SECURING SAP LANDSCAPE With Microsoft

October 26, Marieke van de Putte

SECURING SAP LANDSCAPE

01 | WHY

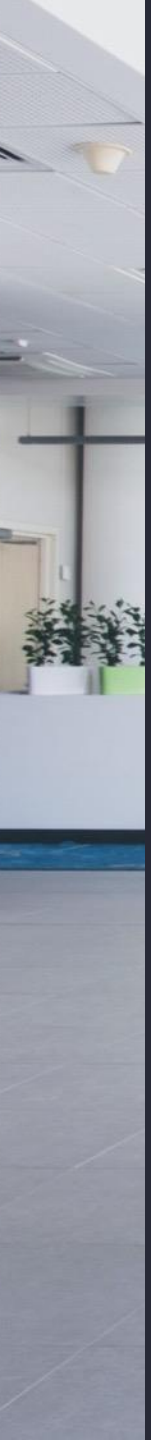
02 | WHAT

03 | HOW (PROTECTOR TOOLS)

04 | CALL TO BE SECURED

1

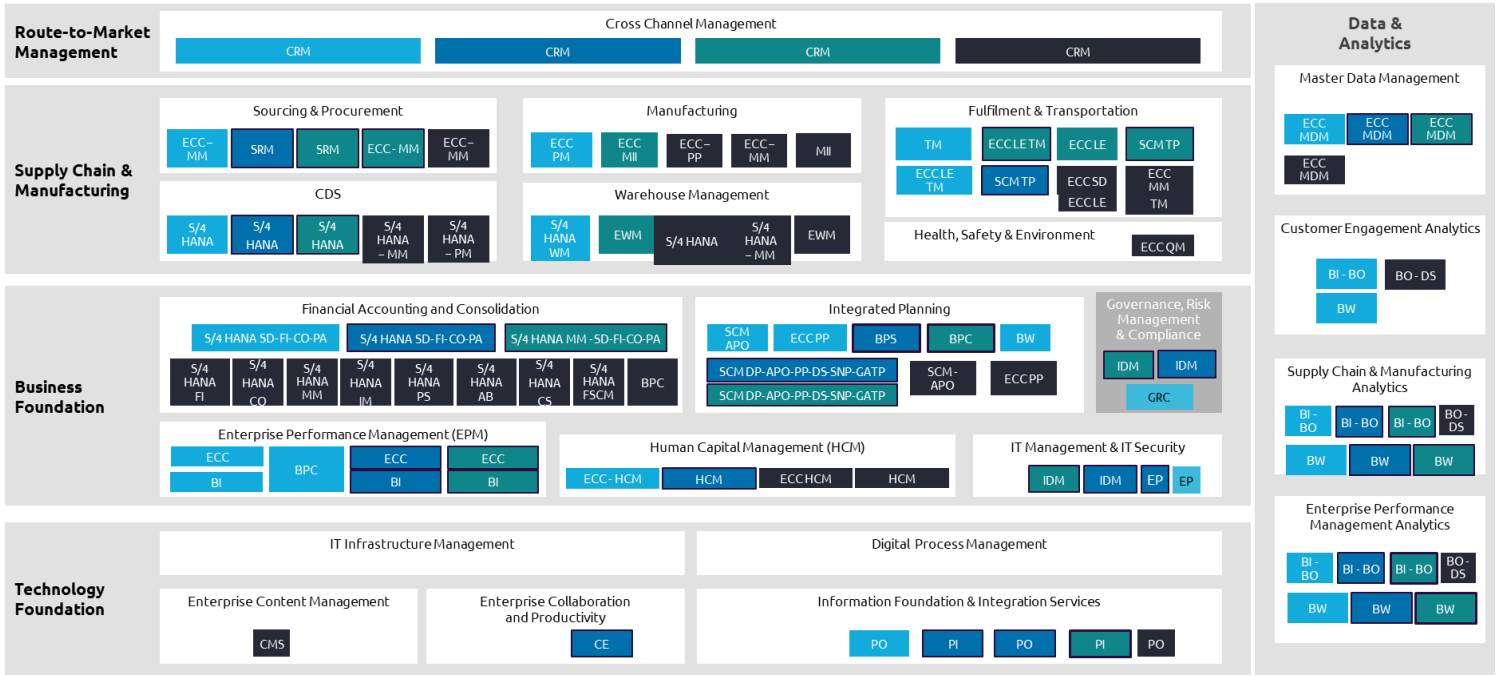
THE WHY



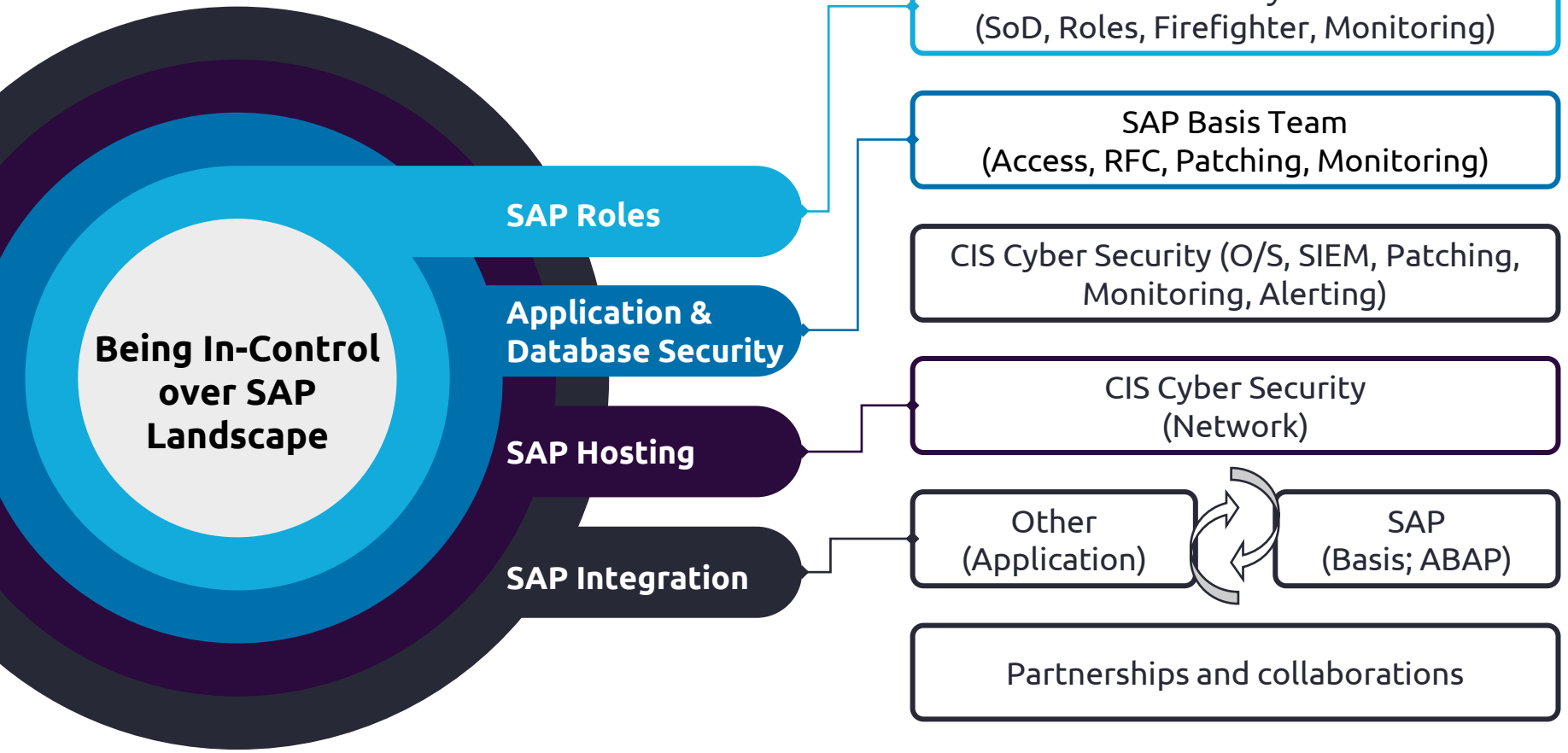
MICROSOFT SENTINEL AND SAP

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

EXAMPLE OF CUSTOMER GLOBAL SAP ESTATE



LEVERAGING OUR COMPETENCIES TO PROVIDE OUR NEW INTEGRATED SECURING THE SAP LANDSCAPE SERVICES



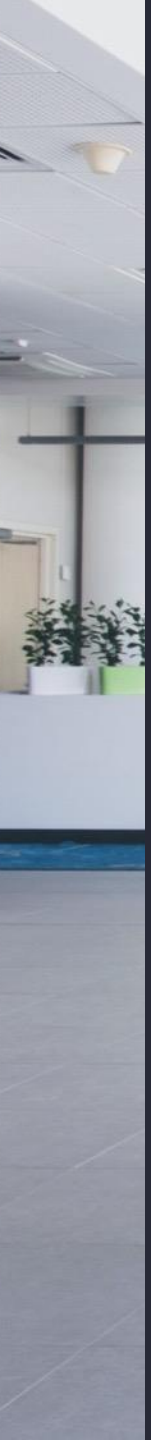
Our Teams

- SAP Security Team (SoD, Roles, Firefighter, Monitoring)
- SAP Basis Team (Access, RFC, Patching, Monitoring)
- CIS Cyber Security (O/S, SIEM, Patching, Monitoring, Alerting)
- CIS Cyber Security (Network)
- Other (Application) ⇄ SAP (Basis; ABAP)
- Partnerships and collaborations

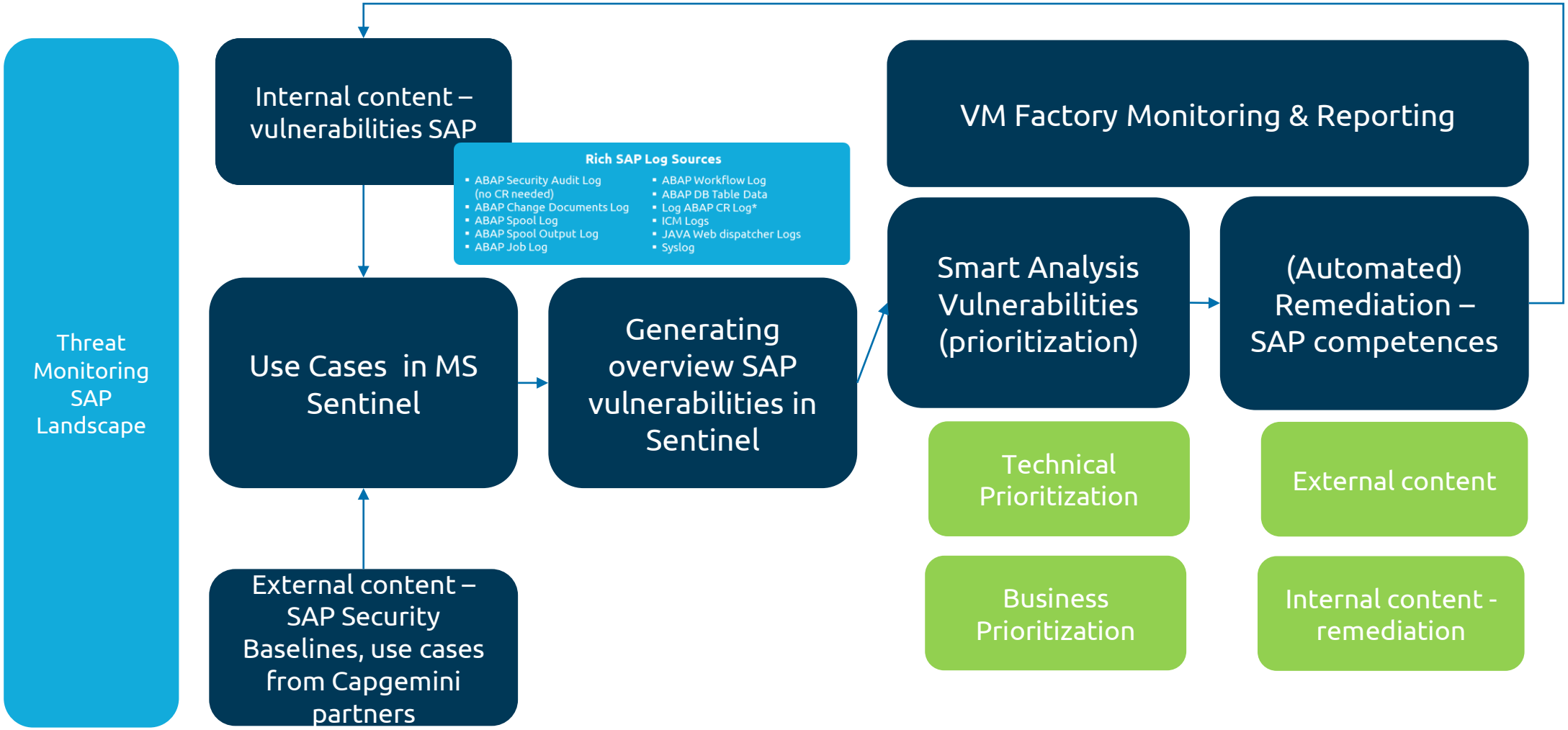
- Capgemini has more than **22,000** SAP professionals who help design, configure, manage, operate and secure SAP systems for our clients
- In addition to that, we have more than **4,000** Cybersecurity professionals worldwide
- We combine and leverage the expertise and experience from our SAP operating teams, SOC operations and Security experts
- Our professionals and clients are facilitated by the collaboration with Microsoft

2

THE WHAT



STORYLINE MS SENTINEL SAP



USE CASE -SAP BTP AUDIT LOGS IN MICROSOFT SENTINEL

The SAP BTP Audit Logs represent different actions taken over the account and (or) data. All entries of the SAP BTP Audit log are grouped into the following areas:

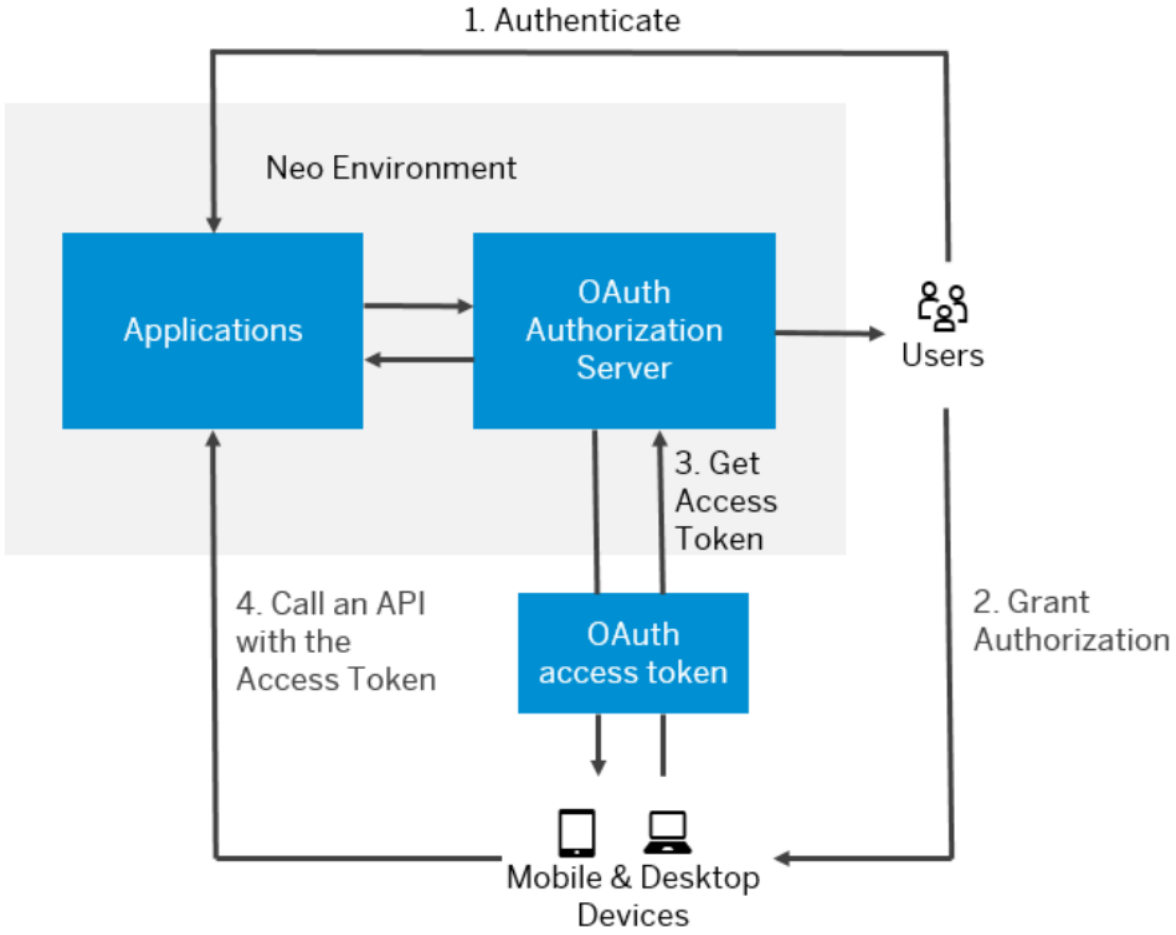
- Identity provider management
- Instance management
- Role collection management
- Role management
- SAML authentication

- To collect and monitor the SAP BTP logs, Microsoft Sentinel uses, inbuilt rules, which can be further enhanced by customized rules.

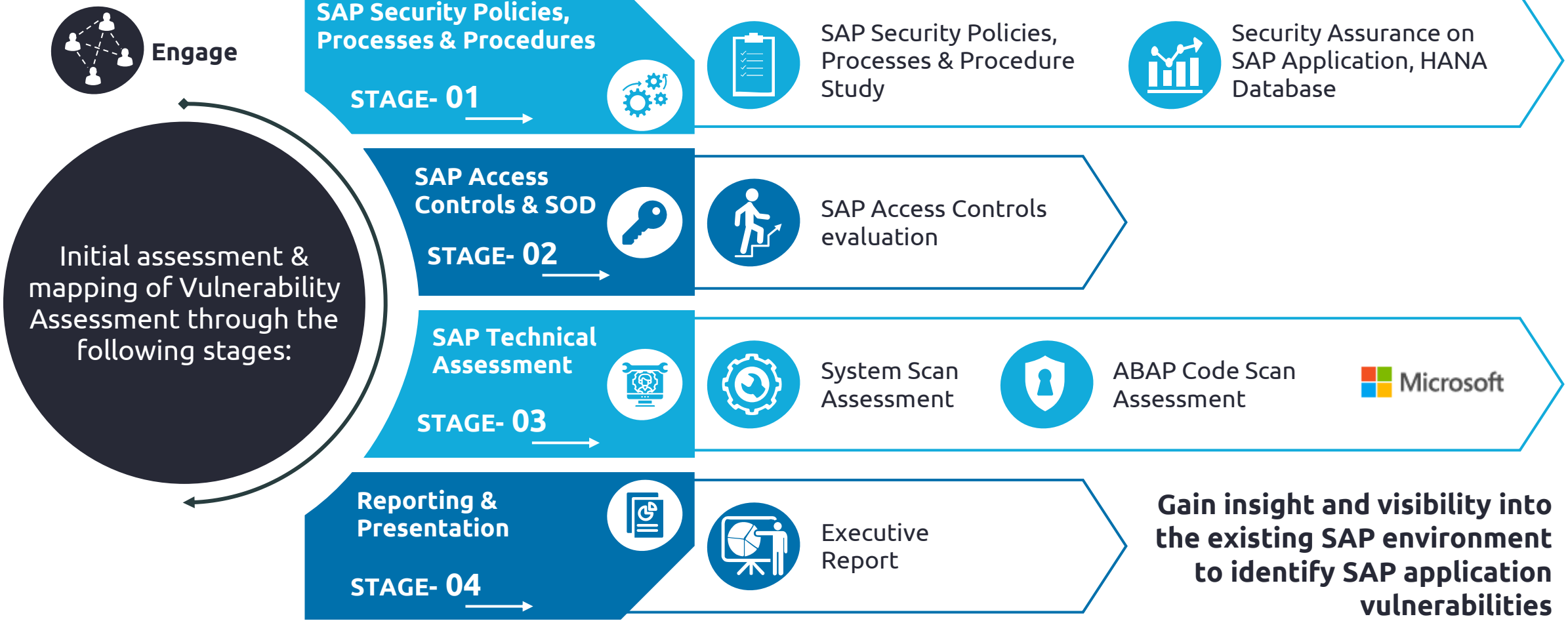
Example:

OAuth 2.0 is an authentication method used by users in SAP BTP and below rules can monitor and raise alerts on unauthorized user logins.

- OAuth 2.0 : Token declared invalid
- OAuth 2.0 : Invalid access token received
- OAuth 2.0 : Client requested invalid access grant type
- OAuth 2.0 : Client ID in SAML assertion not same as client ID in request



BASELINE VULNERABILITY ASSESSMENT
DETECT VULNERABILITIES IN SAP ENVIRONMENTS



Gain insight and visibility into the existing SAP environment to identify SAP application vulnerabilities

WE PROPOSE A PHASED APPROACH TO ALIGN OUR METHOD TO YOUR SPECIFIC SECURITY OBJECTIVES, CHALLENGES AND PRIORITIES

01

Assessment: Baseline Assessment

- Conduct an initial vulnerability baseline assessment to come to a shared understanding of the current status, issues, opportunity areas and priorities.
- Agree on remediation priorities and timelines

02

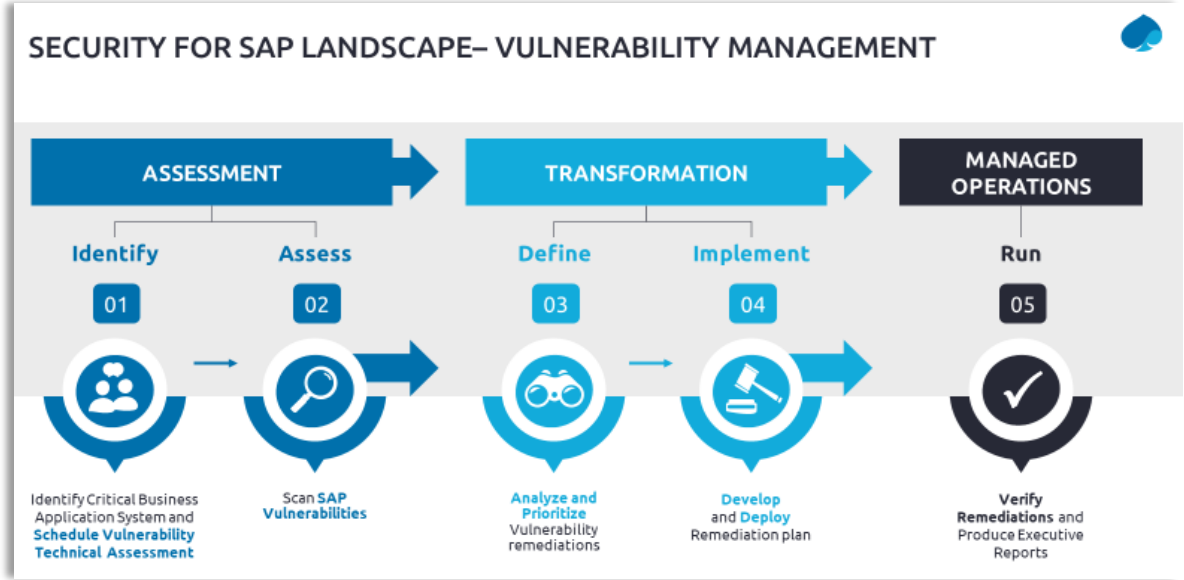
Transformation: Vulnerability Management Scope, Design and Planning

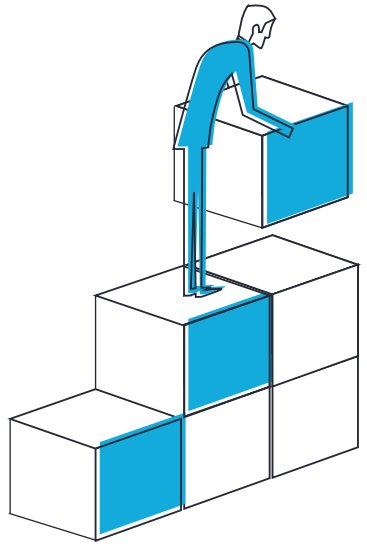
- Adopt the VM scope and approach to the company specific VM objectives and priorities
- Remediation of identified/prioritized improvement areas, to resolve existing exposure and to provide a sustainable foundation for the VM approach
- Build Vulnerability Management operating structure

03

RUN MS Sentinel SAP Security managed services

- Based on agreed scope, including e.g. ongoing VA / VM, Access Control and Authorization Provisioning, Process Control, Risk management, HR Security, HANA DB Security, Real Time Threat Detection





3

CREDENTIALS

SECURING THE SAP LANDSCAPE BUILDING BLOCKS

01 SAP Technology / SAP support

- SAP Managed Services
- SAP Basis Security *(Security Baselines; Security Notes and Patches)*

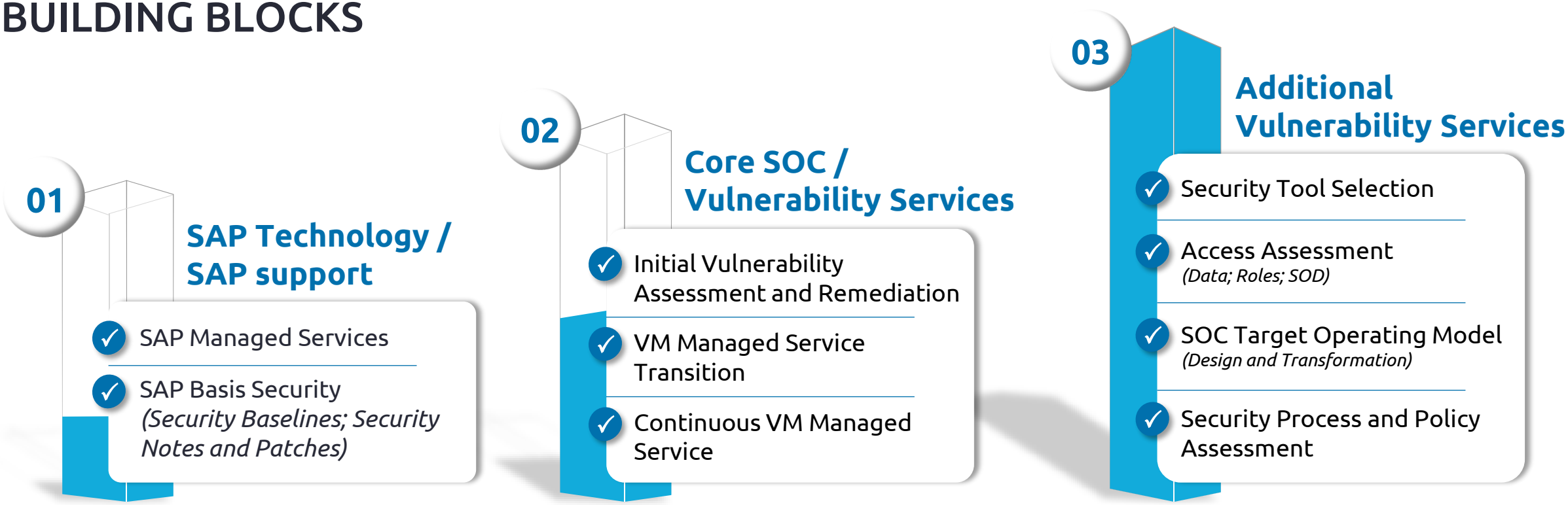
02 Core SOC / Vulnerability Services

- Initial Vulnerability Assessment and Remediation
- VM Managed Service Transition
- Continuous VM Managed Service

03 Additional Vulnerability Services

- Security Tool Selection
- Access Assessment *(Data; Roles; SOD)*
- SOC Target Operating Model *(Design and Transformation)*
- Security Process and Policy Assessment

CAPGEMINI'S EXPERIENCE ACROSS THE SECURING THE SAP LANDSCAPE BUILDING BLOCKS



- For all SAP support customers, we provide the basic SAP security support, including technical baseline and security parameters VA and security notes / patching
- **Client examples**: Dutch international retailer; Global agricultural prod. supplier; Dutch transportation provider.

- We operate Security Operating Centers (SOCs) for a wide range if clients, managing the vulnerabilities related to the IT infrastructure, operating system and applications
- **Client examples:** Global beverages co; Airline co; Shipping hospitality co

- Our SAP teams have extensive experience with SAP access management, ABAP security assessment as well as security process and governance design / implementation
- **Client examples:**
  - International Medical Care: technical baseline and security parameters
  - Multinational pharmaceutical and biotech: SAP Access Control, Access risk management)
  - Hospitality booking platform: Role design and Incident management

CLIENT CASE: SAP TECHNOLOGY / SAP BASIS SUPPORT

SAP Technology / SAP Basis Support - For all our SAP support customers we provide SAP Basic Security Support:

- SAP Security Baseline
- Database Security Baseline
- SAP Security parameters
- SAP Audit Log
- SAP Security Notes & SAP Security Patches

CUSTOMERS

SAP Technology / SAP support

- ✓ SAP Managed Services
- ✓ SAP Basis Security
  (Security Baselines; Security Notes and Patches)

Core SOC / Vulnerability Services

- Initial Vulnerability Assessment and Remediation
- VM Managed Service Transition
- Continuous VM Managed Service

Additional Vulnerability Services

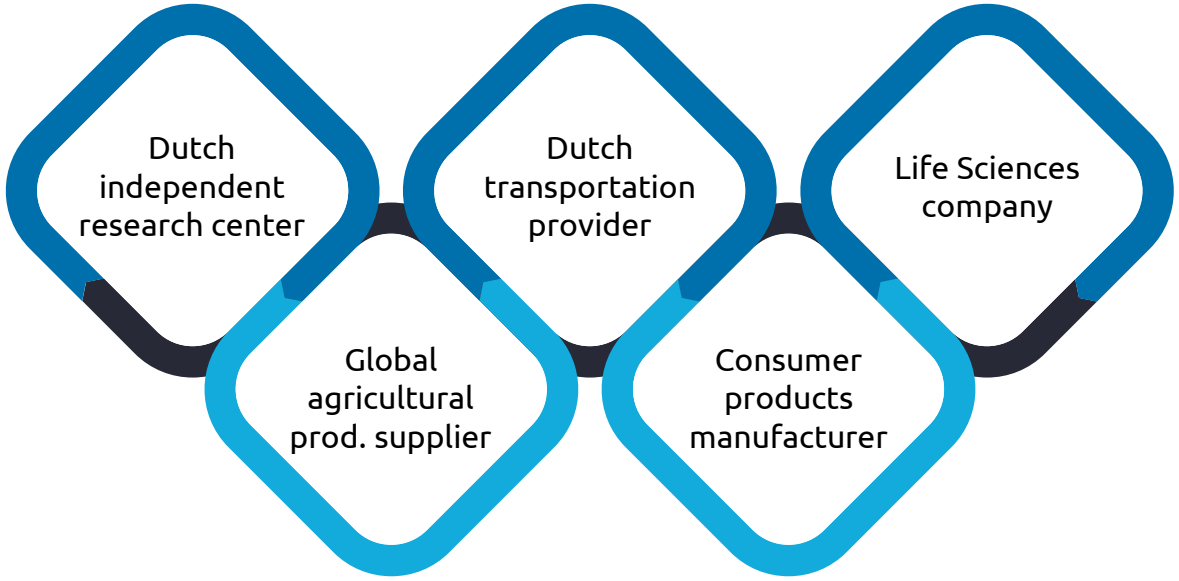
- Security Tool Selection
- Access Assessment *(Data; Roles; SOD)*
- SOC Target Operating Model
  (Design and Transformation)
- Security Process and Policy Assessment

CLIENT CASE: CORE SOC / VULNERABILITY SERVICES FOR SAP CLIENTS

Basic SOC / Vulnerability Services - For some of our SAP support customers we provide *automated* SAP Security Support by closely collaborating Capgemini security partners:

- Vulnerability Assessment
- SAP Security Baseline
- SAP Security Notes
- ABAP Code Scan

EXAMPLE CUSTOMERS



SAP Technology / SAP support

- ✓ SAP Managed Services
- ✓ SAP Basis Security *(Security Baselines; Security Notes and Patches)*

Core SOC / Vulnerability Services

- ✓ Initial Vulnerability Assessment and Remediation
- VM Managed Service Transition
- ✓ Continuous VM Managed Service

Additional Vulnerability Services

- ✓ Security Tool Selection
- ✓ Access Assessment *(Data; Roles; SOD)*
- SOC Target Operating Model *(Design and Transformation)*
- ✓ Security Process and Policy Assessment