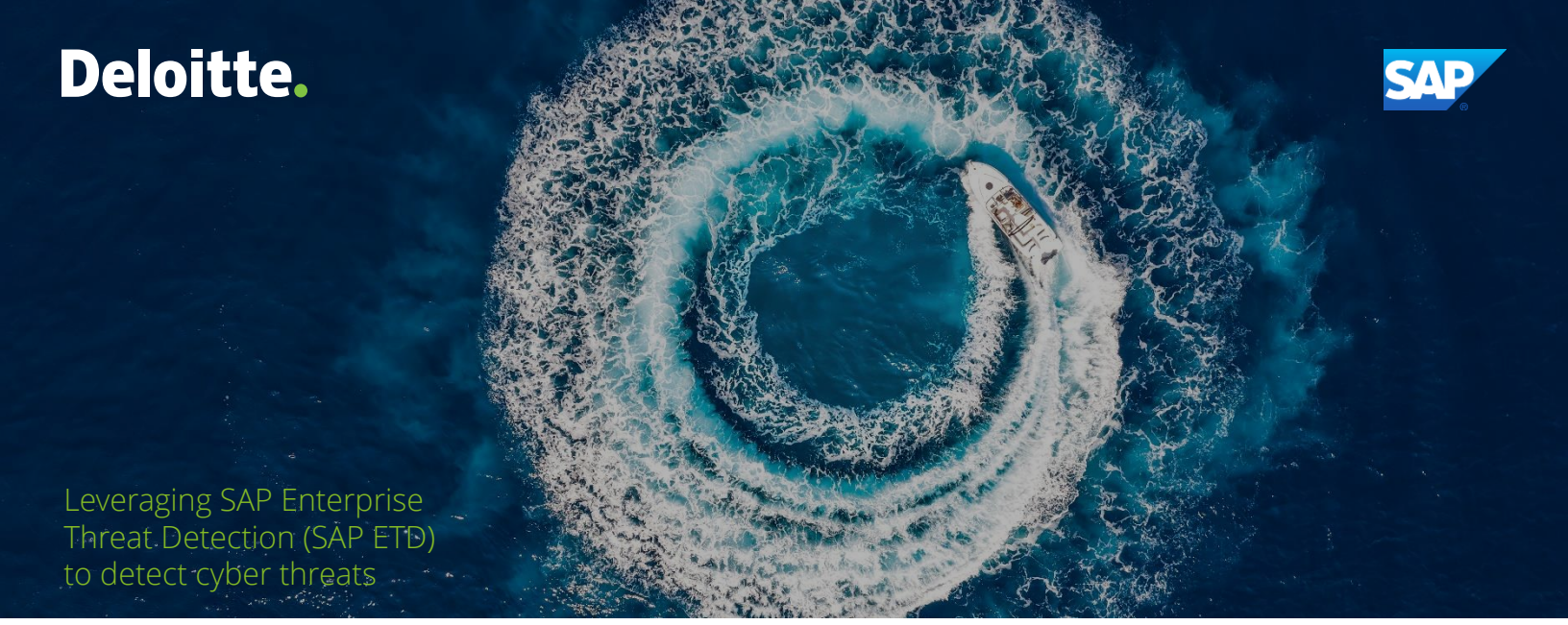


Leveraging SAP Enterprise Threat Detection (SAP ETD) to detect cyber threats

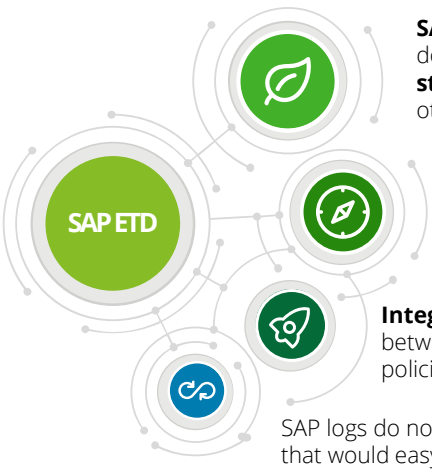
A success story of enterprise threats detection

SAP landscapes are quickly evolving towards more complex and larger environments supporting critical business processes in many organizations. **SAP is now seen as the core system, the digital heart of an organization**, one of the most valuable digital assets and it is vital to protect against cyber threats. Deloitte implemented SAP ETD enhancing visibility and monitoring over organization's SAP landscape. Starting with normalizing all the logs coming from various sources into the solution's security knowledge base, **SAP ETD was able to detect internal threats from internal users and third-party users that were responsible for non-core activities in the organization.** This tool provided security teams valuable insights, **enabling monitoring and detection of fraud attempts and information leaks in SAP**, which are very complex to achieve in a SAP environment, especially in large landscapes.

Why SAP ETD?

Integrating SAP application logs with SIEM applications can be a complex task and raise certain challenges.

SAP ETD delivers in-built connectors to SAP applications and log parsing enabling an easier management, analysis and correlation of logs, as well as an easier integration with other SIEM tools.



SAP systems have multiple types of logs which do not **have a standardized format or structure**: some are stored as log files in OS and others are stored in standard SAP database tables.

Volume - SAP systems usually have hundreds concurrent users and can generate many events logs that can raise up to an high volume of data in a short period of time and this data must be quickly transferred.

Integrations - Monitoring and maintaining many interfaces between SAP systems and SIEM platforms and log retention policies are highly costly in terms of effort and complexity.

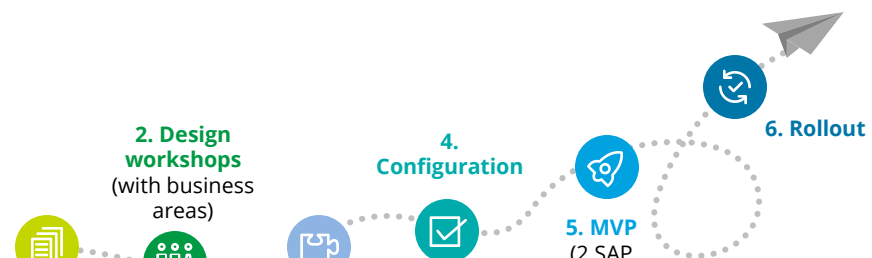
SAP logs do not natively have a standard format or include information that would easy be used for correlation in a SIEM tool.

Our approach

Deloitte's approach for the project included design workshops with business teams who provided valuable insights to design use cases, especially related with fraud activities and exfiltration attacks.

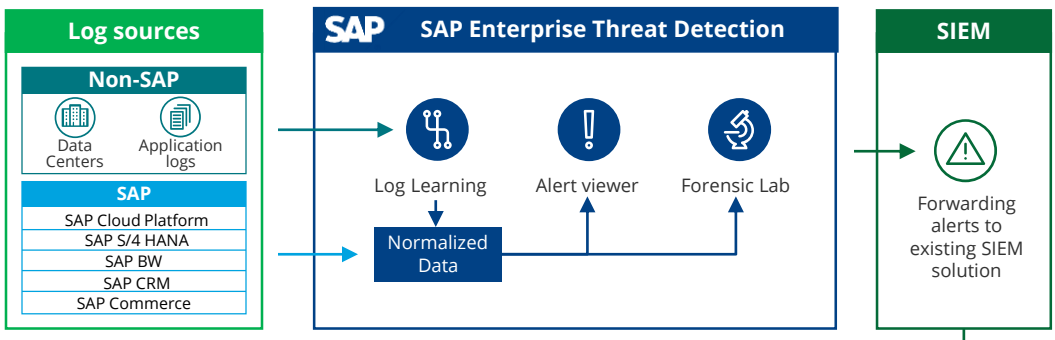
Here's a summary about implementation approach:

1. **Log assessment**: verify which types of logs were active in SAP landscapes to anticipate
2. **Design workshops**: involving business teams to provide insights for use-case design
3. **Architecture design**: Low Level Design about SAP ETD architecture and sizing and how to securely transfer SAP logs to SAP ETD
4. **Configuration**: use-case configuration in SAP ETD and forward alerts to existing SIEM solution
5. **MVP (Minimum viable product)**: Go-live with a MVP which included 3 log sources: 2 SAP systems and 1 non-SAP systems
6. **Rollout**: smooth rollout for the whole SAP landscape and embed SAP ETD in all new implementation products as log sources for this security platform.



Results

- This new tool represented a **major shift in security monitoring over SAP landscapes in this organization.** IT infrastructure logging was being monitored but there was a large lack of visibility over application logging.
- Diagram on the right summarizes how SAP was integrated and how log data and alerts flow in current security landscape.
- ETD is now a driver to **detect data breaches and anomalous user behavior** and fully integrated with existing SIEM solution which **helped SOC team to increase monitoring capabilities without extra effort.**



Examples of alerts generated through SAP ETD:

Data Exfiltration
Detecting when someone is downloading large amounts of sensitive data.

Fraud
Alerts for fraud cases inside the organization.

Acting as Another User
Detecting cases of users creating other users and then using them to do malicious activities.

Debugging
Alert when a user enters Debug Mode in Productive Systems.

Contacts

Frederico Mendes Macias
Partner
+351 966850347
fremacias@deloitte.pt

André Correia de Sousa
Manager
+351 962753775
andrsousa@deloitte.pt