History of SAP Solutions: SAP Enterprise Threat Detection

As part of our SAP solution spotlight series, Winterhawk spoke with SAP's Michael Schmitt (Product Manager) about the ongoing development of SAP Enterprise Threat Detection (ETD).

What is SAP Enterprise Threat Detection?

SAP ETD is a real-time security event management and monitoring solution. Its core capability is to secure SAP systems, enabling customers to detect, analyse and neutralise cyber attacks as they are happening, and before serious damage can occur.

What are the origins of Enterprise Threat Detection?

In 2013, feedback from customers was that they were unable to see in what was going on within the SAP Systems when it came to security. SAP systems were seen as a "black box" and it was difficult to determine whether or not a security issue had taken place.

There are many data capabilities within SAP systems but at that time the technical understanding of the semantics, and what they meant, was lacking. A tool was needed to correlate the different analytics coming out of one SAP system and find out what had really happened. Data was extracted out of a security audit log and out of a business transaction log and these correlated together, but it was unclear whether an attack or suspicious behaviour really was an attack, whether or not it was critical, and what phase the attack was at.

Many attacks are divided into two phases, preparation and execution. The preparation phase is something that you can see before it started and before any real damage is done. SAP ETD enables you to search billions of rows of data and find the correct information within the selections in seconds (e.g.; what did a given user do within an SAP system?).

Michael said, "Later in 2013 we started a POC, checking to see if S/4HANA would have the capability and stability to support real-time processing of data for ETD. Any initial doubts were eliminated when we tried it out - it was fantastic, which meant the POC was big success when it came to the technical feasibility. At the same time, we created a business case - as there were already customers who had said they would buy the solution, the business case was also successful. We began development of SAP ETD in 2014, with the first release in March 2015."

"SAP Enterprise Threat Detection is a real-time security event management and monitoring solution. It enables the customer to detect, analyse and neutralise cyber attacks as they are happening, and before serious damage can occur."

Dr Michael Schmitt
SAP Product Manager

"A staggering 70% of worldwide transactions now involve an SAP system. SAP Enterprise Threat Detection acts as a vital line of defence, enabling organisations to neutralise cyber attacks in real-time."

Linda Hewison
Partner, Winterhawk

About Winterhawk

Winterhawk is a leading global consulting practice, supporting organisations in SAP Security, SAP GRC services and solutions (more than 20) across a variety of SAP environments including SAP R/3, S/4HANA, ARIBA, Fieldglass, Concur and SuccessFactors.

Winterhawk is the Global Solution Partner for the United VARs Alliance (Platinum SAP Partners) servicing over 8,000 clients worldwide.

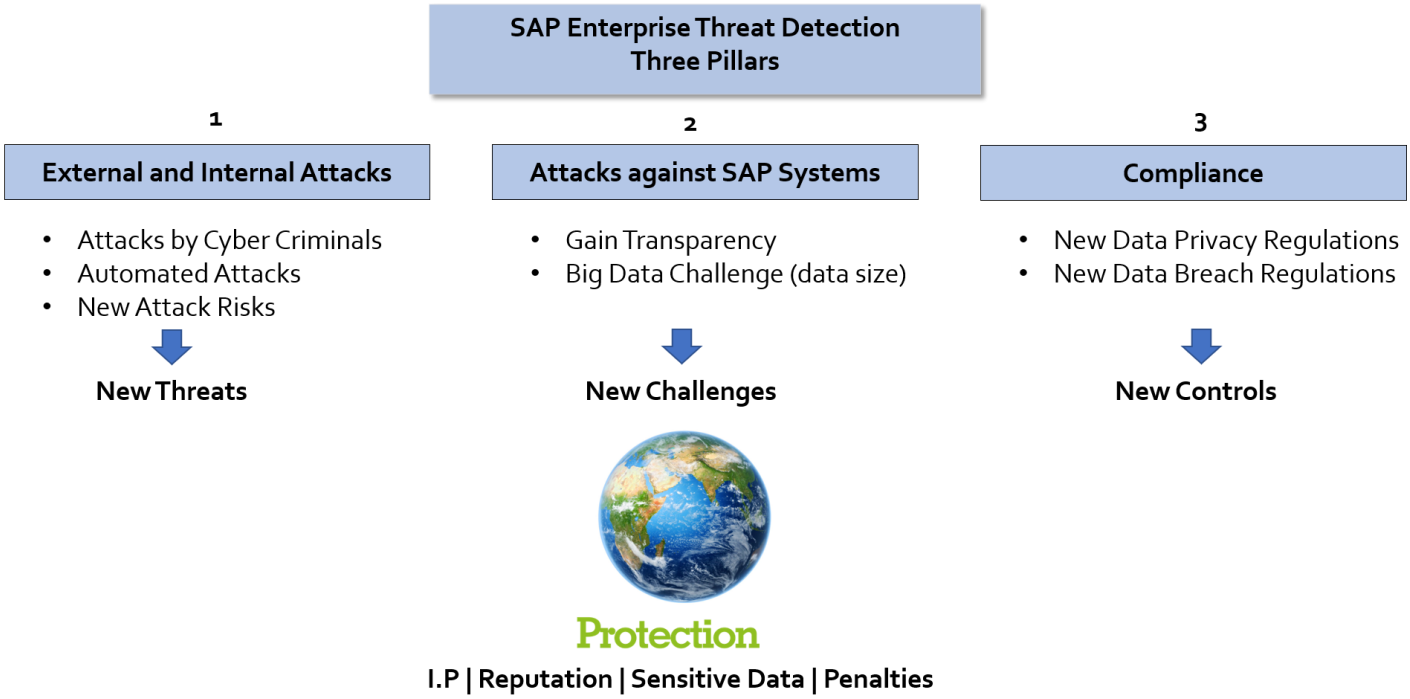
 • Email **info@winterhawk.com** • Website **www.winterhawk.com** • Twitter **@WH_Global** • LinkedIn **Winterhawk**

Who were its first customers?

The first customers were in Germany, where product promotion began, and where there was already a high awareness of security – within the first year, there was further interest from companies in the United States. The clients were not industry or technology specific, and they varied in size, ranging from mechanical engineering to the chemical and sports industries, as well as a large public sector company.

What customer challenges does ETD address?

We look at three pillars when it comes to the importance of SAP Enterprise Threat Detection. The first pillar relates to general cyber attacks from both external and internal threats. The second pillar relates to the lack of transparency in security, which is what drove this product's creation, together with the big data issue. The third pillar is compliance with ever-evolving data protection regulations.



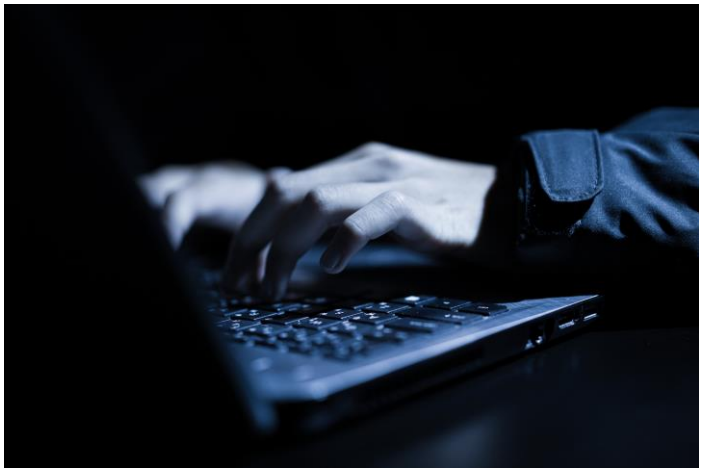
Any insights for C-Suite executives?

Cyber crime, cyber attacks, cyber security – we've become increasingly familiar with these terms over the past decade. They've become the hottest topics in boardrooms, with shareholders and CEOs alike asking their teams, "Are we safe? Are we protected?"

SAP Enterprise Threat Detection provides critical information to the Chief Information Officer (CIO) and Chief Security Office (CISO), who are typically the ones asked to provide assurance about an organisations' data security and risk statuses.

What's next for SAP ETD?

Customer feedback revealed a demand for further integration with other SAP products. A Business Integrity Screening Proof of Concept is currently under development, as there is a correlation of very different information between the two solutions. Traditionally, SAP Business Integrity Screening (on the business side) and SAP Enterprise Threat Detection (on the security side) have been marketed in different ways, but there is an opportunity to bring the two solutions together in the future because SAP gives access to the business transactions.



In the future it will be essential for SAP ETD to connect to all the SAP cloud solutions (SAP SuccessFactors, SAP Hybris / SAP Commerce Cloud, Ariba or S/4HANA These are all on the roadmap and with the aim to deliver some of these connections by the end of the year, along with the first support package. Separate content delivery is also planned on a regular basis, including the newest security patches available for SAP ETD customers to install. This becomes particularly important if there is a need to raise the criticality of a vulnerability or if new security notes are published.

How does SAP Enterprise Threat Detection support the intelligent enterprise?

SAP ETD helps keep systems secure in a continuously changing cyber security threat environment, leveraging powerful and flexible monitoring, detection, and response capabilities. The solution issues actionable alerts in time to neutralise threats to your business-critical assets to help prevent damage to your business and reputation.

- ✓ Identify security lapses in your application landscape readily and efficiently with the real-time data processing combination of smart data streaming services (SDS) and the SAP HANA platform.
- ✓ Consolidate and process large amounts of events with the SAP HANA platform to gain insight at unprecedented speed.
- ✓ Gain an overview of the threat situation, perform forensic investigations, and discover new attack patterns.

Get in touch

SAP Enterprise Threat Detection gives you unmatched insight into suspicious activities in your business application landscape and enables you to identify breaches as they occur.

Winterhawk supports clients in 90 countries. We are proud to be innovative, independent, and cost-effective. Our services are complemented with deep domain expertise, content, accelerators, and toolkits.

Outside of SAP, Winterhawk supports organisations requiring guidance in Access and Identity Management (IAM), Cyber Security (Pen Testing, Network Detection, Antivirus and SIEM); we support clients through Regulatory services and solutions for compliance with GDPR, SOX, FCPA, CCPA as well as standards such as ISO* and also through their Digital, HR and Finance Transformation projects.

Winterhawk has established its head office in the UK, with resources located across EMEA, the United States, Canada, and Australia. Contact us for solution demonstrations and for free assistance with building your business case.