→ MAKING THE WORLD A SAFER PLACE TO DO BUSINESS

TURNKEY

SAP Enterprise Threat Detection (ETD), Cloud Edition as a Managed Service

www.turnkeyconsulting.com

JULY 2023

TURNKEY

Hosts

Andrew Morris

UK Practice Director
Application & Cyber Security

Turnkey Consulting

Rob Tyler

APAC Practice Director
Cyber Security

Turnkey Consulting

Arndt Lingscheid

Global Solution Owner

SAP

www.turnkeyconsulting.com

What we do

Advisory

Implementation

Managed Support

Integrated
Risk Management

Identity &
Access Management

Application &
Cyber Security

BEDROCK

Bedrock Managed Service

Contents

TURNKEY

01

Background and Context

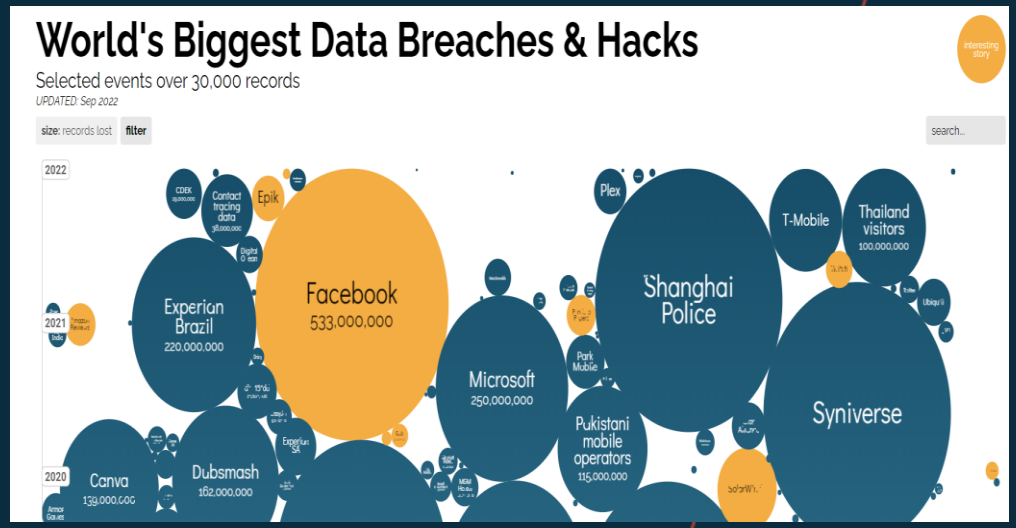
TURNKEY

New legislation is appearing worldwide which is placing a greater emphasis on cybersecurity and data privacy.

- NIS-2
- US National Cybersecurity Strategy
- NIST CSF-2 guidance
- SOCI (Security of Critical Infrastructure – Australia)

All these place a greater emphasis on security, with monitoring for security events becoming a key principle being referenced. This as a response to some high-profile breaches which have occurred in recent years, such as SolarWinds and the Colonial Pipeline hack.

Many Organisations are not fully compliant due to the technical complexity of applications, and unclear ownership. These issues are only going to increase, along with auditor scrutiny.




RESEARCH

More vulnerabilities in industrial systems raise fresh concerns about critical infrastructure hacks

Researchers have revealed details about flaws in industrial systems that could give hackers access to the most sensitive networks.

BY CHRISTIAN VASQUEZ • FEBRUARY 22, 2023


NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs

The shipping giant has suffered millions of dollars in damage due to the ransomware attack.

What Role Does Security Monitoring Play?

WHAT IS SECURITY MONITORING?

Security monitoring (sometimes called SIEM or SIM) is the process of collecting data which can be used to identify potential security threats and then creating and prioritising alerts so that an organization can investigate and respond as necessary.

Often, security monitoring will pull together and correlate event data from multiple sources to validate and enrich the security event information provided.

HOW DOES SECURITY MONITORING HELP?

- Identifying suspicious behaviour and attempts to gain unauthorized access to your network, applications, and devices
- It helps stay on top of evolving threats
- Proactively responding to threats before they become a security incident
- Provide critical information that regulatory and legislative require to prove compliance

TURNKEY

Why Monitoring SAP is so Important

SAP Application owners must work with CISOs to tackle the problem

90%

OF THE REVENUE

SAP systems route a huge volume of the revenue-related data for their customers, meaning SAP application owners take risk in this area very seriously

10%

OF THE IT ESTATE

A CIO, or CISO, who has an entire IT (and often OT) estate to secure against threats, may see the risk profile of the SAP applications through a different lens

50%

OF THE RESPONSIBILITY

Securing SAP systems is not performed in a vacuum, shared ownership of the risks and the controls allows a more co-ordinated approach and better security outcomes overall.

TURNKEY

02

ETD as a Solution

TURNKEY

SAP Enterprise Threat Detection

DEFINITION

SAP ETD provides security monitoring of suspicious events within an SAP application with the aim to detect and stop security breaches in real time

PURPOSE

ETD uses automated processes to monitor user behaviour and identify suspicious activity which could be an Indicator of compromise within your SAP estate.

BULT IN CONTENT

- Pre-defined use cases for security incidents
- Routines for collecting and storing of audit relevant information
- Built in connectivity for native SAP systems

CUSTOMER ADOPTION

More than 400 SAP customers worldwide across many industries who provide constant feedback.

TURNKEY

ETD On-premise and Cloud Edition

PROTECT YOUR CROWN JEWELS

- System events and contextual data is sent to SAP Enterprise Threat Detection
- Data is efficiently enriched, normalised, pseudonymised, analysed and correlated
- Huge amounts of data can be processed
- Automatically evaluate attack detection use cases with real-time alerting
- Forensic analysis and modelling of existing and new attack detection use cases and dashboards
- Powerful investigation engine for drilling into alerts and incidents

ETD CLOUD EDITION (BTP)

- Cloud provisioning
- Integrated managed security service
- Ships with over 45 standard attack use cases
- 24x7 alerting & 8x5 risk based & prioritized investigation of alerts
- Monthly reporting of all incidents and all log data
- Collecting and storing of audit relevant information
- Integration to typical SIEM solution

Extended service availible* for Cloud Edition with customised SLA's

Provides coverage for the SAP portfolio of products

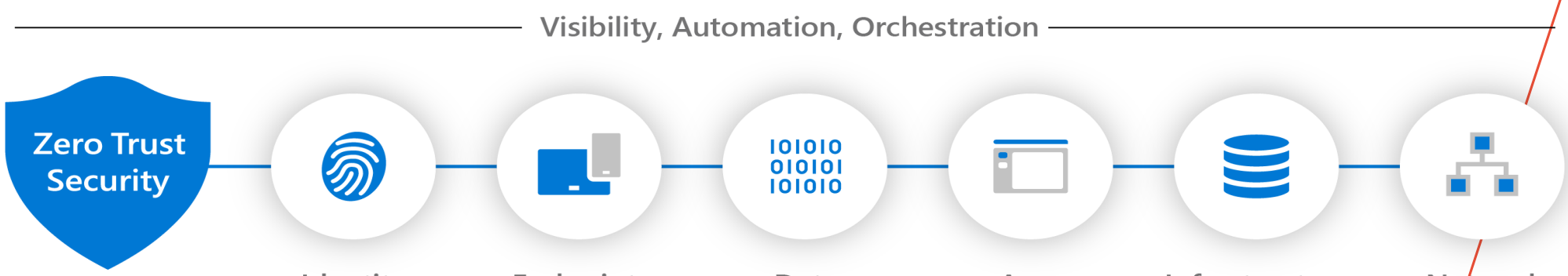
For Cloud Edition SAP will manage all alerts and monitoring, allowing you to focus on response processes

* Planned in Q2 2023

TURNKEY

The Role ETD Plays

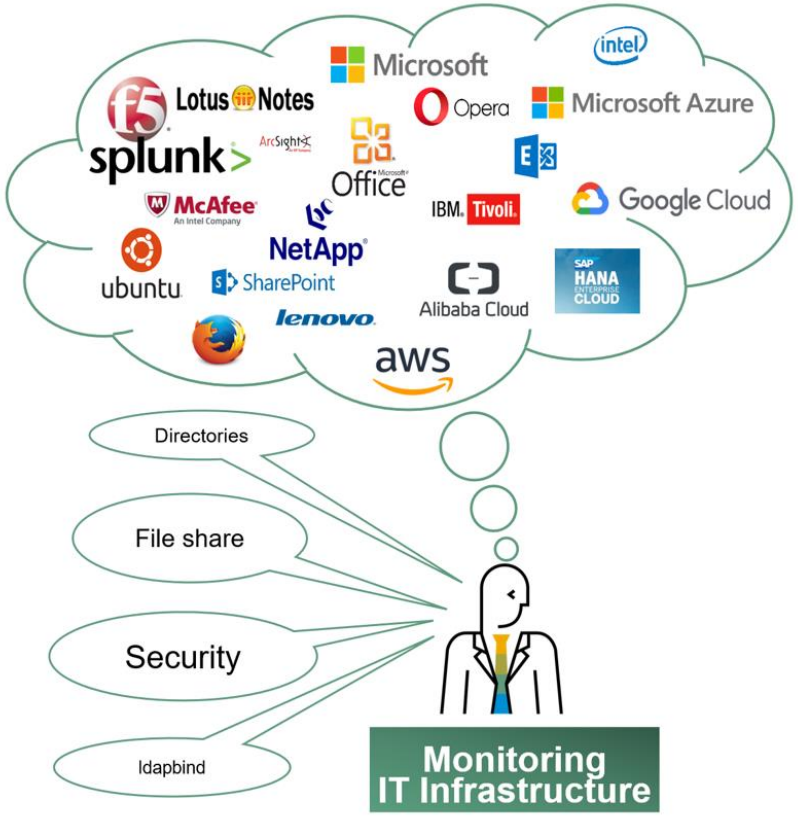
How ETD fits in with the rest of SAPs portfolio of tools to secure your estate

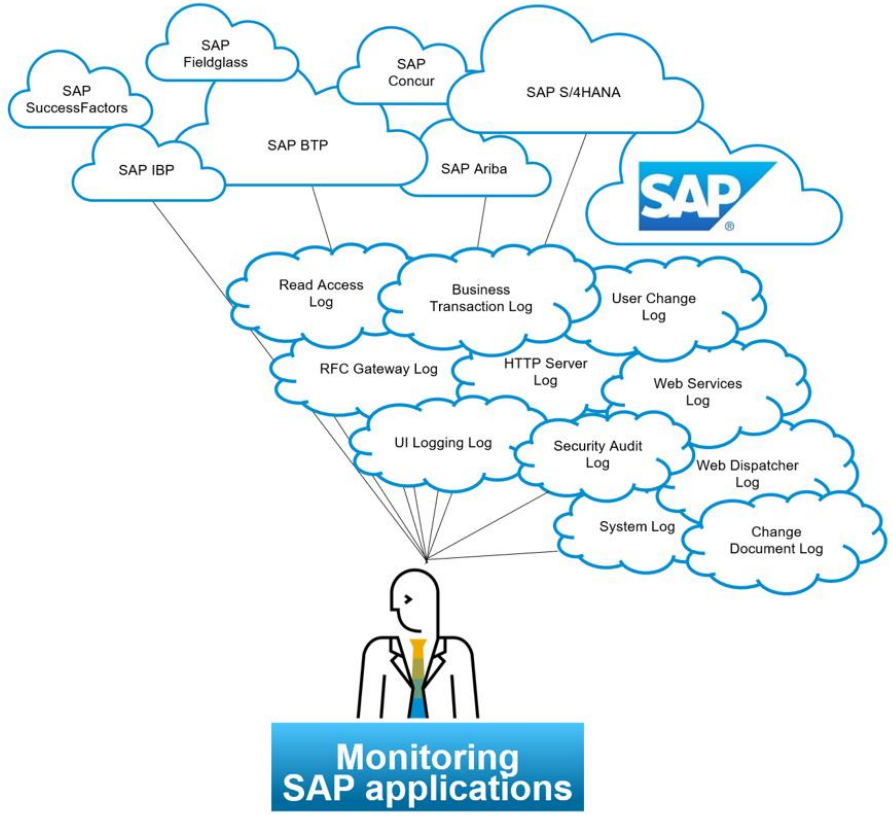


Identity	Endpoints	Data	Apps	Infrastructure
SAP & Enterprise IDAM MFA SSO	Fiori & Mobile Devices (changing the threat vector) **Logging and monitoring**	Access Governance UI Masking RAL Data Custodian **Tracking changes**	DevSecOps (incl. secure coding) **Integrity** BIS CVA	**SOC / SIEM / SOAR integrations** Patch & Vulnerability Management (both at the application and infrastructure layers)

TURNKEY

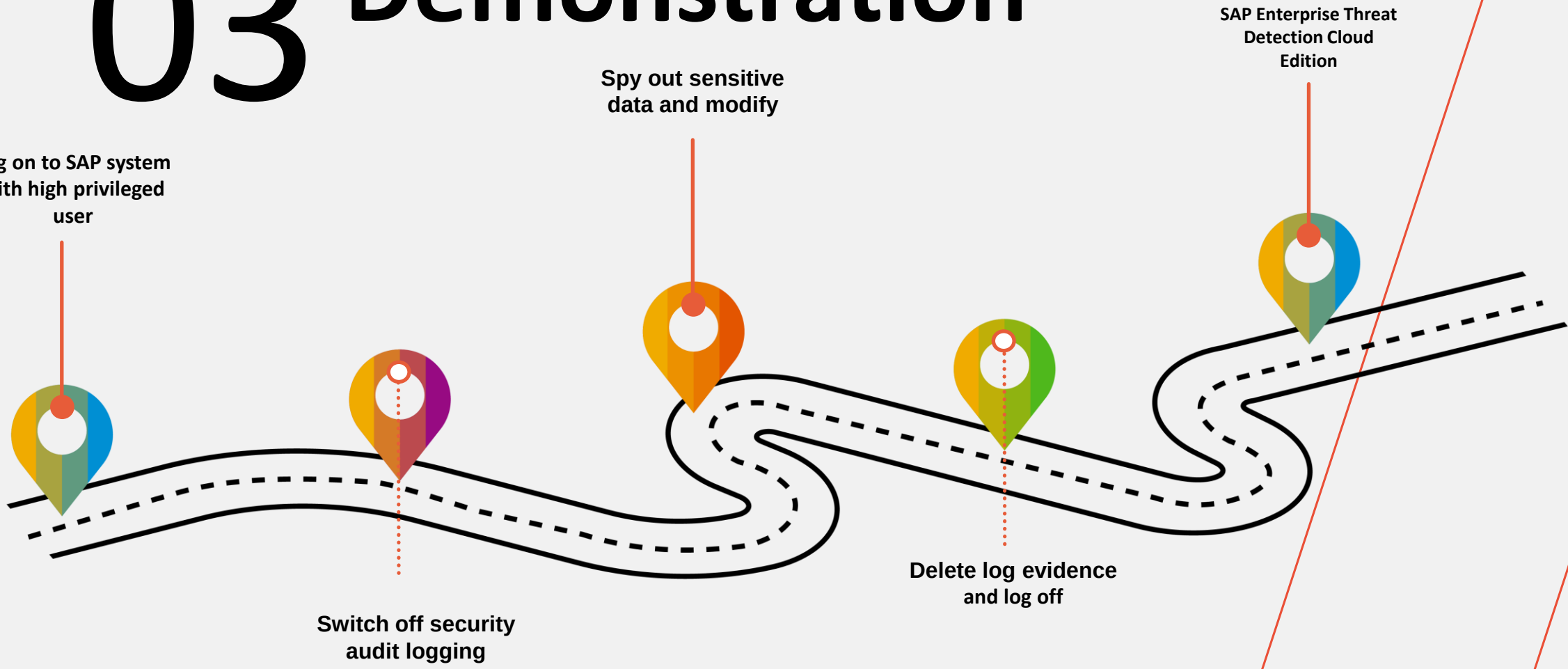
Why Use ETD alongside a Typical SIEM?





TURNKEY

03 Demonstration



TURNKEY

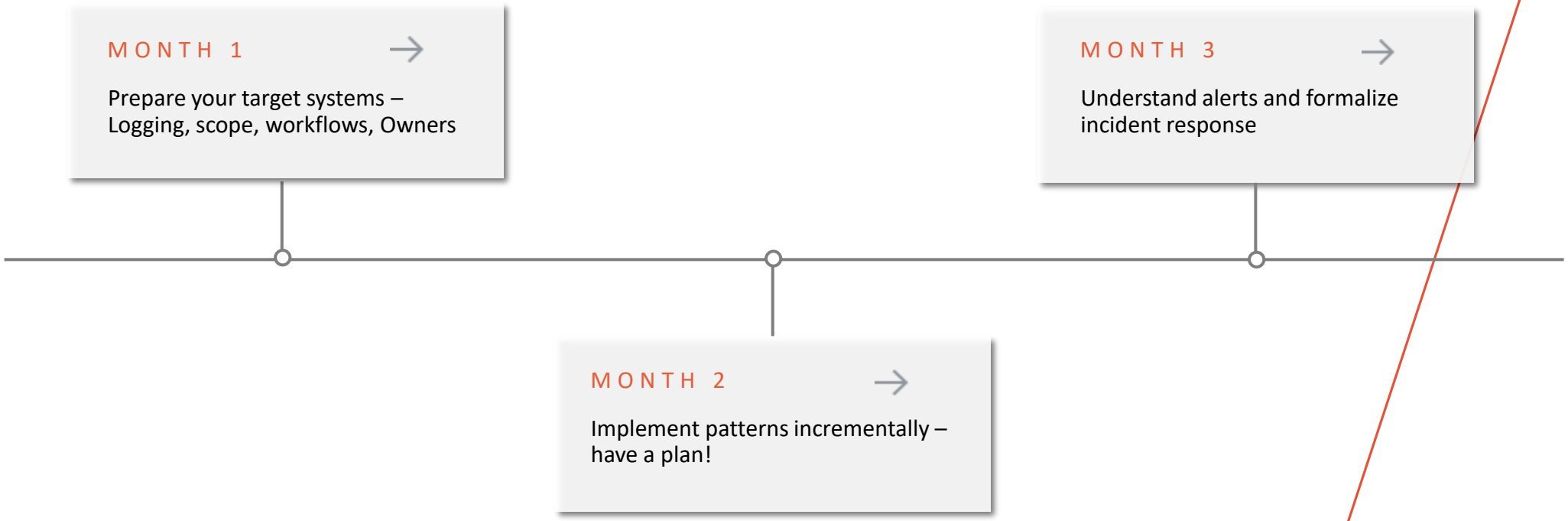
04

Operating ETD – Real World Experiences

TURNKEY

The Customer Journey

The first three months with ETD



TURNKEY

Top Tips for a Successful Implementation

"ETD cloud edition will bring a new level of insight into the operation of your SAP systems, but your organisation will need to be prepared"

- Plan ahead, what systems and tiers are you connecting? Do you have an existing SIEM that ETD will connect with?
- Enable monitoring of new patterns incrementally. Check and adjust for false positives before enabling more to avoid overload
- For on-premise implementations be conscious of existing functionality and leverage that rather than build custom patterns. E.g. Solution Manager Configuration Validation, GRC Process Controls, etc
- Take advantage of all the functionality. Very powerful investigation functionality is availible

Every Organisations Risk Tolerance is different – find what works for you

Testing patterns can be a challenge. Ask your MSP for on-premise implementations if they have any test scripts to trigger events

Leverage your partners and MSP to understand how to respond to incidents

Why a Managed Service Can Help

Take away the pain of managing an on-premise platform and fine tuning required to get accurate alerts

Can integrate with existing teams to ensure the efficient filtering and identification of incidents, and provide guidance on how to handle any detected events

Managed Service Providers often have scripts which can be used to test patterns, and will have knowledge from other organisations about what is effective

Managed Service Providers often offer complimentary services such as Pen Testing, Red Teaming, and reviews of configuration to suggest effective security controls

TURNKEY

Any Questions?

TURNKEY

Thank you!

Andrew.morris@turnkeyconsulting.com

rob.tyler@turnkeyconsulting.com

a.lingscheid@sap.com

www.turnkeyconsulting.com