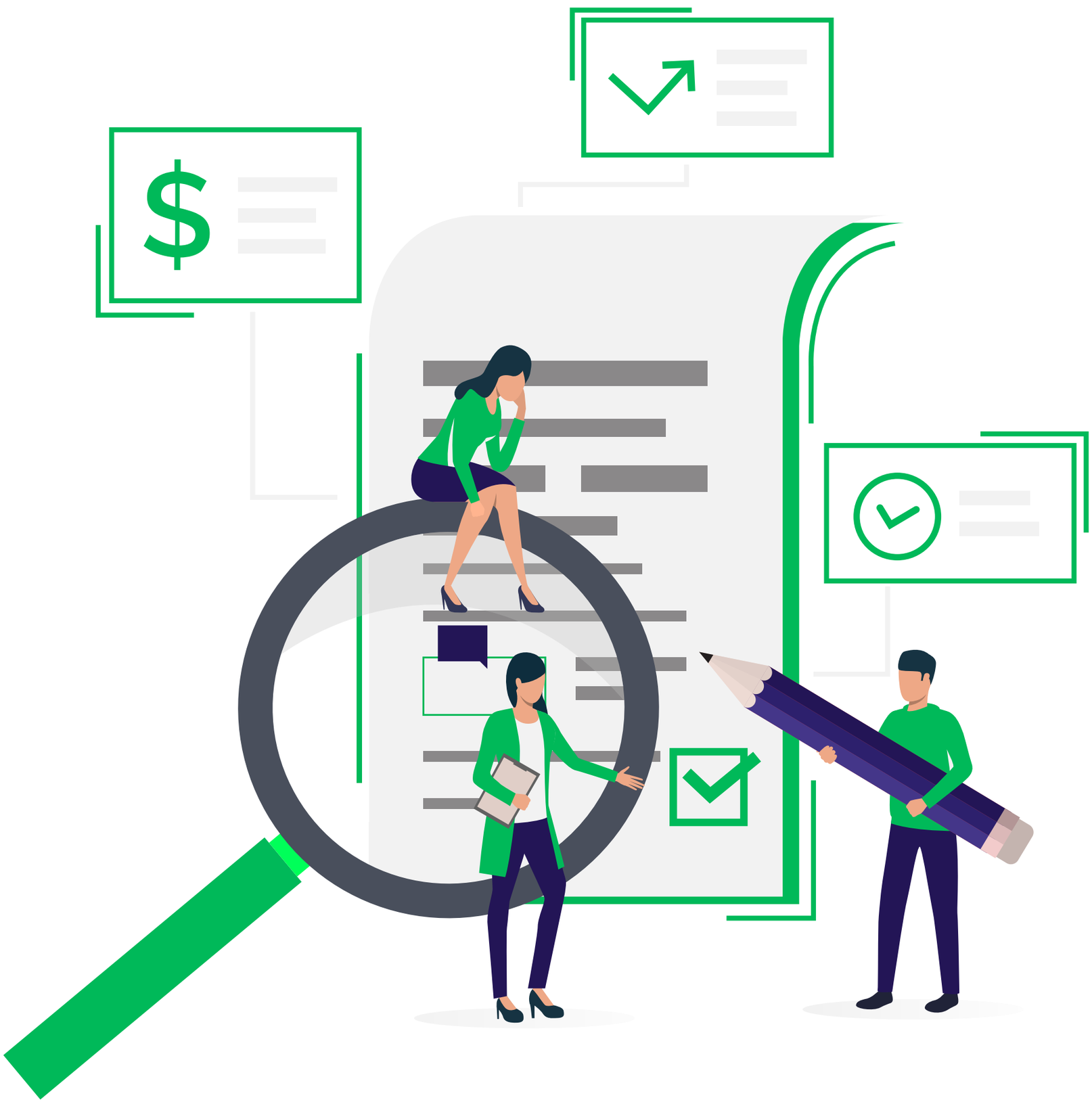
Quick Collective Guide to

MITRE ATT&CK®

and ISO 27001 Frameworks

and How Delinea Leverages Them



For more content like and follow me:

@bertblevins

A Quick Guide to MITRE ATT&CK® and ISO 27001 Frameworks and How Delinea Leverages Them

Manage MITRE ATT&CK® compliance & scoring seamlessly with Delinea's PCCE and CID solutions for Privilege Control for Cloud Entitlements and Cloud Identity Discovery.

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.

Privilege Control for Cloud Entitlements (PCCE):

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:
Allows 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.

MITRE ATT&CK® Framework: An Overview

Definition

MITRE ATT&CK® is an open-source, globally accessible knowledge base that catalogues adversarial tactics and techniques based on real-world observations. This framework aids organizations across the private sector, government, and cybersecurity communities in constructing targeted threat models and defense methodologies.

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

For more content like and follow me:

@bertblevins

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

Definition

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). Some of the key aspects include:

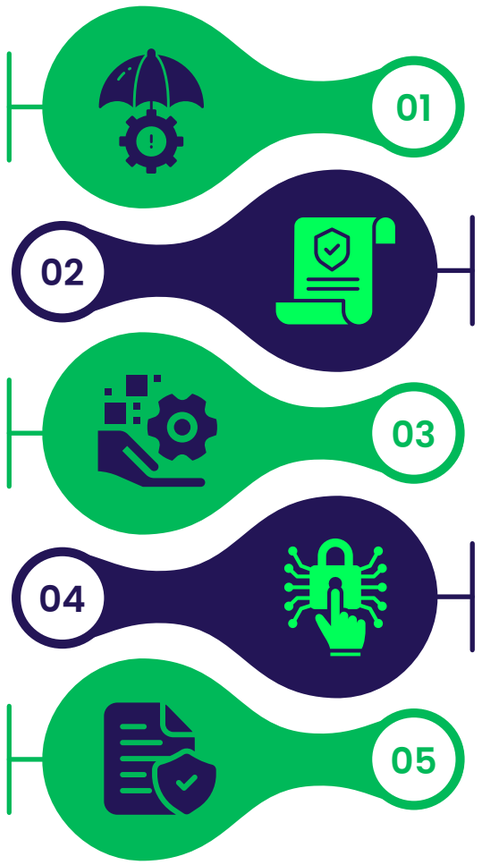
For more content like and follow me:

@bertblevins

Risk Assessment and Treatment:
Identifying, analyzing, and addressing information security risks.

Asset Management:
Proper classification and handling of company information.

Compliance Obligations:
Adherence to applicable legal, regulatory, and contractual requirements.



Security Policies:
Guidelines and standards to protect data integrity and privacy.

Access Control:
Regulations on who can access specific data and systems.

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.

Comparing MITRE ATT&CK® and ISO 27001:

Complementary Security Approaches

Both MITRE ATT&CK® and ISO 27001 provide valuable frameworks for addressing cybersecurity challenges, but they serve different functions and complement each other effectively.

For more content like and follow me:

@bertblevins

Scope:

- MITRE ATT&CK® is primarily a tactical and operational framework that focuses on real-world threat behaviors and methods.
- ISO 27001 is a strategic framework that outlines management processes and controls for securing sensitive information.

Focus:

- MITRE ATT&CK® emphasizes understanding and defending against adversarial tactics, techniques, and procedures (TTPs).
- ISO 27001 centers on establishing a holistic security management system that prioritizes risk management, policy development, and compliance.

Application:

- MITRE ATT&CK® is widely used for threat intelligence, red teaming, and improving incident response through detailed threat modeling.
- ISO 27001 is often pursued for regulatory compliance and to demonstrate an organization’s commitment to secure data management practices.
- Using MITRE ATT&CK® and ISO 27001 together allows organizations to benefit from both a tactical understanding of specific threat vectors and a strategic management system to reinforce their security posture.

Summary:

Leveraging Compliance Scores for a Stronger Security Posture

By combining the MITRE ATT&CK® and ISO 27001 frameworks with Delinea's Privilege Control for Cloud Entitlements (PCCE) and Cloud Identity Discovery (CID), which contain Delinea Checks, organizations can establish a robust, multi-faceted approach to cybersecurity. Each element contributes uniquely:

For more content like and follow me:

@bertblevins

MITRE ATT&CK® offers tactical insights into adversary behaviors, helping organizations defend against specific threats by understanding common tactics, techniques, and procedures (TTPs).

ISO 27001 provides a strategic framework for managing information security holistically, aligning an organization's policies, procedures, and controls with international standards to maintain data confidentiality, integrity, and availability.

Delinea's PCCE and CID solutions strengthen identity and privilege management by continuously assessing cloud entitlements and identities, reducing risk from over-privileged access, and ensuring least-privilege principles are enforced across multi-cloud environments. Within PCCE and CID, Delinea Checks provide a catalog of health checks that enhance visibility into the security posture of applications and systems. These checks focus on preventative security measures and deliver insights as a compliance score, helping organizations proactively identify vulnerabilities and address potential risks.

Together, these frameworks and tools enable organizations to leverage compliance scoring effectively. By aligning with the requirements and methodologies of both MITRE ATT&CK® and ISO 27001, an organization can use Delinea's PCCE, CID, and integrated Delinea Checks to monitor and manage privilege while assessing system health comprehensively. This integration provides real-time data on compliance, risk, and overall security posture, with Delinea Checks offering an actionable score that highlights gaps and guides preventative and remediation measures The resulting compliance scores serve as a valuable metric, enabling continuous improvements and reinforcing the organization's resilience against evolving threats.

Share your thoughts in comments below