Core Components

The ISO 27001 framework includes a comprehensive set of requirements to establish, implement, maintain, and continually improve an Information Security Management System (ISMS).

Implementation Phases

ISO 27001 provides a roadmap for organizations to secure their data assets by implementing policies, controls, and procedures tailored to their specific needs. Key phases in the ISO 27001 lifecycle include:

Scope and Policy Development:
Defining the ISMS scope and establishing security policies.

Risk Assessment and Management:
Identifying potential risks and implementing controls.

Implementation and Documentation:
Documenting controls and communicating them to stakeholders.

Performance Evaluation:
Regularly reviewing and auditing the ISMS for improvements.

Continuous Improvement:
Enhancing controls and adapting to new threats and vulnerabilities.

IdentitySecurity.net

Share your thoughts in comments below

For more content like and follow me: @bertblevins