Welcome Back to CISSP Bootcamp Day 4

Michael J. Shannon

Class will begin at 10:00 am Central Standard Time

Authorization Mechanisms & Identity Management

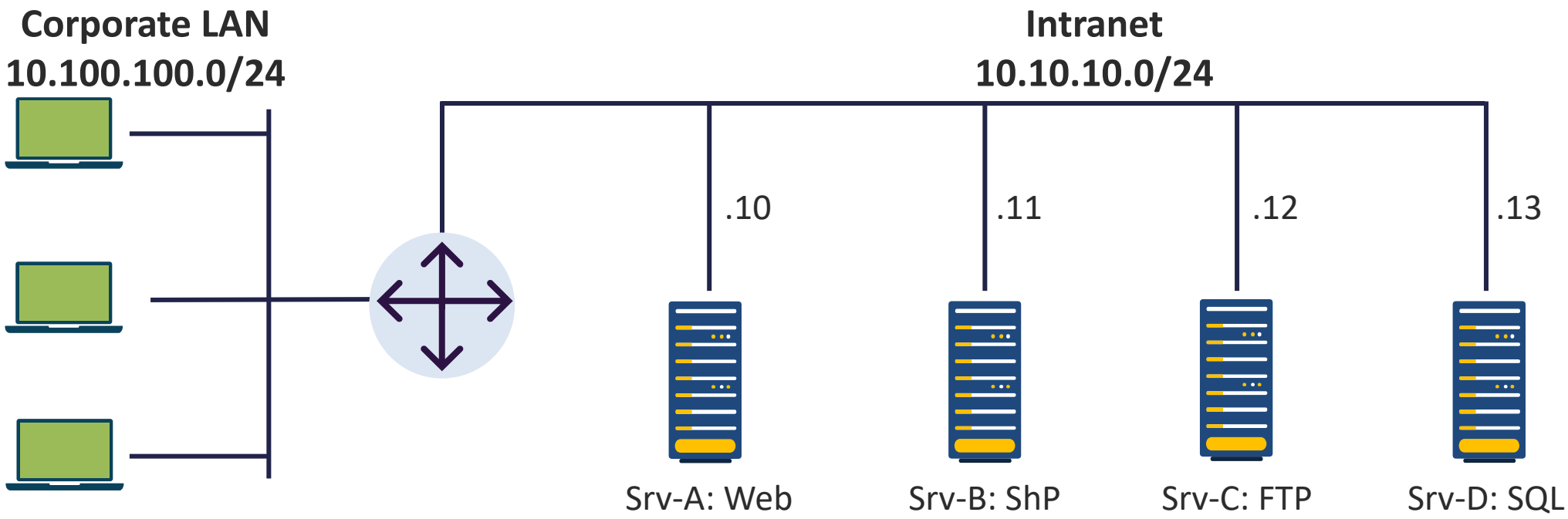
Objectives

- Survey rule-based, role-based, discretionary, mandatory, attribute-based, and risk-based controls
- Describe access policy enforcement and review
- Compare provisioning and deprovisioning
- Explain role definition, transition, privilege escalation, and service accounts management

Rule-based Access Control

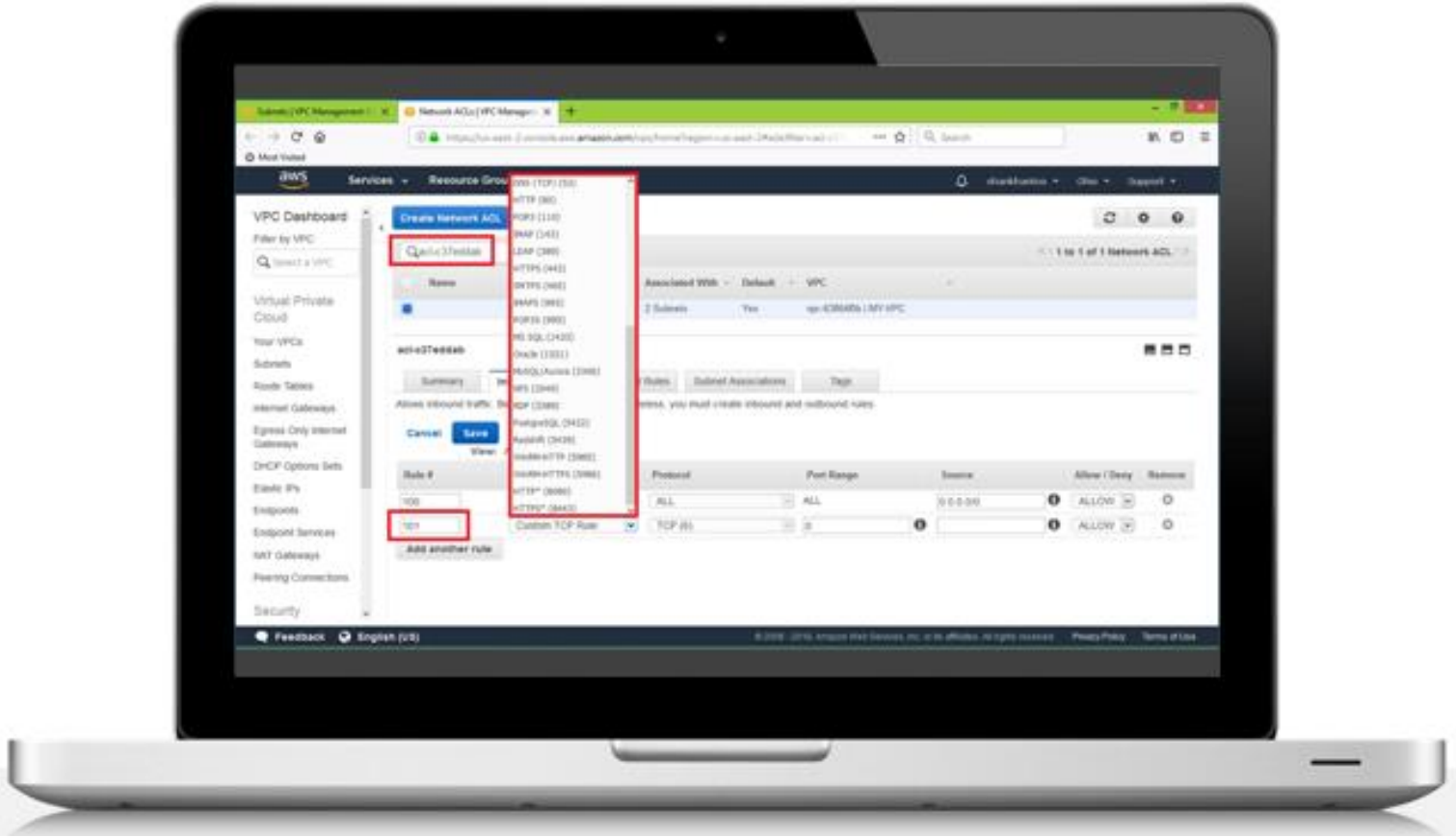
- Rule-based access control involves the static or dynamic assignment of allow/permit and deny statements in the form of an access list or ruleset
- It is based on criteria defined by the custodian or system administrator
- It could also be a time-based access control list (ACL) if Network Time Protocol (NTP) is being used
    - Example: A user is only allowed access to a drive on a server from 6 a.m. to 6 p.m. Monday through Friday
- It is common for infrastructure devices like routers, switches, and firewalls to use rule-based access controls

Rule-based Access Control List




```
access-list 100 permit tcp any 10.10.10.10 eq  www
access-list 100 permit tcp any 10.10.10.10 eq  443
access-list 100 permit tcp any 10.10.10.11 eq  www
access-list 100 permit tcp any 10.10.10.11 eq  443
access-list 100 permit tcp any 10.10.10.12 eq  ftp
access-list 100 permit tcp any 10.10.10.12 eq  ftp-data
access-list 100 deny ip any any log
```

Cloud Service Provider (CSP) Rule-based Network Access Control List (NACL)



Role-based Access Control (RBAC)

- With RBAC, access decisions rely on org chart, roles, responsibilities, or location in a user base or directory group
- The roles are usually set based on evaluating the essential objectives and architecture of the enterprise
- An RBAC framework is determined by security administrators, officers, or built-in to the system – not at the discretion of the user
- For example, in a medical center, the different roles may include doctor, RN, PA, specialist, technician, attendant, receptionist, etc.
- RBAC may also be integrated into a relational database management system (RDBMS)

RBAC Pros and Cons

- Easy to implement and control
- Roles are assigned using written security policy
- Built into many security frameworks
- Aligns with accepted security principles

- Scope creep can take place over time
- Roles and access must be audited rigorously
- Multitenancy capabilities need things like Active Directory (AD) organizational units (OUs)

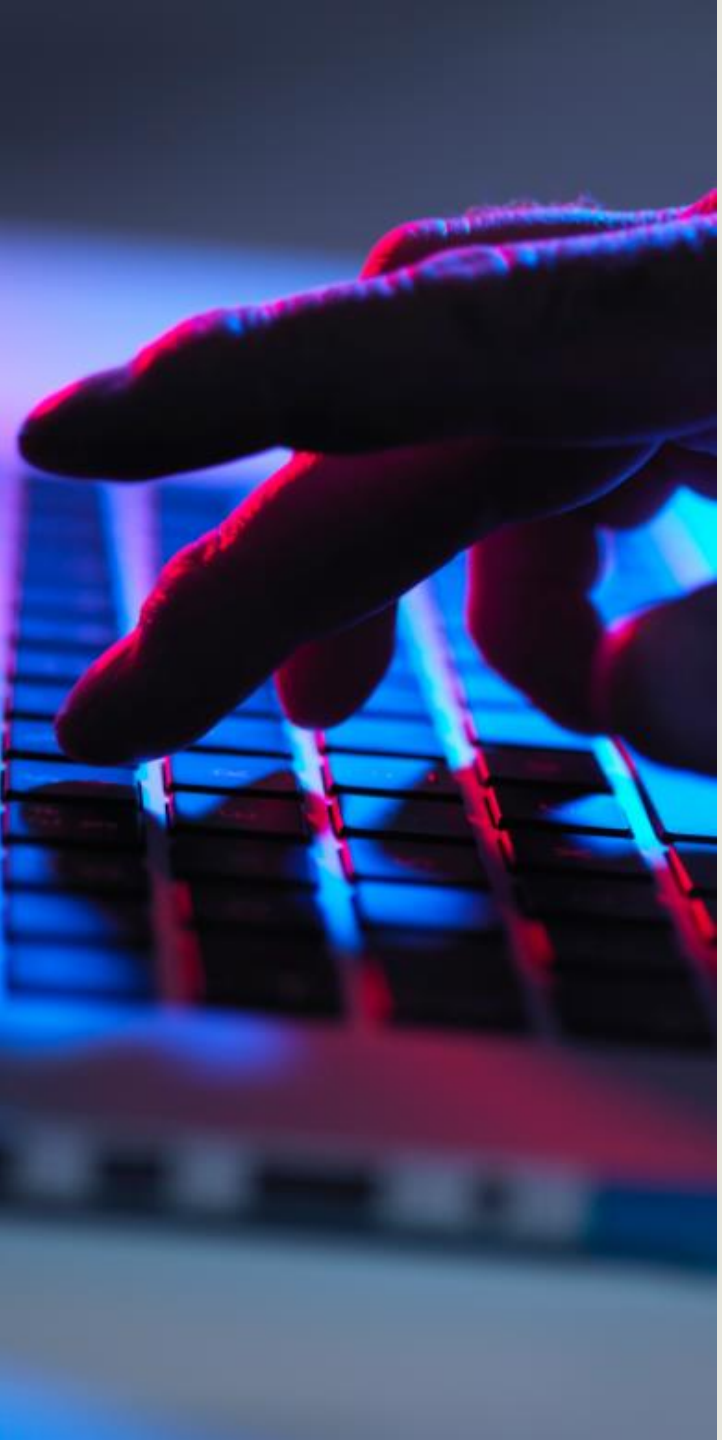
Working with Discretionary Access Controls (DAC)

In this demo…

We will explore examples of Discretionary Access Controls

Mandatory Access Control (MAC)

- MAC is strictly nondiscretionary and secures data by assigning sensitivity labels, then compares the labels to the level of subjects
  - MAC models are designed by "committee"
- It can be designed in a lattice structure with rules based on the levels directly above and below
- It is appropriate for extremely secure systems, such as multilevel secure military and government agency applications
- Its main advantage is that access based on "need to know" is strictly adhered to and scope creep is minimized



Mandatory Access Control

- NIST defines the MAC model as "an access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system
- A subject that has been granted access to information is constrained from doing any of the following:
  - Passing the information to unauthorized subjects or objects
  - Granting its privileges to other subjects
  - Changing one or more security attributes on subjects, objects, the information system, or system components
  - Choosing the security attributes to be associated with newly-created or modified objects
  - Changing the rules governing access control"

Bell-LaPadula

- All MAC systems are based on the Bell-LaPadula model for confidentiality
- This was the first mathematical model with a multilevel security policy used to define the concept of a secure state machine and models of outlined rules of access
- It focuses on ensuring that subjects with different clearances are properly authenticated by having the necessary security clearance, need to know, and formal access approval before accessing an object under different classification levels

Bell-LaPadula Ruleset

Simple security rule: A subject at a given security level cannot read data that resides at a higher security level (no read-up rule)

Strong star property rule: A subject who has read and write capabilities can only perform those functions at the same security level – nothing higher and nothing lower

Star property (*) rule: A subject at a given security level cannot write information to a lower security level (no write-down rule)

Tranquility principle: Subjects and objects cannot change their security levels once they have been instantiated (created)

*There is an **optional Discretionary Security Property** – if a subject (a Director) has a certain high-level access on an object, they can transfer rights to another (subject) of their choice. However, there must be a comprehensive access control matrix in place to document all the different permissions the subjects have.*

Biba Model

- Biba uses a lattice of integrity levels (unlike Bell-LaPadula)
- It is also an information flow model (like Bell-LaPadula) because it is most concerned about data flowing from one level to another
  - **Simple integrity rule** (no read down): States that a subject can not read data from a lower integrity level
  - **Star integrity rule** (no write up): States that a subject can not write data to an object at a higher integrity level
  - **Invocation property**: States that a subject cannot invoke (call upon) a subject at a higher integrity level

Clark-Wilson (C-W) Integrity Model

- Clark-Wilson was developed after Biba with the intention to improve on perceived weaknesses in that model
- The integrity goals of C-W are:
  - To prevent unauthorized users from making modifications
  - To ensure separation of duties prevents authorized users from making improper modifications
  - To confirm well-formed transactions and maintain internal and external consistency

Attribute-based Access Control (ABAC)

- ABAC weighs dynamic authorization profiles against the attributes of the subject's actions and requests
- ABAC relies upon evaluation of
  - People's characteristics
  - Attributes of IT components
  - Heuristics
  - Environmental factors and situational variables
  - User behavioral analysis (machine learning)
- ABAC systems can also enforce both DAC and MAC models

ABAC Attribute Categories

Actions: Specific actions such as copying, pasting, deleting, reading, or writing

Users/Subjects: The principal acting on the resource with attributes, like ID, job roles, and security clearance

Resources/Objects: Files, data blocks/volumes, blob data, applications, servers, and application programming interfaces (APIs) with attributes, such as creation date, owner, and data sensitivity that make them unique

Environmental: Includes contextual factors like time, location, communication channel, authentication factor, and the device being used or accessed

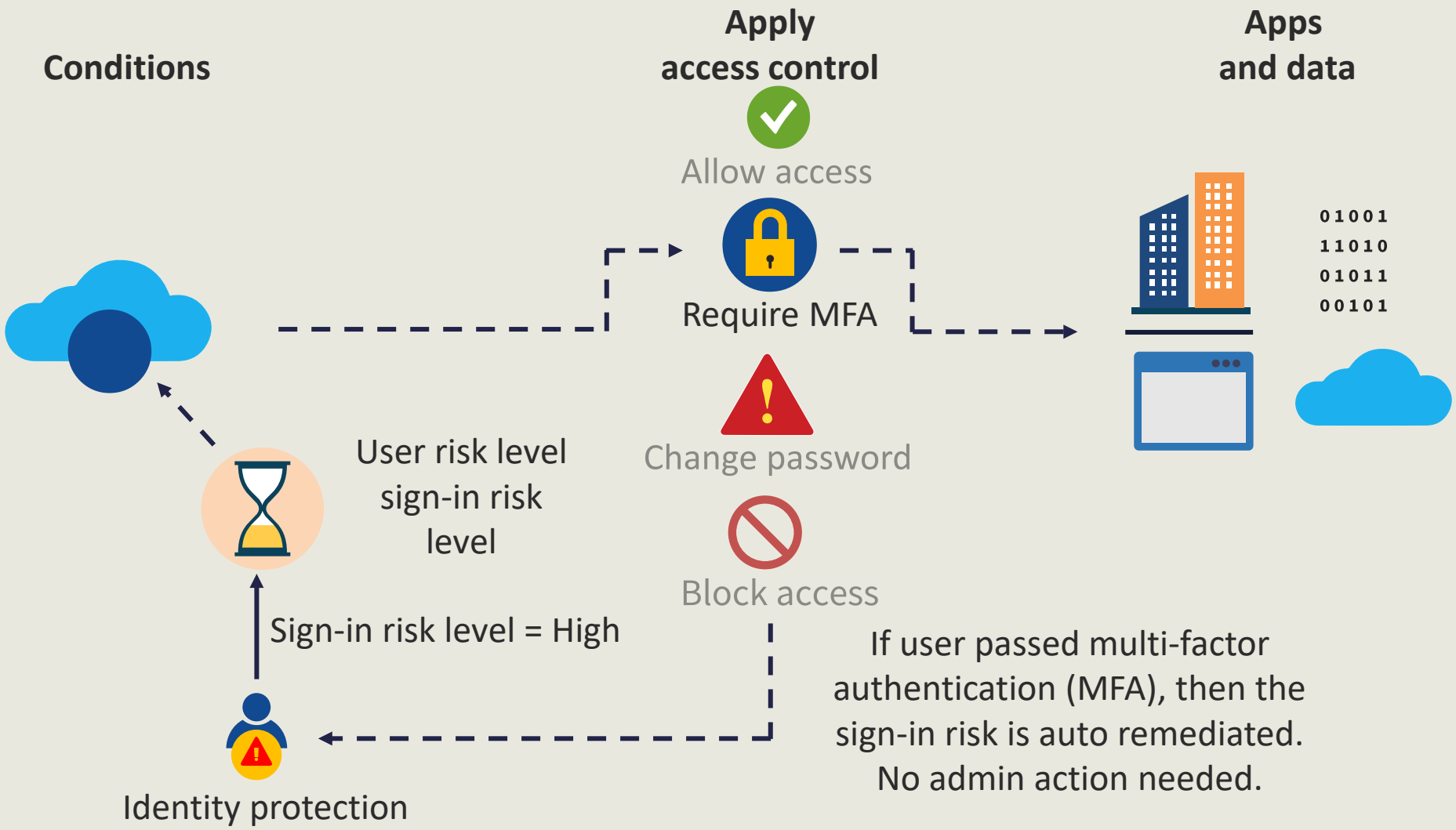
ABAC EXAMPLES

- Leveraging Cisco Identity Services Engine (ISE) to apply AuthN policies based on different variables and inserting security group tags into egress frames leaving switches
- Google BeyondCorp ZTNA in a software-defined network running on IEEE 802.1X
- CSP managed policies/roles such as AWS Verified Access CEDAR policies that customers can construct to provide attribute-based access to their own web applications and containers (serverless and server-based)

Risk-based Access Control

- Risk-based access control utilizes dynamic risk assessment to calculate the risk of certain transactions and activities
- It can be implemented in either a basic mode or the strong risk-access control mode
- This approach is a newer method for securing the most sensitive information by leveraging session attributes and user/device behavior monitoring
- It is often enhanced with advanced machine learning (ML) engines and AI tools for user and system behavioral analytics

Microsoft Entra ID Risk-based Access Control



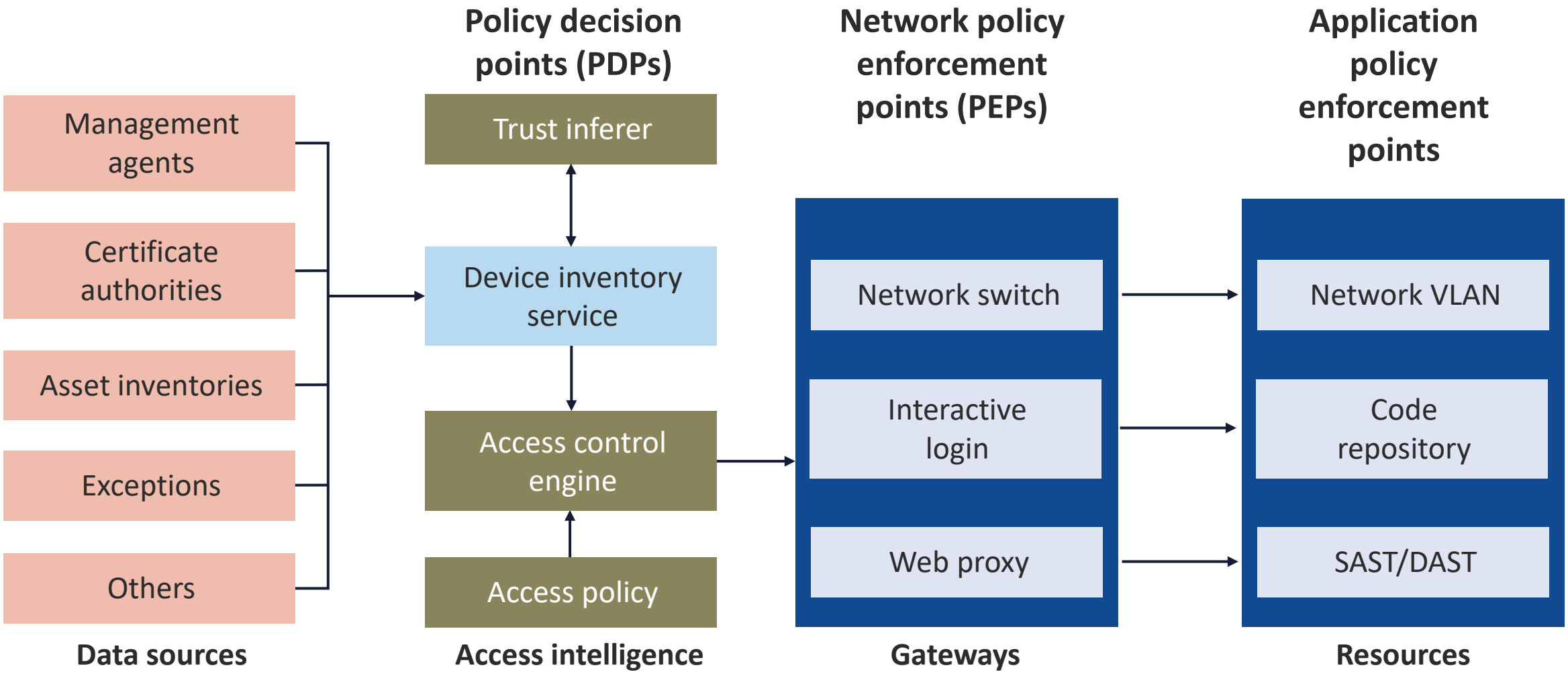
Access Policy Enforcement

- The emerging solution for enforcing access policies is Zero Trust
- Zero Trust Network Access (ZTNA) is the technology that empowers the implementation of a Zero Trust security model, which accepts the fact that threats exist both inside and outside a network
- A ZTNA initiative leverages policy decision points and policy enforcement points

7 Tenets of Zero Trust According to NIST SP 800-207

1. Rigorously enforce authentication and authorization
2. Maintain data integrity
3. Gather data for improved security
4. Consider every data source and computing device as a resource
5. Keep all communication secured regardless of network location
6. Grant resource access on a per-session basis
7. Moderate access with a dynamic policy

Google BeyondCorp Internal ZTNA Solution



Account Access Review

- Access reviews allow organizations to proficiently control:
  - Group membership
  - Admission to enterprise applications
  - Role assignments
- Microsoft Entra ID is an example of technology that empowers administrators to work together with users from inside the organization and with external users
- Users can join groups, invite guests, link to cloud apps, and be a teleworker from personal devices

Account Access Review

- User access must be revised frequently to assure that only the proper subjects have constant access
- Self-service portals allow for better access management functionalities
  - Ensuring that Joiners and Movers have the access they need to be productive
  - Making sure that old access is removed
- Administrators should also proactively engage with resource owners to assure they habitually review who has access to their resources

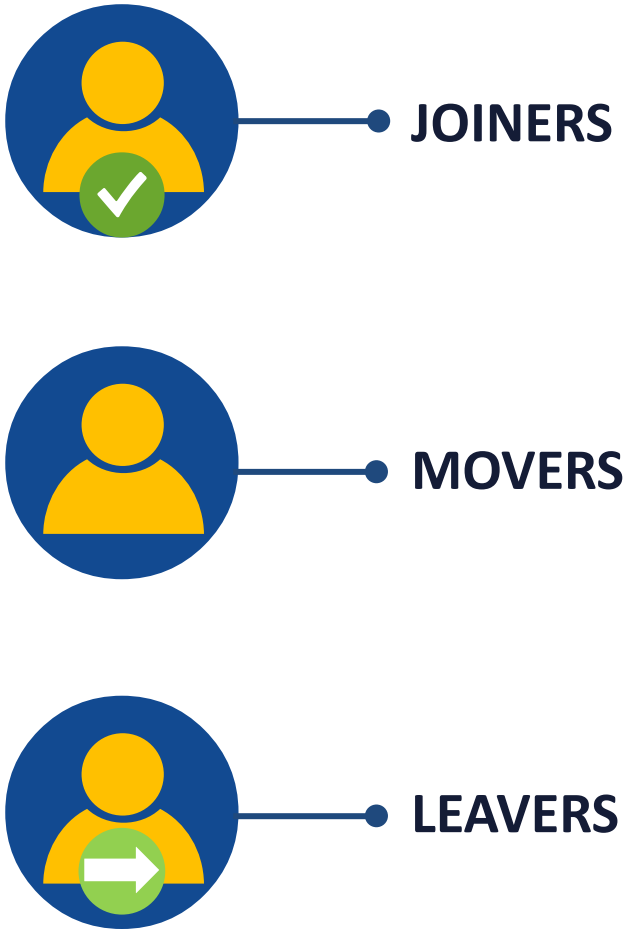
Account Access Practices

- Confirm that there are not too many users in privileged roles (especially with discretionary access control)
- Limit the number of users that are Global Administrators and/or root level Linux users
- All guest or partner accounts should be disabled and removed as soon as possible
- When automation is not possible, generate rules for dynamic membership on security groups
- Create a review process on groups to ensure that those who still need access keep access

Account Access Practices

- Ask group owners to periodically review the group membership before the group is used in a different risk context
  - This is critical in highly projectized organizations with a high degree of cross-functional activities
- For certain business critical resources such as business critical applications, compliance processes may demand regular reconfirmation and justification for continued access

Identity Types



Provisioning (Onboarding)

- Identity management (IdM) provisioning involves administering user accounts and assigning of access privileges, typically by group membership
- Onboarding of devices and certificates is often handled using the mobile device management (MDM) team of enterprise mobility management (EMM)

Provisioning (Onboarding)

- When done correctly, a standardized and automated service desk is used for on-boarding, transfers, sporadic access audits, and off-boarding of
  - Organizational employees and contractors
  - Third-party business partners
  - Customers

Key Challenges

- Ever-increasing costs of user account management and help desk/service desk implementations
- Low priority for proper account creation, approval processes, and auditing
- High cost of constant compliance audits of user account administration practices
- Complicated provisioning processes that are unique to different business applications, systems, and platforms
- Lack of timely account suspension and deletion policies and processes for terminated groups and users

Deprovisioning (Offboarding)

- When users no longer need access due to job changes (transfer) or termination, deprovisioning involves revoking access and disabling accounts
- This assists in countering the risk of orphaned accounts with needless privileges
- According to the Identity Management Institute almost 49% of former employees log back into their accounts after offboarding

Deprovisioning (Offboarding)

- Deprovisioning averts unauthorized access by completely revoking privileges as soon as a subject leaves or moves
- Like provisioning and continuous certification, deprovisioning should be automated to offload the tedious tasks of revoking permissions and deleting roles
- This is especially critical when the employee leaves under less than positive circumstances
- Adhering to identity management best practices keeps your organization safe from advanced persistent threats

Role Definitions

- **Officers**
  - Member of executive management or "C-suite" or "C-team" that is ultimately responsible for due diligence and due care of security governance
- **Owners**
  - May own the physical or digital asset in some enterprises
  - May assign rights and permissions (sharing) in a DAC model
  - May assign tags and classification levels

Role Definitions

- **Custodians (or Controllers)**
  - The keepers of the asset or information from a technical and tactical perspective
  - Maintain confidentiality, integrity, availability, authenticity, and non-repudiation services
- **Stewards**
  - Manage the asset, data, and metadata from a business perspective
  - Ensure compliance (standards/controls) and quality control
  - More likely to interface with internal and external customers as a program or product manager
  - Stewards may also be digital asset managers for IRM

RACI Charts

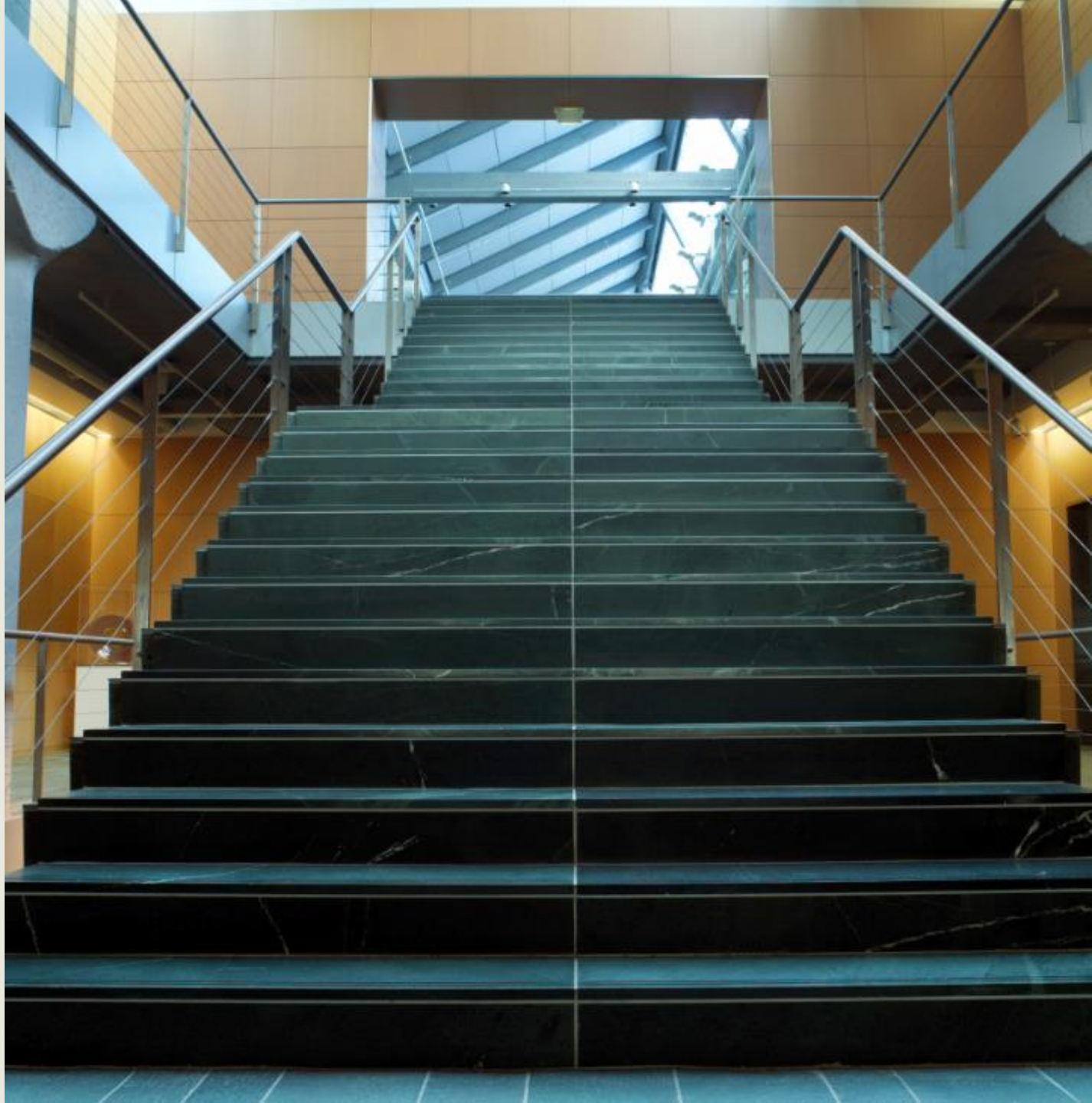
R – Responsible **A** – Accountable **C** – Consulted **I** – Informed

	GRC* Department	Legal Department	Security Team	IT Operations
Establish the provider requirements	R/A	C	C	I
Build the governance scheme	R/A	C	C	I
Assess cloud vendor	A	I	R	R
Build the architecture	I	I	A/R	R
Conduct cloud migration	I	I	C	A/R

**GRC – Governance, Risk, and Compliance*

Privilege Escalation

- Increasing access permissions for trusted users to complete specific tasks based on:
  - Ad hoc elevation
  - Part of a service desk implementation
  - The discretion of a resource object owner
- Gaining unauthorized privileged access into a system
- An aspect of the cyber kill chain when the attacker accesses a system with limited privileges and then elevates access rights to get more unauthorized control



Examples of Privilege Escalation (elevation)

- When a Windows Local or Domain Administrator switches to "Run As…" from their normal user account to conduct privileged actions
- A situation where a Linux user runs "sudo" (which either stands for "substitute user do" or "super user do") to run a program as another user – often the root user
- Attackers conduct credential exploitation to leverage weak passwords or steal credentials from known IT administrators

More Examples of Privilege Escalation

- A kernel exploit to target weaknesses at the core of an O/S, letting attackers escalate privileges
- Attackers exploit unpatched vulnerabilities in applications or the operating system
- Weak service configurations are abused and exploited to sidestep privilege controls
- Using a tool like Mimikatz to extract plaintext passwords and hashes from random memory to empower privilege escalation

Service Accounts Management

- A service account is a user account generated to offer a security context for services running on network operating systems like Windows and Red Hat Enterprise Linux (RHEL)
- In a nutshell, service accounts are non-human accounts instantiated specifically to aid communication and interaction between different applications, systems, or services
- Service accounts are not like user accounts associated with human users and can be a vulnerability if not managed closely

Service Accounts Management

- These accounts dictate the ability of the service to access local and network resources
  - Directory servers
  - Web servers
  - Email servers
  - Messaging and conferencing servers
  - Load balancers
  - Domain name service (DNS) servers
  - Dynamic Host Configuration Protocol (DHCP) servers
  - NTP servers

Types of Windows Service Accounts

- **Standalone Managed Service Accounts** are meant for isolating domain accounts in critical applications, like IIS, SharePoint, and Exchange
  - These can be utilized for services on a single system, but they cannot be shared between multiple servers or used in replicating server clusters with multiple nodes
- **Group-managed Service Accounts** are managed domain or realm accounts that offer automatic password management and extended functionality over multiple servers in a domain

Types of Windows Service Accounts

- **Virtual Service Accounts** are generated automatically by the operating system for service activities
  - They use the computer's account as their security context and simplify configuration by removing the need to manually manage account credentials
  - These service accounts are excellent for services that run under a Local System or Network Service account in hypervisor and virtual machine environments

RHEL Service Accounts

- Administrators will create service accounts on the Red Hat Hybrid Cloud Console for the following use cases:
  - The application or service must access certain resources
  - The application or service needs to access resources without human involvement
  - The application or service needs to access resources from multiple locations

Security Audit & Controls Testing

Objectives

- Describe internal, external, third-party audits and controls testing locations
- Explain vulnerability assessment and penetration testing
- Describe log and code reviews and testing
- Learn about synthetic transactions, benchmarks, misuse case testing, coverage analysis, and interface testing
- Explain compliance checks

Internal Audits

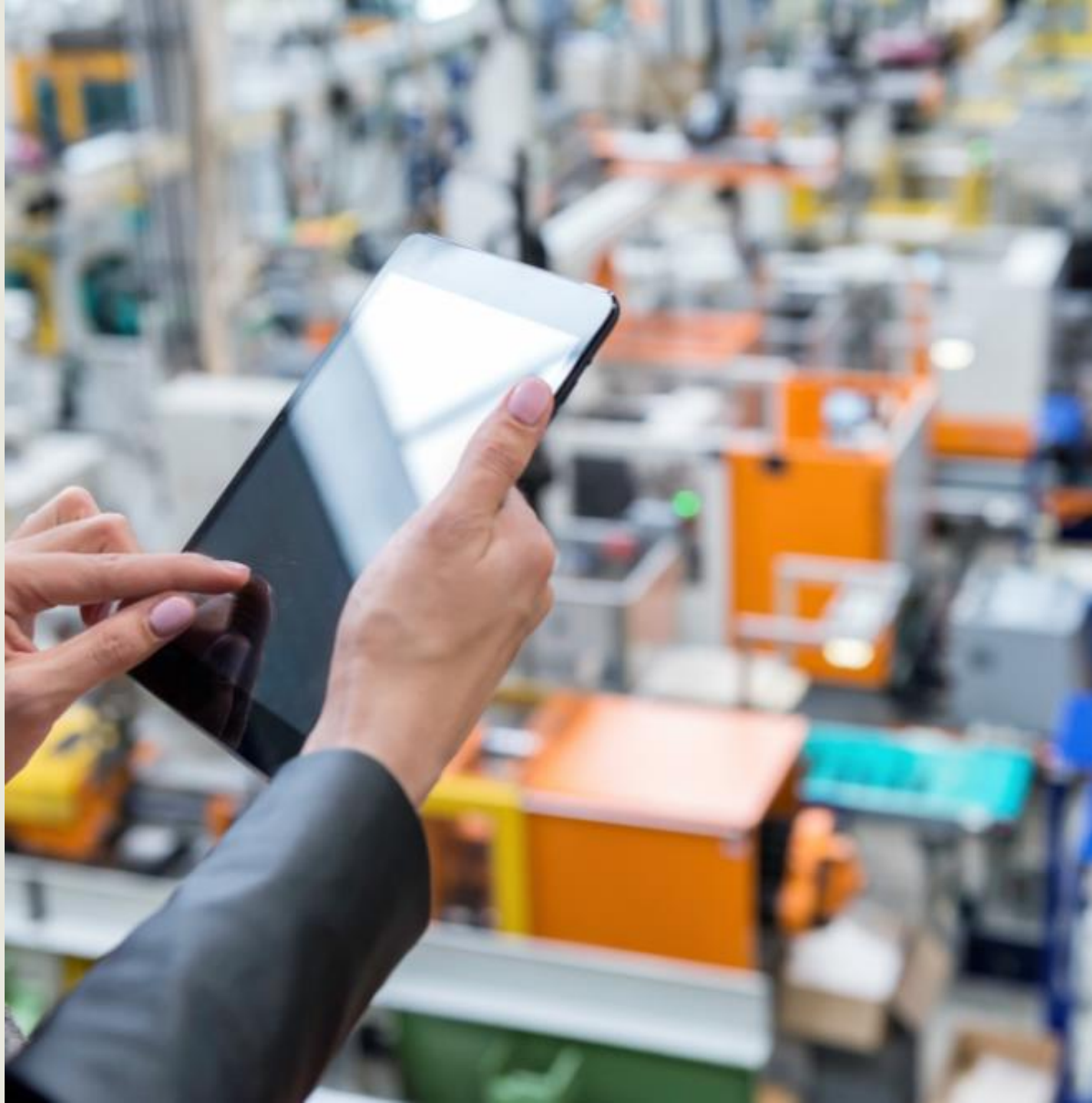
- An internal security audit (cybersecurity audit) is a complete examination of an organization's information systems
- This assessment commonly evaluates system and application security against a baseline or checklist of industry best practices, recognized standards, matrices, and government regulations
- Internal audits are typically self-assessments conducted by objective stakeholders using established key indicators and metrics

Internal Audits

- A comprehensive security audit will commonly measure the security controls based on:
  - Physical aspects of the system and facility environments in which the hardware is housed
  - Application and systems security patches, upgrades, and updates based on implemented policies
  - Known and yet-to-be-discovered vulnerabilities and weaknesses in configurations and implementation

Internal Audits

- A comprehensive security audit will commonly measure the security controls based on:
  - Gap analysis and maturity modeling of all security governance strategies
  - The way that employees create, use, store, and share sensitive information and data
  - The organization's overall security strategy, posture, maturity level, policies, initiatives, and security control assessments



External Audits

- Some security-centric audits may also be a part of formal external or compliance audits
- These are conducted by a third-party audit team (a regulator or insurer for instance) with the goal of certifying against ISO 27001 or getting a SOC 2 attestation

External Audits

- External audits can often include:
  - Compliance attestation and certification
  - Insurers determining policies and premiums
  - Penetration testing and vulnerability assessment team
  - Corporate threat-hunting teams
  - Financial and accounting audits
  - Investigations from government agencies or departments
  - Tax audits

Third-party Audits

- A third-party audit can also be a type of external audit
- The key differentiator is that these audits are completely out of an organization's control
- Third-party audits can be unwanted and conducted by law enforcement or other government interventions
- These may result in invasive legal holds on data or information
- They can lead to temporary or permanent disruption of the organization

On-premises Auditing and Controls Testing

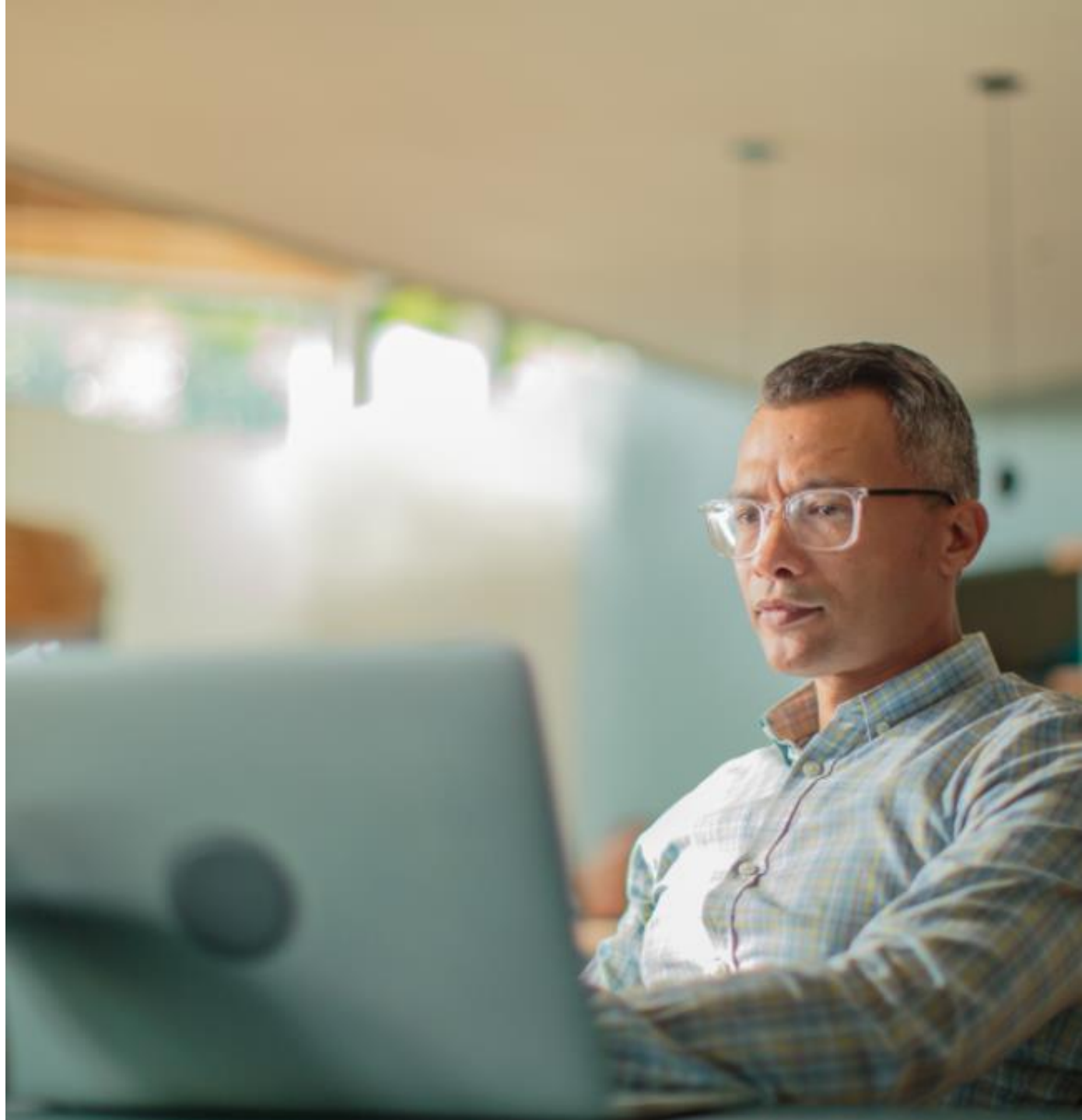
- The auditing process is much like any other initiative in that it needs strategic planning, due diligence, tactical optimization, and continual iterative improvement (i.e., due care)
- A security control assessment (SCA) is a formal test of a system against a pre-defined set of metrics
- It is performed in, with, or independently of a full security test and evaluation (ST&E), which is performed as part of an official security authorization

On-premises Auditing and Controls Testing

- These tests will appraise the operational plan (or planned implementation) of controls
- The results are a risk assessment report that represents a gap analysis documenting the system, application, or data risk
- Tests conducted should include audits, security reviews, vulnerability scanning, and penetration testing

The Capability Maturity Model (CMM)

- The Capability Maturity Model (CMM) is a methodology used to advance and enhance an organization's software development process
- The model consists of a five-level evolutionary path of progressively prepared and systematically more mature processes
- It is like ISO 9001 standards that specify an effective quality system for manufacturing and service industries



Capability Maturity Model

Initial (chaotic): Chaotic, ad hoc, individual heroics
Level 1

Repeatable (implicit): Process is not codified or defined and is still vulnerable to inconsistency
Level 2

Defined (early explicit): Process is defined and documented as a standard business process
Level 3

Managed (mature explicit): Process is controlled and can be adjusted or adapted to projects without measurable losses of quality
Level 4

Optimized (purely explicit): Process management results in deliberate process optimization and improvement
Level 5

Public and Hybrid Cloud Auditing and Controls Testing: CIS

- The Center for Internet Security (CIS) is a common source for auditing security controls
- CIS Benchmarks are best practices to securely configure various systems and are available for more than 140 technologies
- CIS Benchmarks are security configuration guides created by government, business, industry, and academia
- These are established using a special method constructed from an accord of global cybersecurity experts from across the globe

Public and Hybrid Cloud Auditing and Controls Testing: CSA

- The dominant methodology for auditing and testing public cloud controls comes from the CSA
- The Cloud Controls Matrix (CCM) is 197 control objectives structured in 17 domains covering all key aspects of cloud technology
  - It is often used for the systematic assessment of a cloud implementation
  - It is considered the de facto standard for cloud security assurance and compliance
- The STAR Level 1: Security Questionnaire (CAIQ v4) offers an industry-accepted way evaluate cloud services

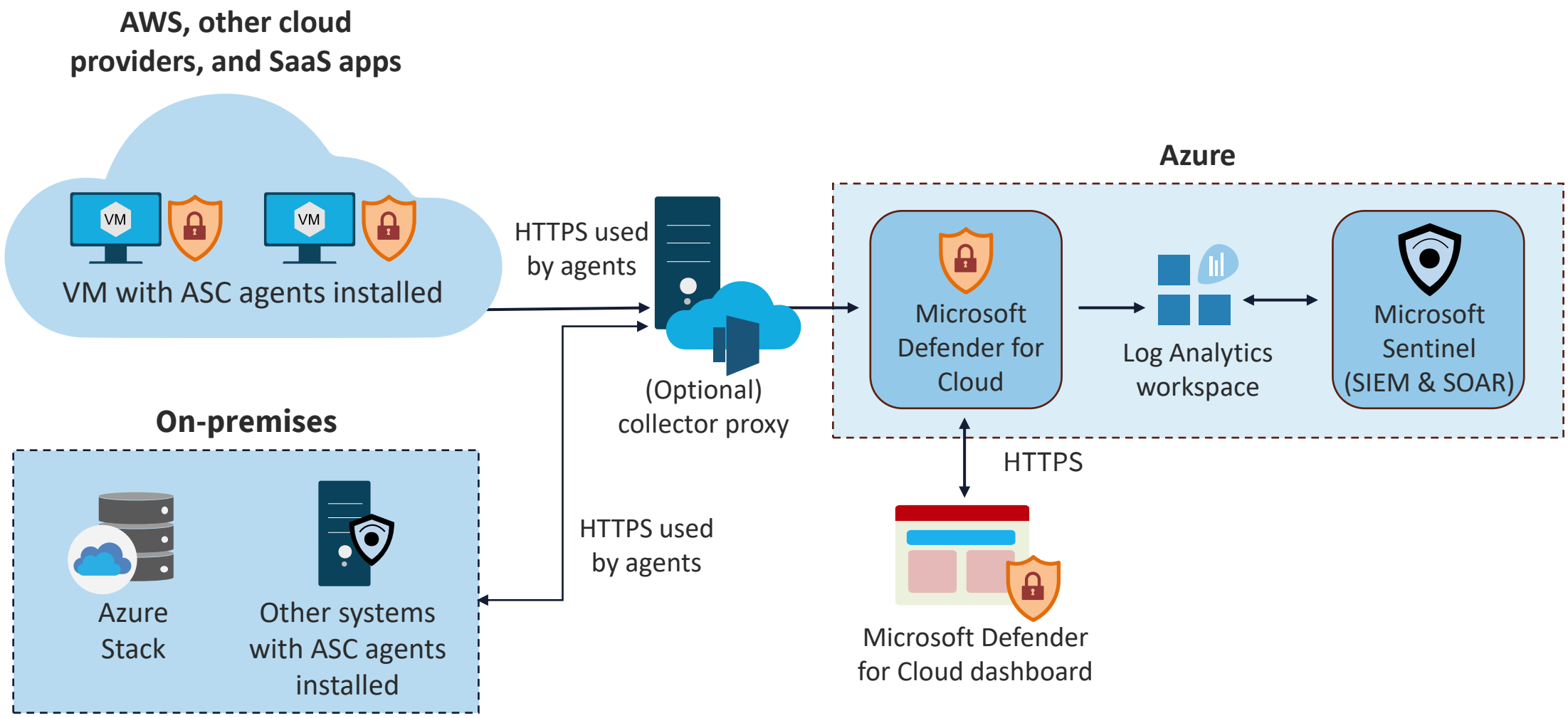
Metrics Cloud Auditing and Controls Testing: CCM Domains

1. Audit & Assurance (A&A)
2. Application & Interface Security (AIS)
3. Business Continuity Management and Operational Resilience (BCR)
4. Change Control and Configuration Management (CCC)
5. Cryptography, Encryption & Key Management (CEK)
6. Datacenter Security (DCS)
7. Data Security and Privacy Lifecycle Management (DSP)
8. Governance, Risk Management and Compliance (GRC)
9. Human Resources (HRS)

Metrics Cloud Auditing and Controls Testing: CCM Domains

10. Identity and Access Management (IAM)
11. Interoperability and Portability (IPY)
12. The Infrastructure and Virtualization Security (IVS)
13. Logging and Monitoring (LOG)
14. Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
15. Supply Chain Management Transparency and Accountability (STA)
16. Threat and Vulnerability Management (TVM)
17. Universal Endpoint Management (UEM)

Hybrid Cloud Analysis with Azure Sentinel



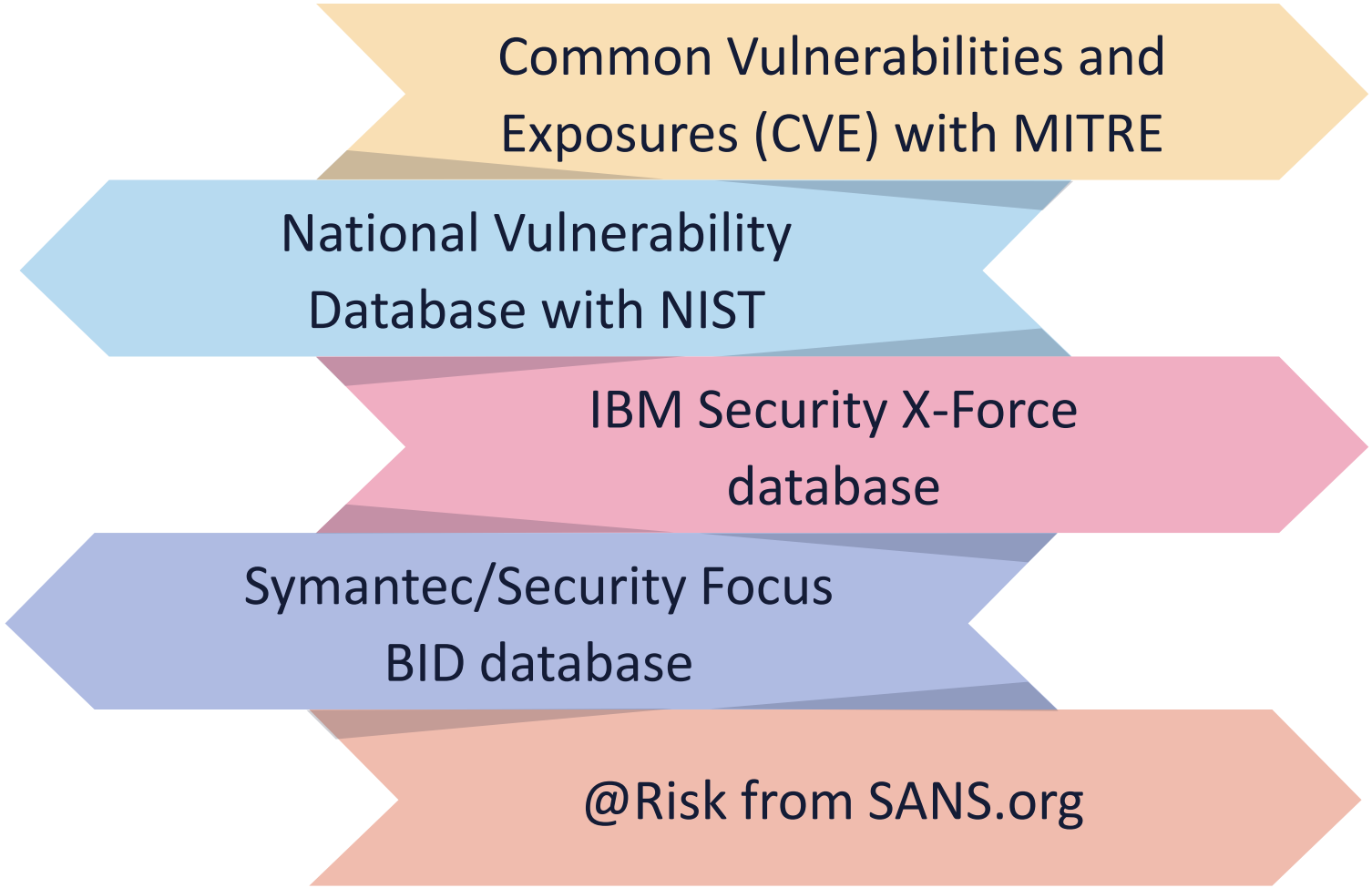
Vulnerability Assessment

- A vulnerability assessment is best quantified as a percentage of probability and not just a vague list of "scary things"
- It involves the likelihood that a threat agent's actions will result in a loss (frequency and magnitude)
- It can be a derived value from the threat capability of actors combined with the resistance of existing security controls
- A vulnerability assessment and scanning is typically a regularly scheduled and highly automated processes

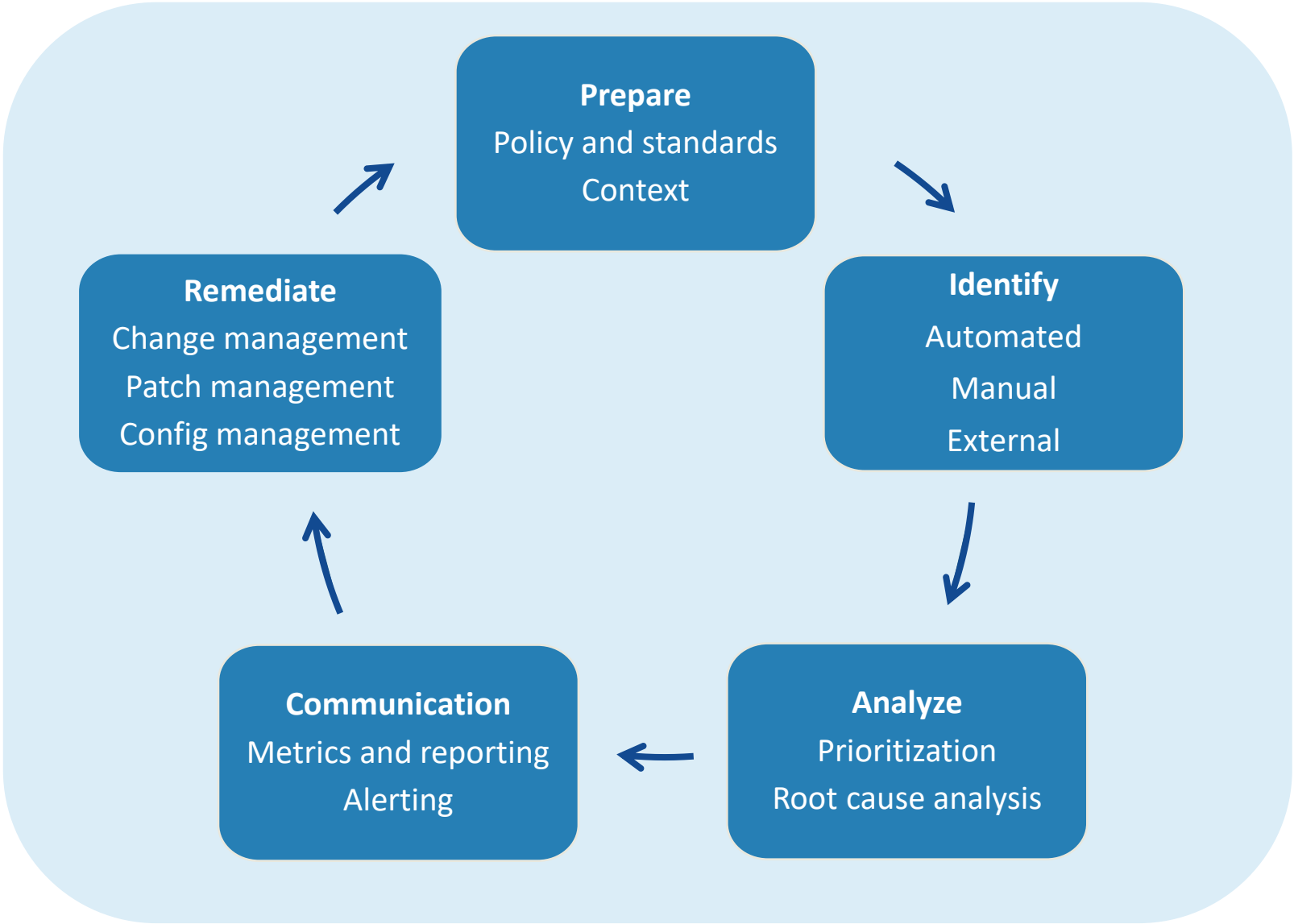
Vulnerability Assessment Sources and Tools

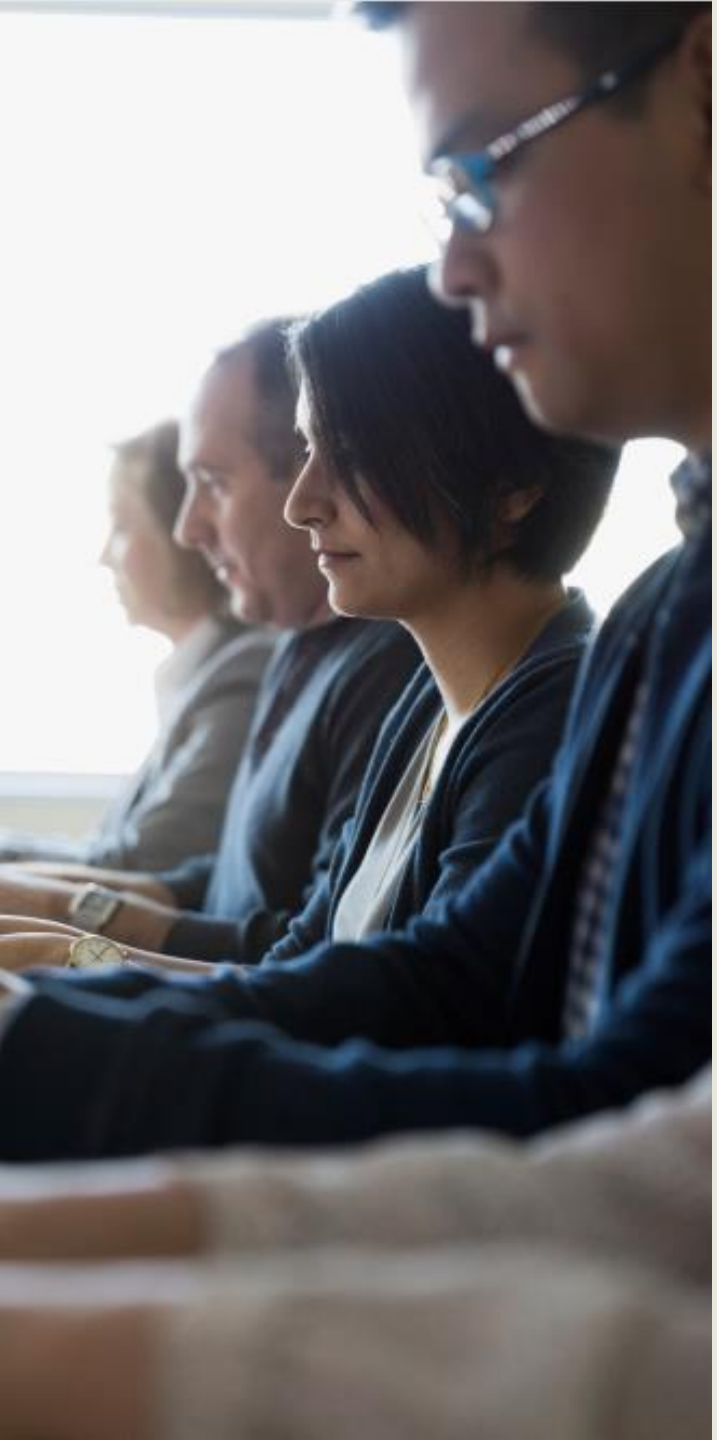
- Security, application, and system logs (e.g., syslog)
- SNMP traps and informs
- NetFlow collection
- Next-gen IPS and EDR alerts and logging
- Scanners like ZAP and Burp Suite
- Exploit kits (e.g., Parrot, Kali)
- SIEM and SOAR systems
- Vulnerability databases (e.g., MITRE, NVD, Cisco, PAN)

Vulnerability Databases



Vulnerability Assessment Life Cycle

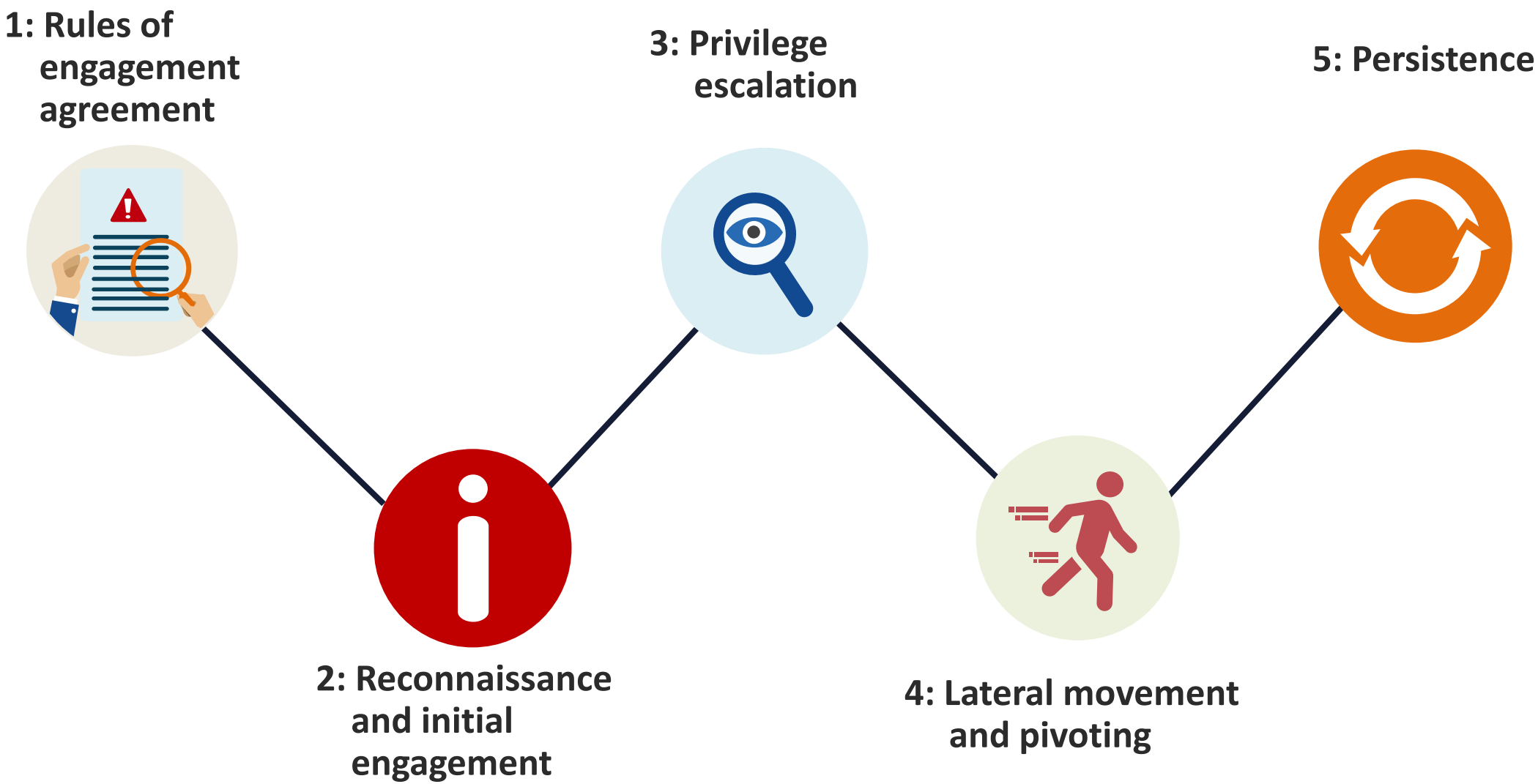


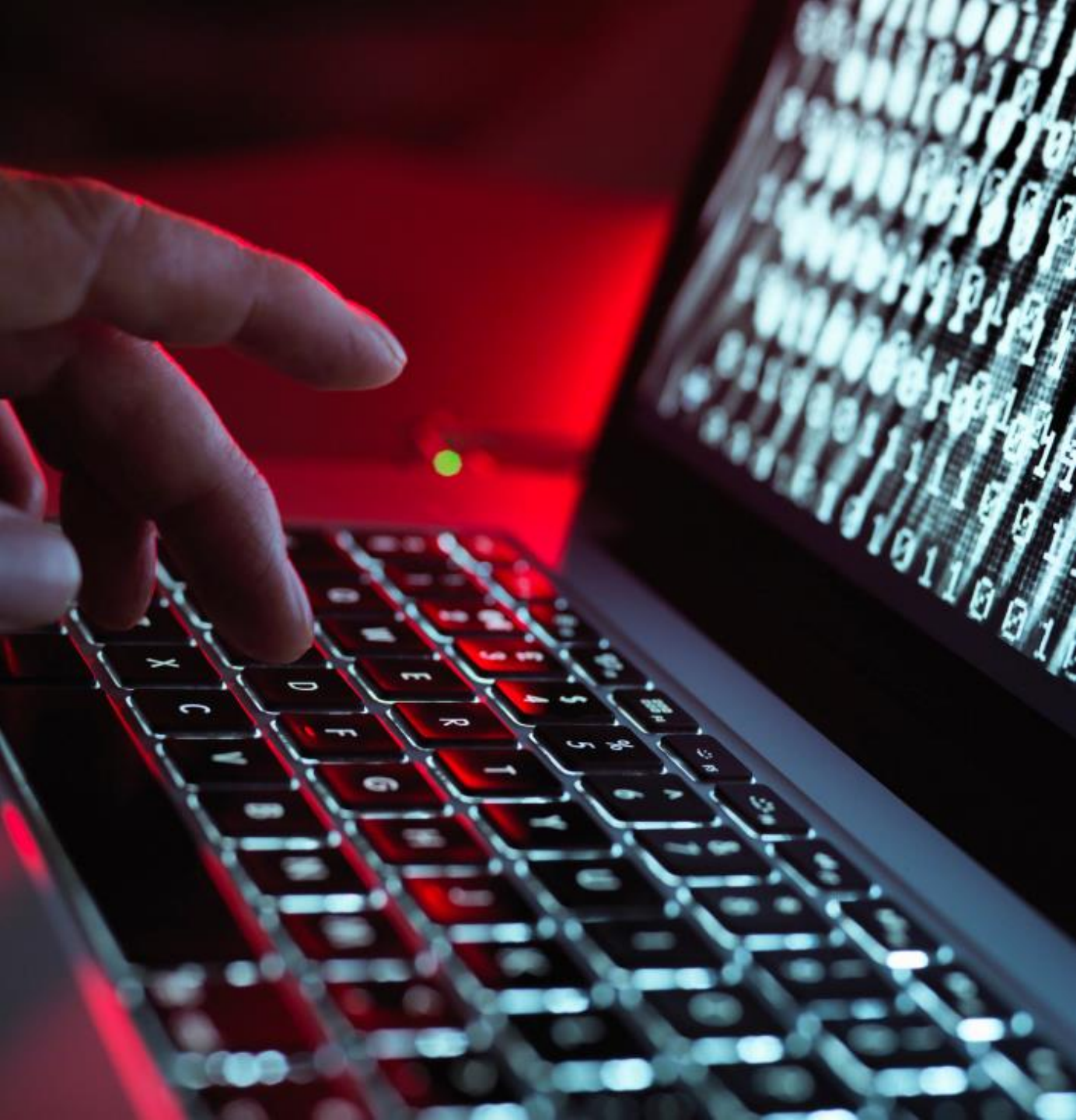


Penetration Testing

- Pen testing is a more elaborate test in which assessors simulate real-world attacks to identify methods for evading the security features of an application, system, or network
- It often involves launching real attacks on real systems and data using attack tools and techniques
- It can be very useful for determining the following:
  - How well the system tolerates real-world style attack patterns
  - The likely level of sophistication an attacker needs to successfully compromise
    the system
  - Additional countermeasures that could mitigate threats against the system
  - The defenders' abilities to detect attacks and respond

Penetration Testing Life Cycle

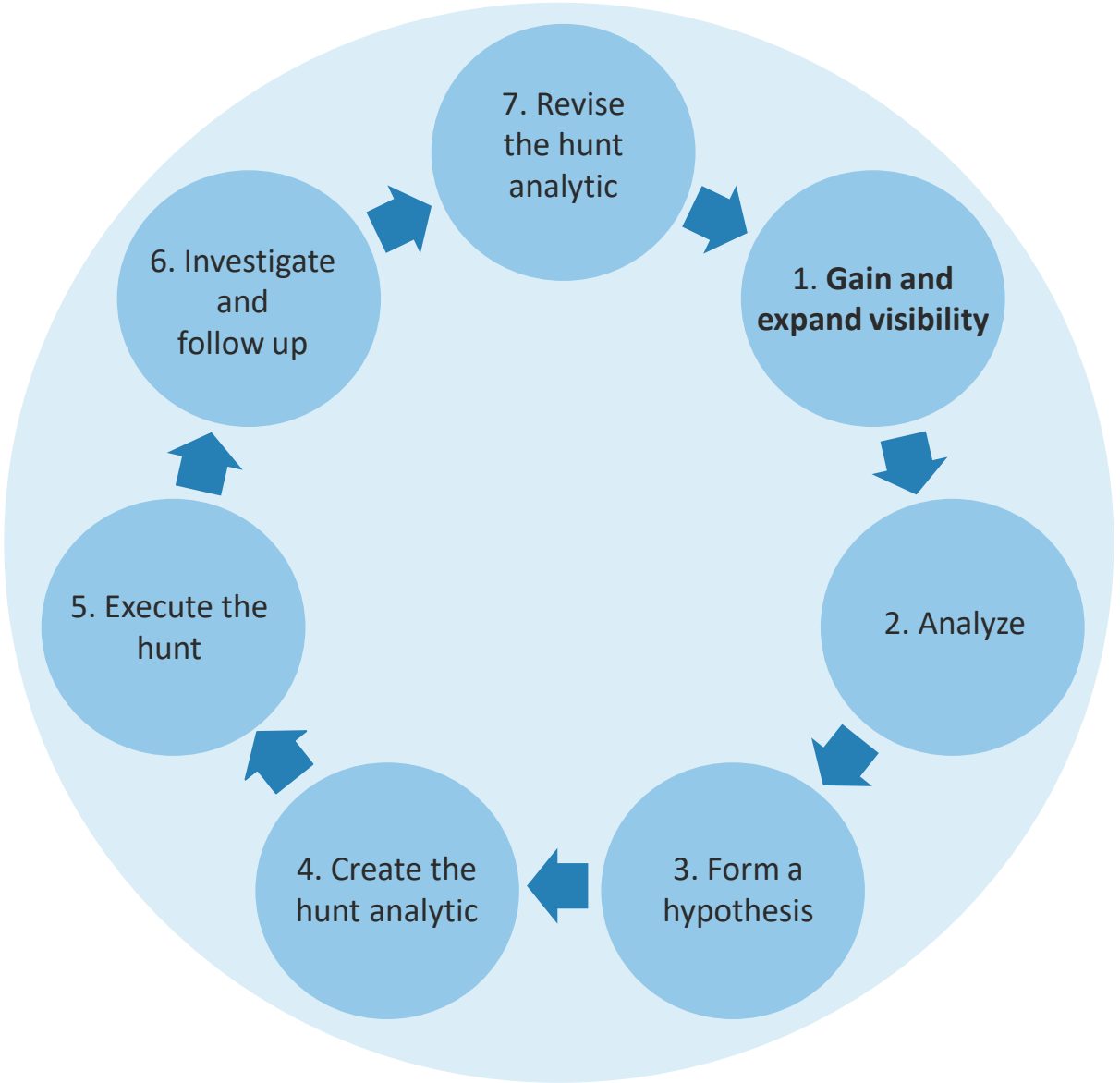




Threat Hunting

- Also called "hunt teams"
- Threat hunting involves groups of cyber investigators aggressively seeking out threats on a network or system
- They may also be compliance/regulatory auditors or insurance company teams
- They attempt to quickly recognize anomalies and discover historic patterns in data and indicators of compromise (IoCs) to counter cybercriminals and mitigate threats
  - Red teams are the attackers
  - Blue teams are the defenders
  - Purple teams are the observers and analysts

Threat Hunting Life Cycle



Log Reviews

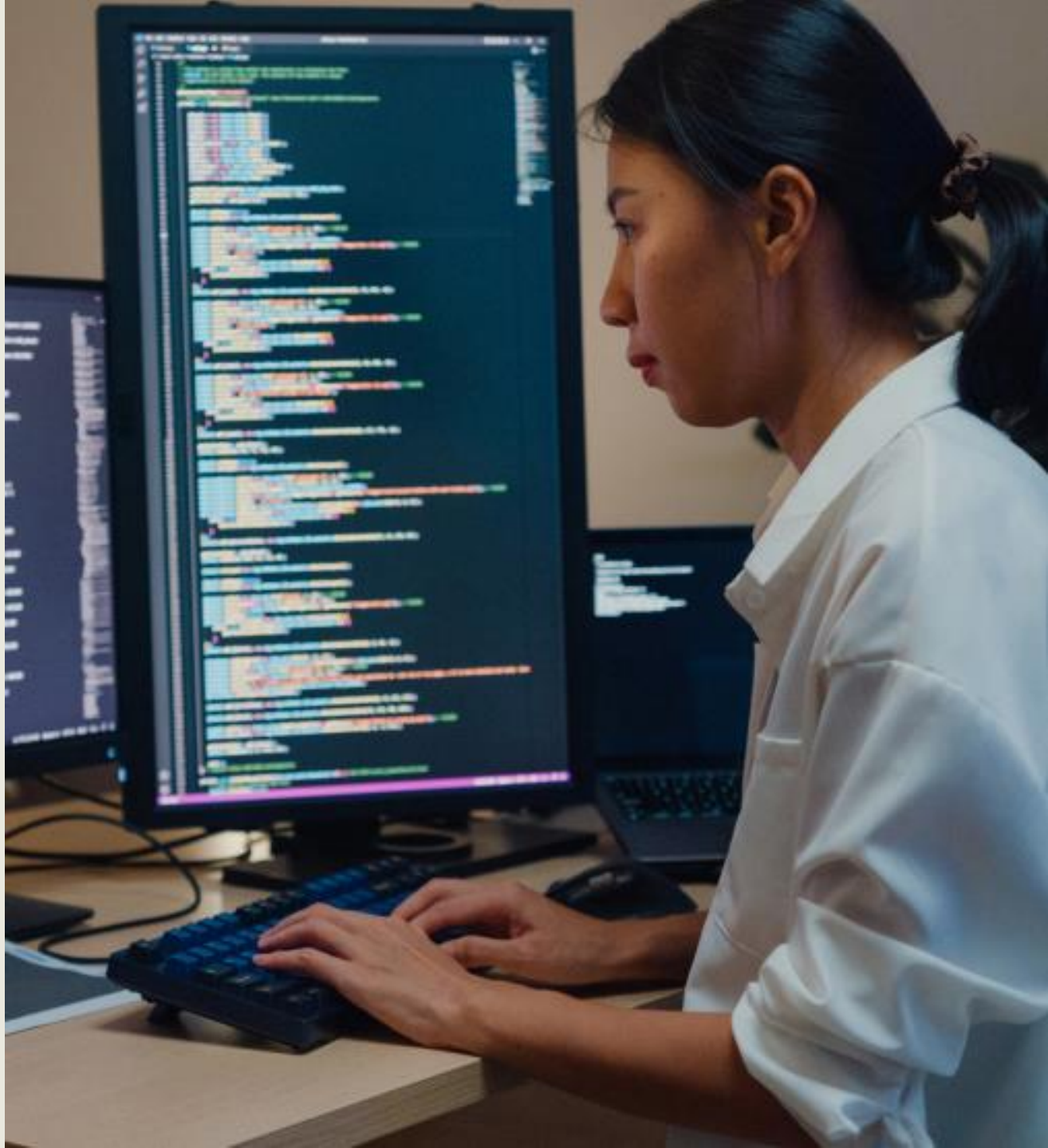
- Security managers must do much more than simply collect logs and event data
- Many will fill terabytes of RAID arrays with logs from IPS/EDR systems and anti-virus solutions without performing meaningful reviews and analysis
- Although it is critical to collect as much data as possible in the beginning, administrators should quickly filter and sift out the meaningful information, leading to knowledge and wisdom

Log Data

- What events and incidents have occurred?
  - Isolate, aggregate, correlate, and deduplicate the pertinent error messages, event IDs, etc.
- What applications, systems, and services were affected?
  - Logs must collect relevant system names and IP addresses, dependencies
- When did it happen?
  - There should be a secure NTP system to create accurate time and date stamps synchronized with a centralized atomic clock
- Who was logged in?
  - Events should be mapped to a unique ID
  - Have logs or logins been erased or deleted?

Code Review and Testing: SAST

- Static application security testing (SAST) tools are also known as code analyzers that conduct a direct white-box analysis of the application source code
- The analysis runs on a static view of code, in that the code is not running at the time of the assessment
- SAST security tools are mainstream and are widely adopted throughout the software industry
- They have broad programming language support and use concepts that are relatively easy to comprehend
- SAST code analyzers have no visibility of the execution flow, can be slow, inaccurate, and outdated, and often need additional customization and/or tuning



Code Review and Testing: DAST

- Dynamic application security testing (DAST) tools are most often web scanners like OWASP ZAP and Burp Suite (i.e., vulnerability scanners)
- When compared to SAST, they perform black-box analysis in that they do not have access to the code or the implementation specifics
- DASTs only inspect the system's responses to a series of tests designed to highlight vulnerabilities
- They function independently of the underlying application platform and offer solid support for manual pen testing
- A top-level DAST detects only ~20% of issues, and an experienced security background is needed to interpret the results

Code Review and Testing: IAST

- Interactive application security testing (IAST) combines the advantages of a SAST and a DAST solution offering:
  - The benefits of a static view, because they can see the source code
  - The benefits of a web scanner approach, since they see the execution flow of the application during runtime
- It can detect ~100% of OWASP benchmark in real-time with no false positives and is proper for QA and production environments, analyzing dependencies as well as legacy components
- There is no need to scan or attack the application
- IAST integrates and communicates with task management systems to create unified workflows

Code Review and Testing: RASP

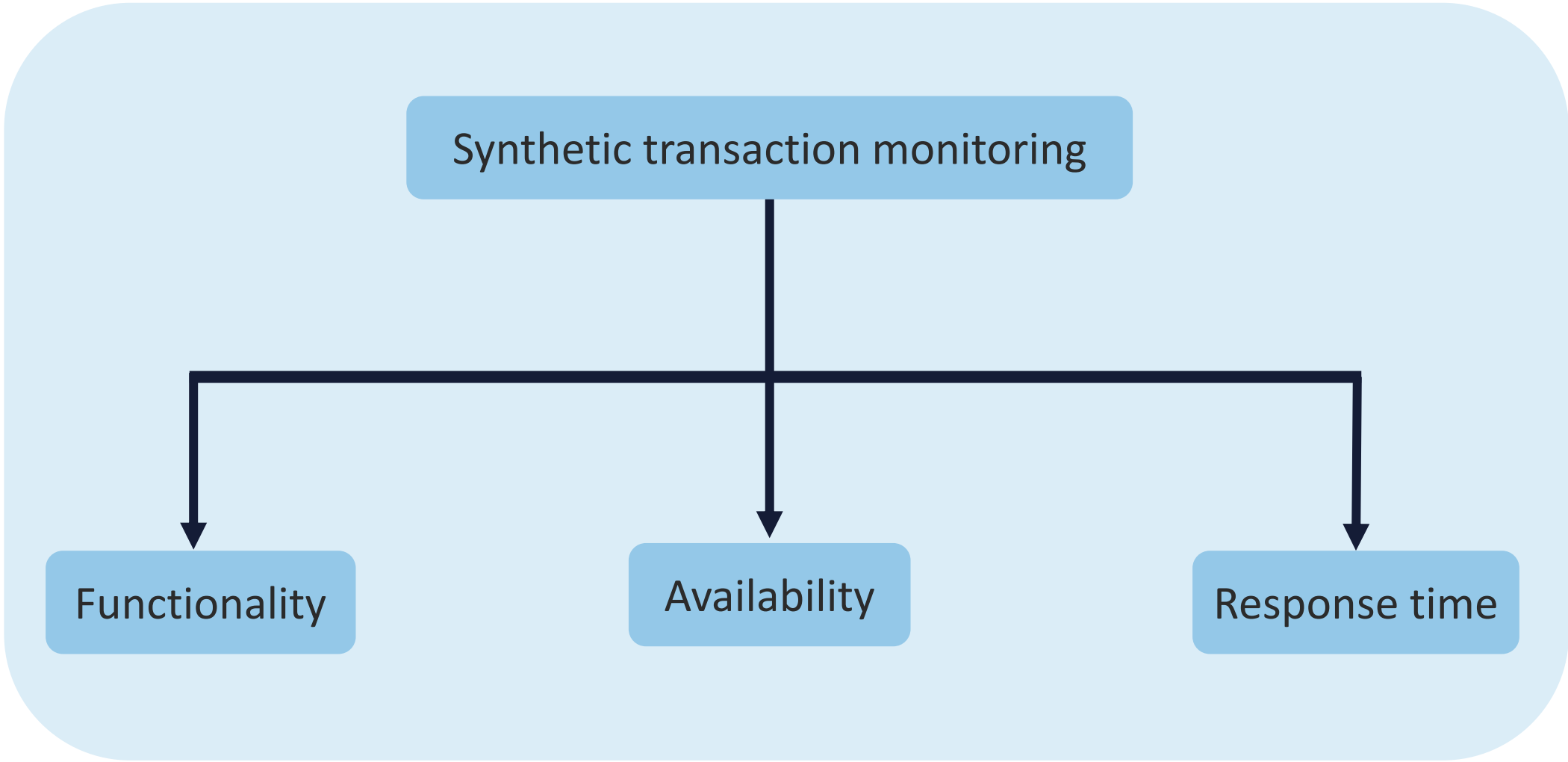
- Runtime application self-protection (RASP) is a newer approach to protect running applications
- As opposed to a web application firewall (WAF) perimetral approach, a RASP solution protects applications from the inside
- It has better visibility of the dataflow and the consequences of each input that the application gets
- RASP is key for groups involved in Agile and CI/CD SDLC

Code Repository Security

- Application code is only as secure as the methods and systems used to generate it
- Some of the advantages that come with using a secure code repository are version control, peer review, and built-in auditing
- It is critical that the repository is an adequately secure central point of code storage and management
- Attackers can change a code base without your knowledge or permission due to loss/compromise of access credentials or breach of the core service
- If appropriate due diligence is applied to security measures, the benefits of using a code repository far outweigh the risks

Synthetic Transactions Testing

- Synthetic transaction testing uses scripted transactions to simulate the behavior of real users – often against banking, brokerage, and other financial services sites
- It is often used to monitor the performance and operations of applications or websites to recognize and send alerts about issues that could affect the end users
- Synthetic transaction testing usually involves multiple phases or scenarios across different plugins or features

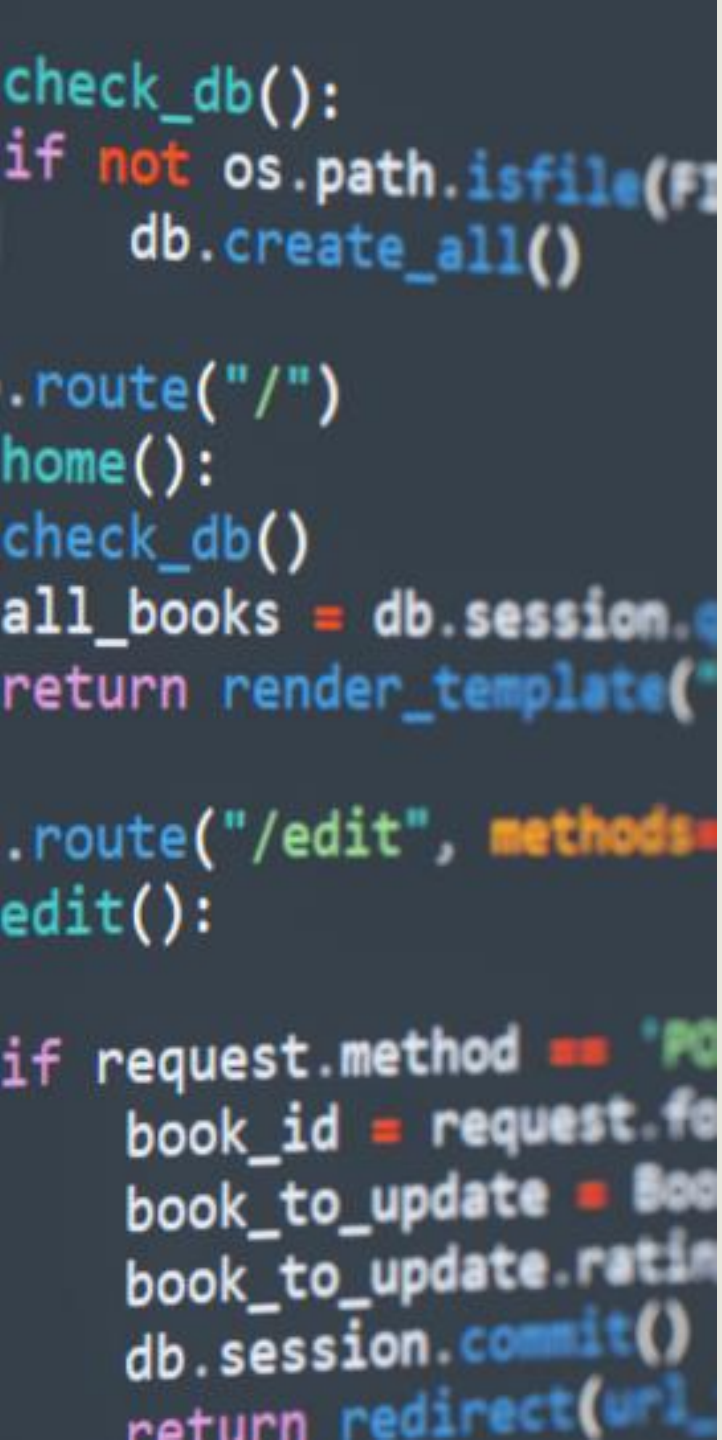

Synthetic transaction monitoring
Functionality
Availability
Response time

Benchmark Testing

- Benchmark testing is used to verify and validate the performance of an application or app against standardized criteria called benchmarks
- These metrics include throughput, error rate, and server response time
- Benchmark testing allows DevOps teams to determine how well an application performs under different scenarios
- Benchmark testing is a systematic approach that appraises the performance, proficiency, and capability by comparing applications, systems, hardware, software, or components against set standards

Misuse Case Testing

- Misuse case testing is also called "abuse case testing"
- This is a software and system testing approach that involves analyzing and generating test cases based on how an application **should not be used**
- It can anticipate malevolent activities or scenarios by testing the application's response to abuse such as input validation errors or unauthorized access attempts
- A misuse case offers an effective basis for security testing that gives visibility into the interactions between the advanced persistent threat actors and the system or app being developed



Coverage Analysis

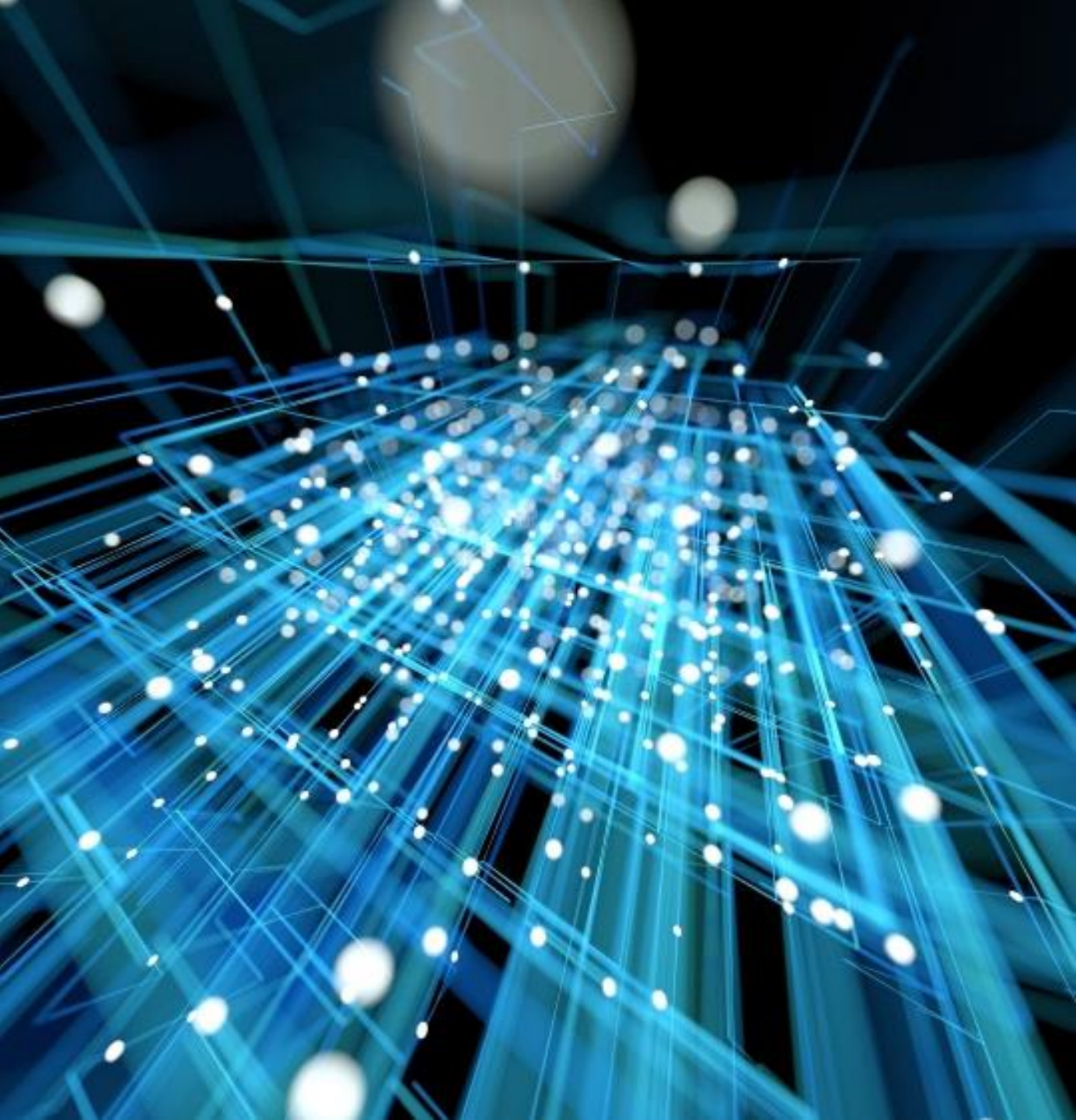
- In the context of security assessment, coverage analysis of code is common in software development
- Code coverage analysis is vital for recognizing code weaknesses, mitigating risks, and improving software effectiveness and reliability
- It assists in detecting untested code paths that may result in dormant issues or vulnerabilities
- Software developers can ensure that critical aspects of the codebase are meticulously tested

Coverage Analysis

- Threat coverage analysis is also applied to the systematic evaluation of a security operations center (SOC) by:
  - Pinpointing the threats that the SOC needs to detect
  - Defining the necessary detection rules, techniques, algorithms, and models
  - Certifying data collection from relevant sources (i.e., SIEM)
  - Validating rule efficacy with testing and automation (i.e., SOAR)
  - SOC coverage analysis is a security engineering challenge and an occasion for continual improvement

User Interface Testing

- User interface (UI) testing is a practice that appraises the interface where users interact with software or applications
- The focus is assuring that the visual aesthetics, functionality, and usability of a GUI, CLI, and voice user interface (VUI) are optimized and free of errors
- When the user first visits a website, the first impression is made and can affect how long the user stays on the site
- It is critical to perform UI testing of all websites, load balancers, CDN nodes, and web applications



Network Interface Testing

- Network interface testing is a gray-box testing technique used to verify the proper and anticipated behavior of interconnected networks in provisioning services to end users
- It is also common to analyze Infrastructure as Code (IAC) deployments in the cloud to gain visibility into the virtual layer 2 and layer 3 interfaces in complex virtual network environments

Application Programming Interface Testing

- API testing is usually performed with static application methodologies
- This software testing is considered an aspect of integration testing
- API testing is conducted at the message layer or the business logic layer with the goal of determining if functionality, reliability, performance, and security expectations are met
- API testing is usually done with a software tool and with assistance from the OWASP API Top 10

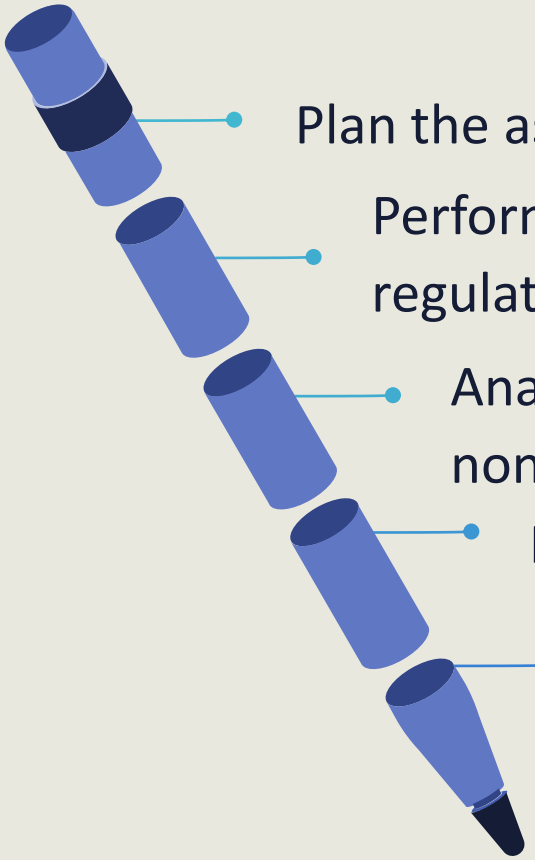
Compliance Audits (Checks)

- Carrying out a compliance audit is different from performing a vulnerability scan, although there will often be some overlap
- A compliance audit decides if a system is configured in agreement with a recognized governance policy
- Sometimes compliance involves auditing more sensitive data and systems
- There are many diverse forms of financial and government compliance requirements

Compliance Audits (Checks)

- Typically, the compliance requirements are minimal baselines that can be taken differently depending on the goals of the organization
- Compliance requirements must be in line with business goals to ensure that risks are correctly recognized and alleviated

Compliance Check Life Cycle



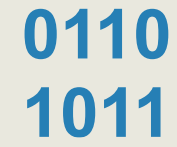
- Plan the assessment: Decide what needs to be evaluated
- Perform a compliance review: Gauge observance of laws, rules, and regulations
- Analyze discoveries and conduct a gap assessment: Recognize points of non-compliance
- Review and report to decision-makers: Communicate the results
- Develop a continual improvement initiative: Take corrective actions

Example: PCI Compliance Checklist

Use and maintain firewalls

Implement password protection

Protect cardholder data



Encrypt transmitted data

Use and maintain antivirus

Update software

Restrict data access

Create unique IDs for access

Restrict physical access

Create and maintain access logs

Scan and test vulnerabilities

Document policies

Collecting and Analyzing Security Process Data

Objectives

- Describe account management process, review, and approval data
- Explain key performance, risk indicators, and backup verification data
- Learn about training and awareness process data
- Observe disaster recovery (DR) and business continuity (BC) process data
- Analyze test output and generate reports
- Conduct and facilitate internal, external, third-party, and location-based audits

Collecting Account Management Process Data

- A directory is a database of all logical components that construct the local network
- It is typically managed through remote configuration of attributes associated with various account objects
- One of the main activities is to collect account management process data for gap analysis, privilege creep visibility, and continual improvement

Collecting Account Management Process Data

- Vulnerable and outmoded elements
- Failure to detect and update JavaScript libraries that have known weaknesses
- Absence of third-party origin control
- Origin control enables restriction of specific web assets by comparing the origin of the resource to a third-party library
- Without these controls, there is a higher risk of supply chain risk issues due to allowing unknown or unrestrained third-party code that has access to data in the site's origin

Collecting Account Management Process Data

- There are several methods for collecting data from account management and directory services:
  - Using Lightweight Directory Access Protocol (LDAP) and LDAP with Transport Layer Security (TLS)
  - Database queries and views such as Structured Query Language (SQL)
  - API calls and requests
  - Custom third-party solutions from Software as a Service (SaaS) providers

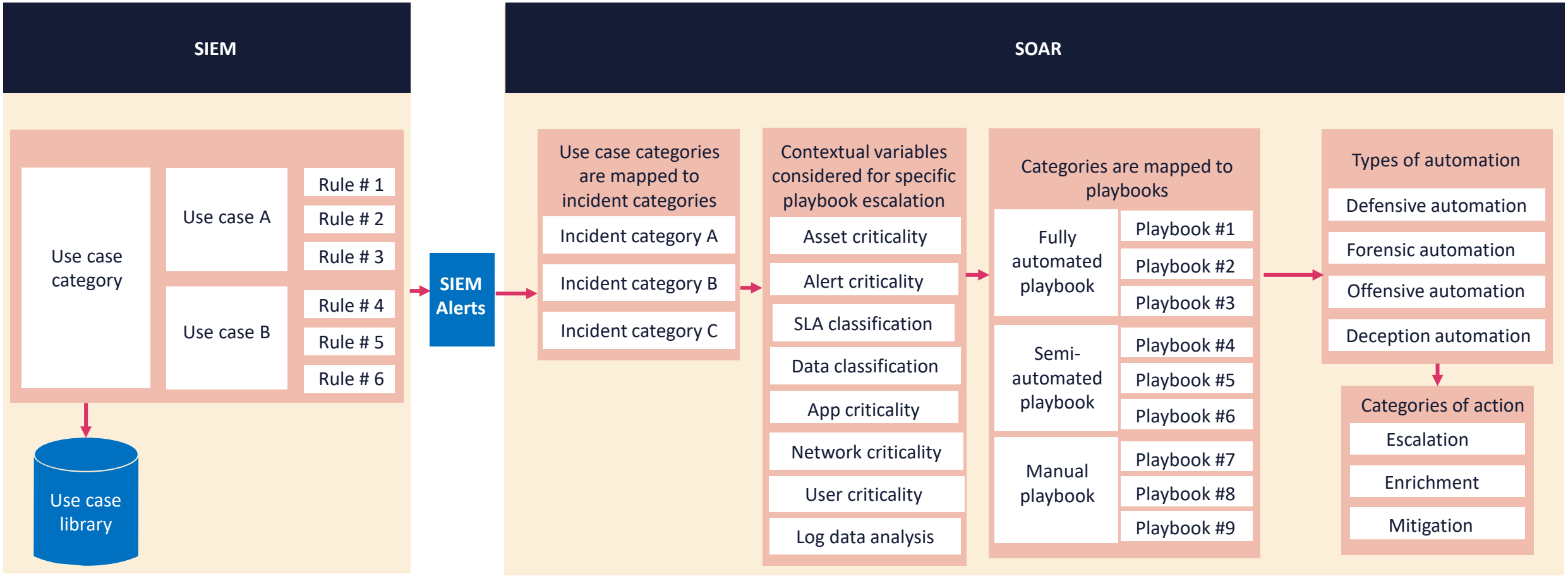
Collecting Security Management Data

- A key function for security managers is to collect security process data for management review and approval
- Reports and presentations must be compiled for steering committees, executives, C-suite members, and other stakeholders
- The most common methods for gathering this type of security data would be to use a traditional SNMPv3 systems or a security information and event management system (SIEM)

Collecting Security Management Data

- SIEM operates by gathering network telemetry and security-related event data from a variety of sources an organization such as firewalls, intrusion prevention system (IPS) sensors, servers, applications, and more
- This data is aggregated into a central repository, where it undergoes correlation analysis to identify patterns, anomalies, and potential security incidents
- The results of SIEM are often sent to a local or cloud-based security orchestration, automation, and response (SOAR) system

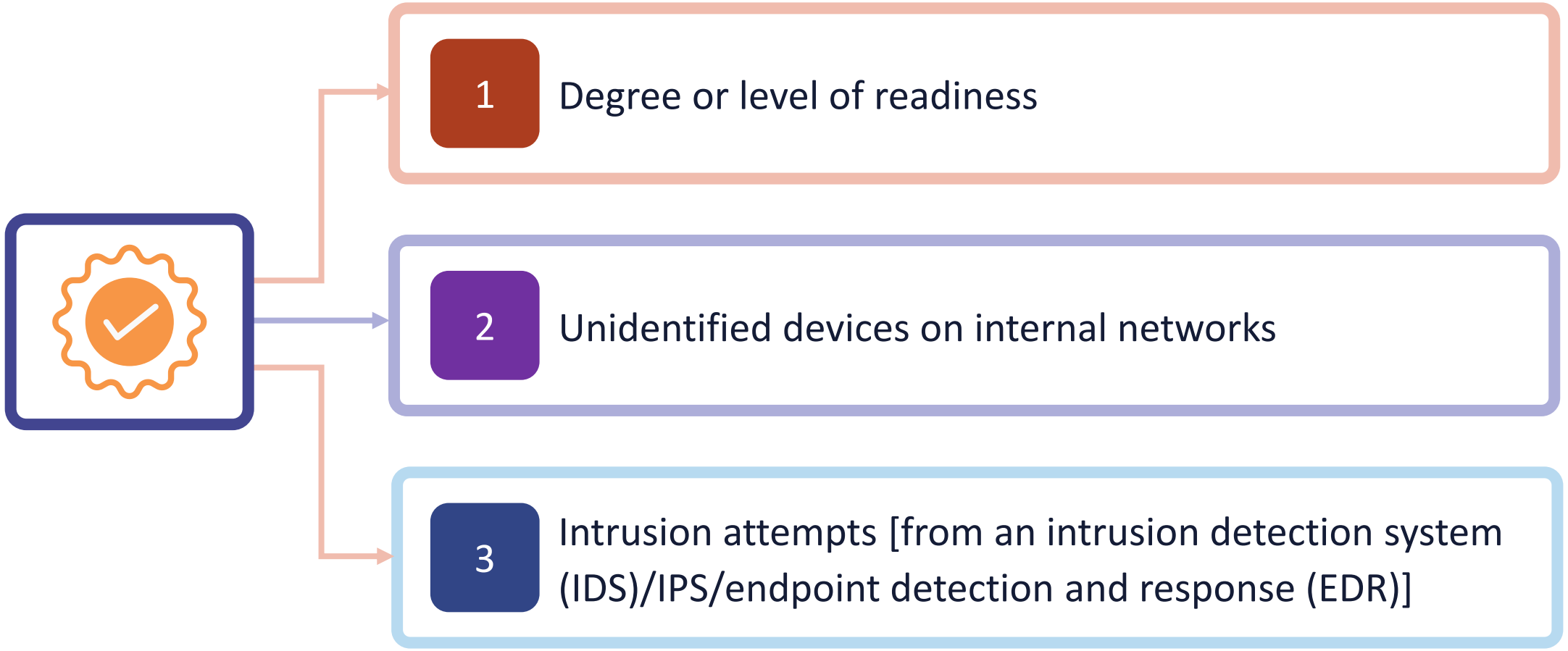
Collecting Security Data with SIEM and SOAR



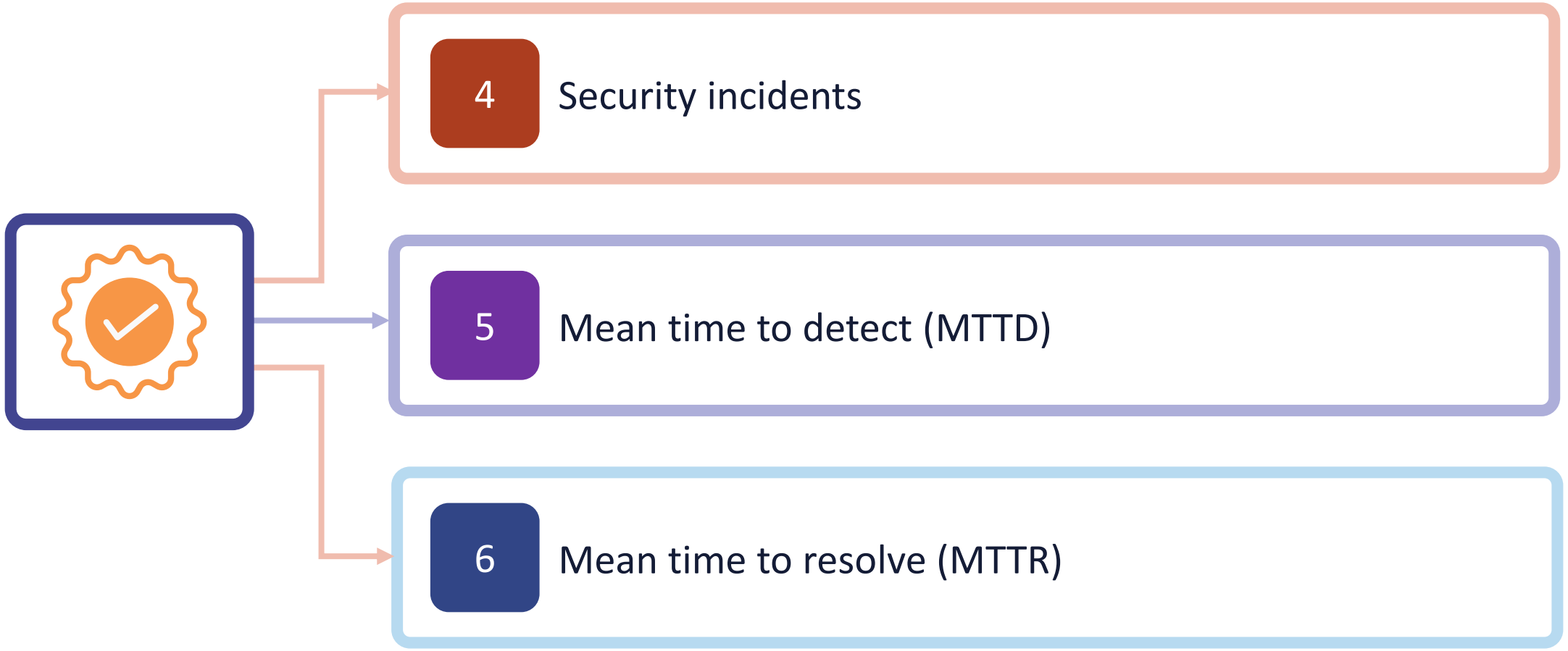
Key Performance and Risk Indicators

- Security managers can get a snapshot of team performance and functionality by analyzing key performance indicators (KPIs) and key risk indicators (KRIs)
- These metrics can help professionals better apprehend what were the right decisions and which controls are missing the mark
- It is a big enabler for refining decision-making about future security initiatives
- Key metrics and critical success factors (CSFs) deliver quantitative data to present to upper management and committee members to justify and improve risk management decisions

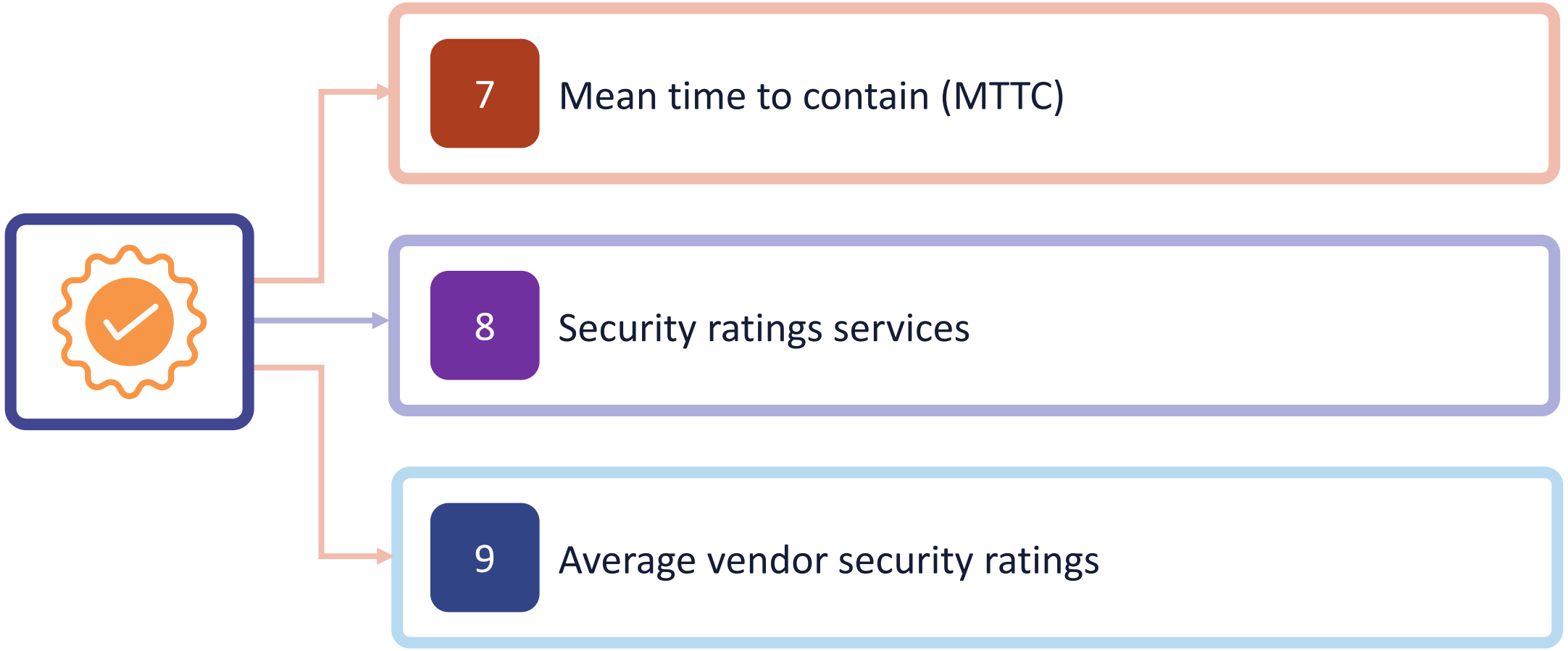
Security Management KPIs AND KRIs



Security Management KPIs AND KRIs



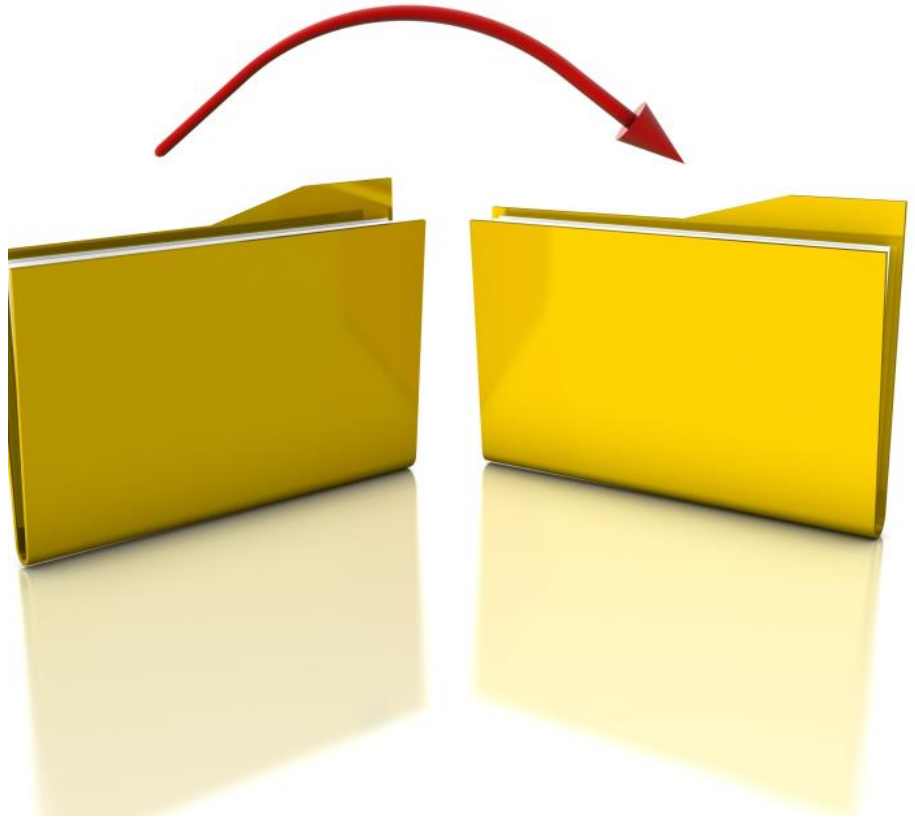
Security Management KPIs AND KRIs



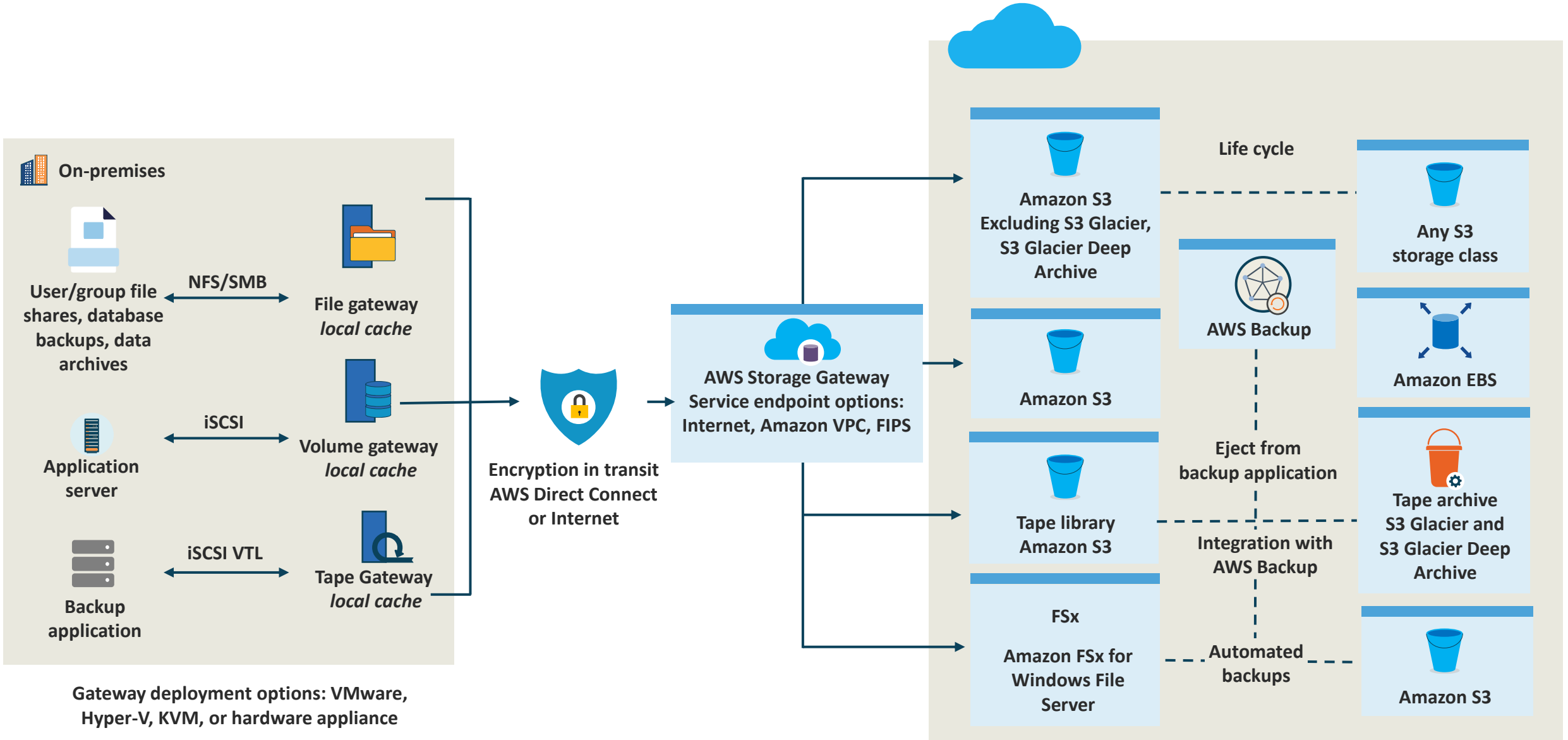
Security Management KPIs AND KRIs

Verifying Data Backup

- The primary incident response control for ransomware is a tested and verified data backup process
- This verification procedure is also a critical aspect to overall disaster recovery planning
- Modern hybrid cloud solutions with on-site physical or virtual storage gateways are enhancing the backup policies and processes
- **Hypervisor storage (pods or datastore) clusters are key modern targets**

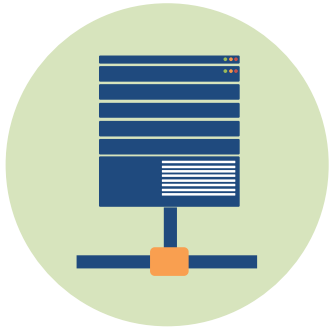


Example: AWS Storage Gateway



Gateway deployment options: VMware, Hyper-V, KVM, or hardware appliance

Backup Verification Best Practices



Intermittently verify all manual backups

Examine backup data analytically

Test backups in various cases (misuse or abuse case)

Backup Verification Best Practices

Focus on mission-critical data first

Confirm available space and budget for backups

Understand availability vs. durability service-level agreements (SLAs)

Training and Awareness Process Data

- A critical administrative control is ongoing training and awareness programs
- Managers must evaluate the results of all training modalities and targets
- The data gathered for analyzing and optimizing training and awareness must be meaningful and comprehensive
- Participants should also be provided with an avenue for giving open-ended subjective feedback

Security Training Monitoring and Reporting

- Security training monitoring and reporting must be scoped to the specific audience to deliver different types of security training:
  - Basic security awareness
  - Technical security
  - Security management
  - Compliance
  - Threat hunting and red/blue team

Security Training Monitoring

- The Net Promoter Score (NPS) is considered the gold standard customer experience metric
- In this context, the NPS score measures participant loyalty by looking at their probability of recommending a given security training experience
- NPS scores are measured with a single-question survey and reported with a number ranging from -100 to +100, where a higher score is desirable

Security Training Reporting

- The NPS score evaluation would only be a part of the reporting process
- Often peer and supervisory evaluations should be performed to offer valuable critique and reinforcing feedback to the one delivering the training
- This evaluation should also include the origin content, graphical representations, test questions, and various modalities of the training
- All reporting best practices mentioned in this Security+ training should be considered

Business Continuity Process Data

Business impact analysis (BIA)

- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete BIA
- Receive complete BIA questionnaire forms
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill any gaps

Recovery strategies

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies

Plan development

- Develop plan framework
- Organize recovery teams
- Develop relocation plans
- Write business continuity and IT disaster recovery procedure
- Document manual workarounds
- Assemble plan
- Validate and gain management approval

Testing and exercises

- Develop testing, exercise, and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update the business continuity plan (BCP) to incorporate lessons learned from testing and exercises

Business Impact Analysis Metric Data

- **Recovery Time Objective (RTO)**
  - The target amount of time within which a process must be restored after a disruption
- **Recovery Point Objective (RPO)**
  - The maximum targeted period in which an asset or data may be lost
    from an IT service due to a major event
- **Mean time to repair (MTTR)**
  - The average time needed to repair a failed system or module
- **Mean time between failures (MTBF)**
  - The number of failures per million hours for a product
- **Maximum tolerable downtime (MTD)**
  - Absolute maximum amount of time that a resource, service, or function can be unavailable before experiencing loss

Disaster Recovery Process Data

- All process data in digital AND physical formats with high redundancy
- Step-by-step instructions on how to recover each aspect of critical systems, applications, and data
- Backup and restore plans with order of restoration
- Contact information for key stakeholders, partners, and vendors, including succession order
- Contact information for law enforcement, legal, insurance companies, and media outlets
- Location of hot spares, software and CD keys, security access keys and failsafe passwords, and other valuables
- Site locations and descriptions (cold, warm, hot, cloud)

Analyzing and Reporting on Remediation Testing

- Remediation testing generates reports on vulnerabilities with an outline and summary on fixes and workarounds (including compensating controls)
- The reports serve as a checklist (plan review) test for security teams to prioritize weaknesses by severity
- Once developers deploy an update or patch, they can perform another scan or retest to validate the patch against a baseline

Analyzing and Reporting on Remediation Testing

- Output generated from remediation tests:
  - Unpatched operating systems and applications
  - SQL injection and cross-site scripting (XSS) vulnerabilities in web sites and web applications
  - Weak account credentials
  - Insecure direct object references (IDOR)
  - Device misconfigurations

Exception Handling Output

- Lead developers often initiate an application reporting service to help further reduce (or even eliminate) the rate of exceptions
- When exceptions occur, teams need rich and concise error messages to enhance proper exception handling to stop apps and applications from hanging or crashing
- An application that does reporting should:
  - Circumvent, causing exceptions by averting as many invalid requests as possible
  - Trap exceptions and offer specific error-handling codes whenever feasible
  - Handle error cases that do not trigger exceptions

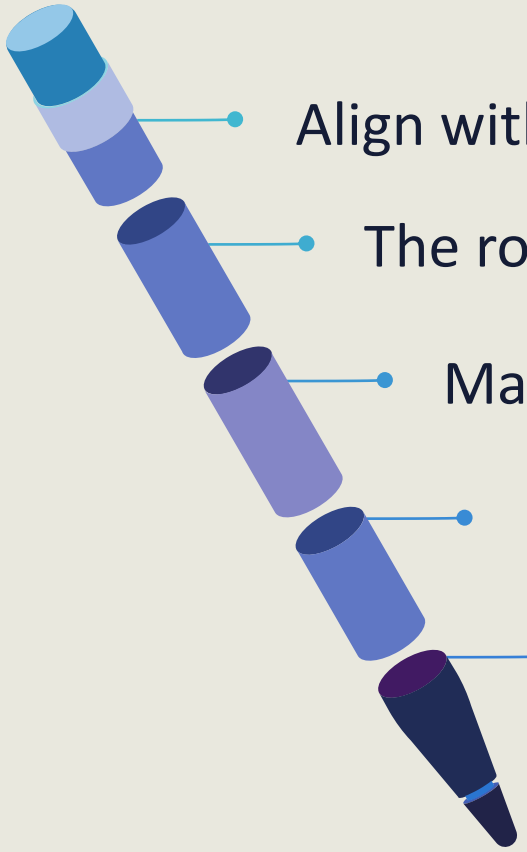
Reporting on Ethical Disclosure

- Ethical disclosure reporting is a critical organizational process to deliver transparency
- These reports are core to assure proper, professional, and ethical conduct
- This is necessary if the enterprise intends to be honest, precise, and wide-ranging when delivering the information for policy or regulatory purposes
- There exists an ever-present tension between professional duties and personal preferences or gain

Audit Results Reporting

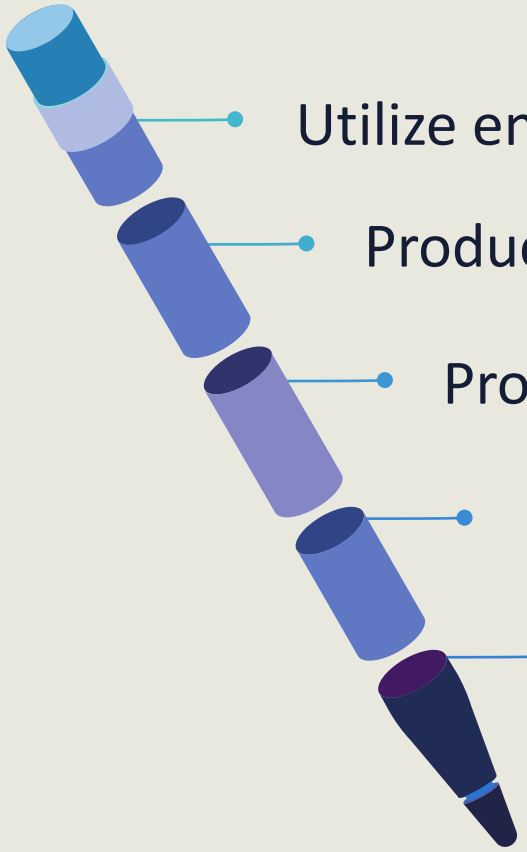
- Security audits can be driven by programs such as SOC2, COBIT, CIS, CSA, and more
- The audits will often be scoped based on:
  - Internal (inside organizational control)
  - External (outside organizational control)
  - Third-party (outside of enterprise control)
  - Location-based (on-premises, cloud, hybrid)

Security Audit Reporting Best Practices



- Align with customer guidance, policies, standards, and processes
- The routine should correspond to the vulnerability scanning schedule
- Maintain a consistent structure over the life cycle for improved results
- Purge outdated and obsolete security scan results data
- Engage with the consumers of the reports frequently and assess possible improvements

Security Audit Reporting Best Practices



- Utilize engaging dashboards (Azure Sentinel, Cisco Splunk)
- Produce with different audiences and technical knowledge in mind
- Provide glossaries and definitions – do not assume understanding
- Make reporting as interactive and dynamic as possible
- Replace pie charts with boxplots and scatterplots (R language)