SAPinsider

This article appeared in the Apr ▪ May ▪ Jun 2016 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.

WIS pubs

Martin Plummer
(martin.plummer@sap.com) is the senior product specialist for SAP Enterprise Threat Detection. He joined SAP in 2000 after seven years in the defense industry, where he worked in research and development. He holds degrees in applied physics and optoelectronics.

An Integrated Approach to Identifying Security Risks

How the Latest Enhancements to SAP Enterprise Threat Detection Enable Integrated Analysis Across Your Landscape

As technology continues to evolve and expand its reach — bringing previously unimagined interconnectedness through networks such as the Internet of Things — the sophistication and scope of cyberattacks continue to grow as well. With attacks on the rise that hijack network-connected devices and manipulate, not just steal, data (imagine the implications of a modified pressure sensor reading in an oil pipeline or manipulated stock prices),[1] rapid threat detection is a critical need for enterprises.

To help its customers address these challenges, SAP provides SAP Enterprise Threat Detection, a native SAP HANA application that SAP itself uses to help protect its own business systems. Released for general availability in March 2015, SAP Enterprise Threat Detection combines the high-performance complex event processing functionality of the SAP Event Stream Processor (SAP ESP) engine with the real-time capabilities of SAP HANA to quickly identify suspicious patterns in your landscape. It gathers log data from monitored applications and systems, normalizes that data into an interpretable format using SAP ESP, and then performs attack pattern analysis and generates alerts using SAP HANA.

The speed at which SAP Enterprise Threat Detection analyzes security-relevant log data is a significant advantage in combating cybercrime — the earlier you can address a threat, the less opportunity there is for damage to your business. And you can take advantage of this speed to monitor both SAP and non-SAP systems. Used as a stand-alone security monitoring solution, SAP Enterprise Threat Detection effectively correlates and analyzes security-relevant log data regardless of its original source.

However, organizations often already have specialized monitoring solutions in place, such as solutions for sandboxing potential malware, as well as more general security information and event management (SIEM) solutions for gathering and analyzing log data. The latest release of SAP Enterprise Threat Detection — support package 03 (SP03) for version 1.0, planned for Q1 2016 — enables you to have the best of both worlds by leveraging the strengths of your existing tools while benefitting from the depth and speed of SAP HANA and the processing capabilities of SAP ESP.

This article explores some of the enhancements included in this new release of SAP Enterprise Threat Detection. In particular, it looks at how external tools can integrate

[1] Wired, "The Biggest Security Threats We'll Face in 2016" (January 1, 2016; www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016).

information from SAP Enterprise Threat Detection and how the solution can now more easily consume log data from non-SAP systems.[2]

Providing Threat Information to External Tools

In many cases, organizations running both non-SAP and SAP systems have already invested time and resources into getting an SIEM solution up and running to help protect their landscapes, and their SAP systems represent a blind spot that they want to cover by extracting data from those systems and incorporating it into their SIEM solution.

While SAP Enterprise Threat Detection can provide external SIEM solutions with the log data from SAP systems, it makes little sense to use the application simply as a glorified data extractor. A more savvy approach is to first use the speed and attack detection functionality of SAP Enterprise Threat Detection to identify potential threats, and then make that distilled information available for the external tool to incorporate into its threat analysis.

SAP Enterprise Threat Detection identifies threats by running attack detection patterns on log data and generating alerts when suspicious patterns are found. The information contained in these alerts — such as system, user, and terminal information — can be very useful for threat analysis, and using the distilled information in these alerts rather than the raw log data vastly reduces the amount of information to be transferred to the external tool while also increasing that information's value.

[2] For a detailed overview of SAP Enterprise Threat Detection, see my article "Safeguard Your Business-Critical Data with Real-Time Detection and Analysis" in the October-December 2014 issue of *SAPinsider* (SAPinsiderOnline.com).

With SP03, there are multiple options for making SAP Enterprise Threat Detection alerts available to external tools. You can:

- Push alerts via email
- Push alerts in JavaScript Object Notation (JSON) format
- Pull alerts from SAP Enterprise Threat Detection using a JSON API

Push Alerts via Email

Email notification of alerts is a useful feature for smaller organizations with security teams that do not have the resources to continually monitor their screens, or for organizations with integration processes that rely on email. With this approach, the recipient of the email can incorporate the information contained in the alerts as needed into the external tool for use in the analysis.

Here, we'll look at how to switch on email notifications for all SAP Enterprise Threat Detection alerts of a certain severity level or higher, as well as the user-specific configuration that is required for specifying a recipient of the emails (with the assumption that the required SMTP settings are already configured in the SAP Enterprise Threat Detection system).

Before you start, be sure to select your attack detection patterns and tune them to your own needs, so that you are not inundated with email messages. Once you are confident that your alerts are being generated in manageable quantities and with the appropriate relevancy, go to the Manage Alert Publishing settings of SAP Enterprise Threat Detection and select Publish via Email (see **Figure 1**). Then specify the minimum severity level for the alerts to be sent via email and the address that will appear as the sender of the email.

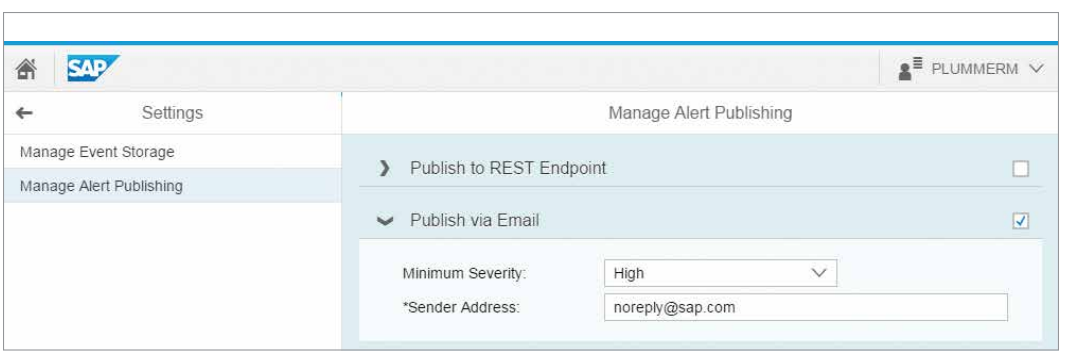

Figure 1 Specify the type of publishing for the alert and the minimum severity level required to publish the alert

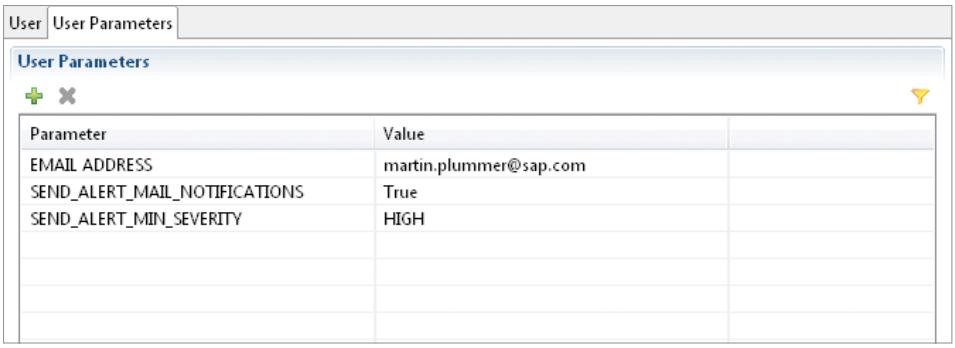

Figure 2 Specify the user parameters for the recipient of the emailed alerts in the SAP HANA studio

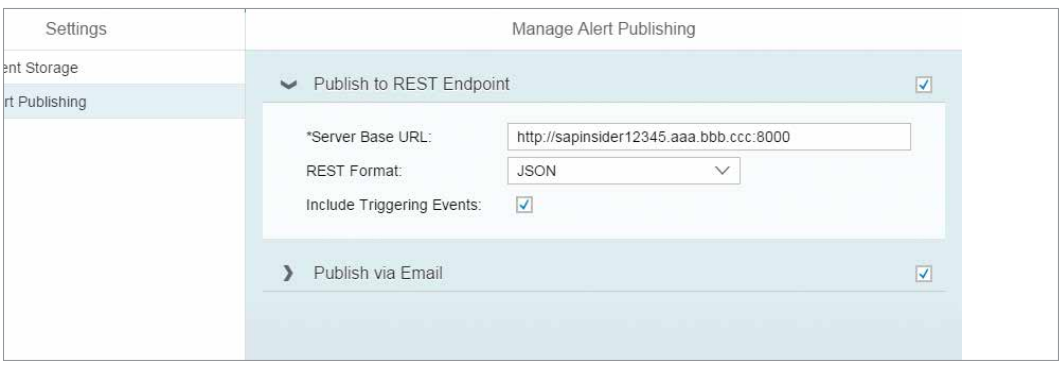

Figure 3 Configure SAP Enterprise Threat Detection to publish alerts in JSON format

The user-specific settings for the email recipient are made using either the desktop-based SAP HANA studio or the SAP HANA web-based development workbench, a browser-based development tool for native SAP HANA applications included with SAP HANA extended application services (known as "XS"). In the development tool, you must navigate to the user (under Security > Users) and on the User Parameters tab (see **Figure 2**), set the specific parameters SEND_ALERT_MAIL_NOTIFICATIONS and SEND_ALERT_MIN_SEVERITY accordingly, as well as the email address of the recipient.

With the configuration shown for the example, the specified email address receives a message for each execution of an attack detection pattern that results in at least one new alert that has, at a minimum, a high level of severity. Included in the email are a description of the pattern, the severity, the systems affected, and a list of the new alert IDs. Clicking on an alert ID opens SAP Enterprise Threat Detection at the relevant alert for further analysis.

Push Alerts in JSON Format

SAP Enterprise Threat Detection can also send its alerts to an external system as a REST-based service in JSON format.[3] In addition to sending standard alert information (AlertId, AlertSeverity, PatternName, and so on) from SAP Enterprise Threat Detection, it is possible with the JSON approach to include information about the events that caused the alert. Keep in mind, however, that including this additional event information could add considerable volume to the amount of data that is transferred.

To publish alerts in JSON format, in the Manage Alert Publishing settings of SAP Enterprise Threat Detection, select the Publish to REST Endpoint (see **Figure 3**). Then specify the base URL of your SAP Enterprise Threat Detection server and whether to include the events that triggered the alert.

Next, you need to edit the destination object for SAP Enterprise Threat Detection alerts (alerts.xshttpdest) to point to the recipient of the alerts, which is your external system or SIEM solution. Open the web-based admin tool included with XS for the basic maintenance, such as security and authentication, of native SAP HANA

[3] Representational State Transfer (REST) is an architectural standard that enables communication between systems via HTTP and using simple text-based message formats such as JSON.

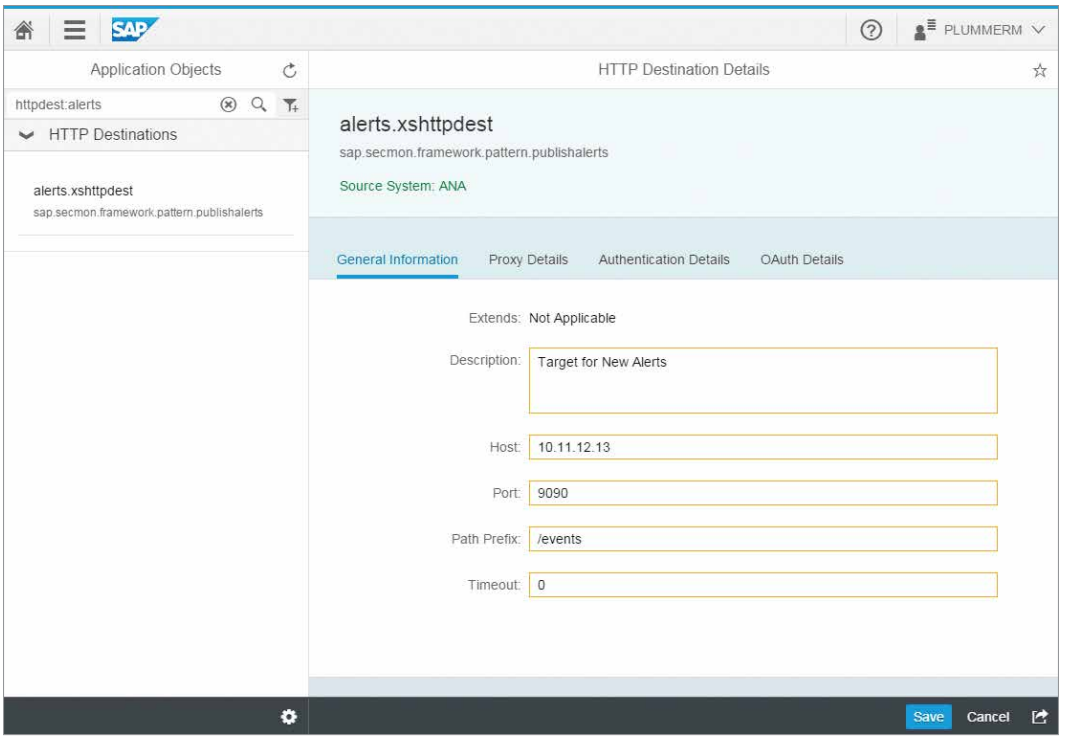

Figure 4 Specify the destination of the JSON-based alert in the XS admin tool

applications. In the XS admin tool, specify the host and port information for the recipient system (see **Figure 4**).

With these configurations complete, your system will now send the alerts to the specified destination system or SIEM solution.

Pull Alerts Using a JSON API

In some cases, you may want to pull alerts from SAP Enterprise Threat Detection into your external tool. This is made possible using the REST-based alert API (/sap/secmon/services/Alerts.xsjs) of SAP Enterprise Threat Detection, which enables alerts to be consumed by external tools in JSON format. You simply query this API from the external tool using the base URL of your SAP Enterprise Threat Detection server and the parameters AlertId, AlertCreationTimestamp, and includeEvents as needed to meet your needs.

For example, the following URL would pull an alert with the ID 2011254895, its triggering events, and a link to the alert in SAP Enterprise Threat Detection:

```
http://sapinsider.aaa.bbb.ccc:8000/sap/secmon/
services/Alerts.xsjs?$includeEvents=true&$qu
ery=AlertId%20eq%2011254895
```

The URL that pulls the alert into an external tool can also be used to view the alert in a standard browser, albeit in a less visually appealing format.

Integrating External Tools with SAP Enterprise Threat Detection

Many SAP customers use specialized threat detection solutions that provide alerts or notifications that can be extremely valuable for monitoring solutions. For example, a warning that a particular terminal is showing signs of danger could signal the need for additional tests to monitor the situation or a closer look at existing data to see if something was missed by the standard detection patterns.

SAP Enterprise Threat Detection is a powerful and efficient tool for real-time monitoring of your system landscape. The latest enhancements enable you to extend these advantages to create a comprehensive monitoring solution by making it even easier to incorporate data from external tools into SAP Enterprise Threat Detection.

Connecting External Log Providers

Systems monitored by SAP Enterprise Threat Detection are known as log providers. Standard log providers that are supported out of the box — such

as the ABAP and Java versions of SAP NetWeaver Application Server and the SAP HANA audit trail log — are connected using built-in integration with SAP Enterprise Threat Detection. When it comes to connecting non-standard log providers, such as external tools, you must consider the most suitable option.

With SP03, the recommended way to connect a non-standard log provider to SAP Enterprise Threat Detection is through the runtime adapter included with SAP Enterprise Threat Detection, which SAP also uses to transmit the audit trail log for SAP HANA from the system log (syslog) to SAP Enterprise Threat Detection. Through the runtime adapter, SAP Enterprise Threat Detection can easily receive syslog messages via User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). Many potential log providers use syslog or something similar to make their logs available, in which case they are already ready to send log data to SAP Enterprise Threat Detection — you simply need to adjust the relevant configuration files to point to SAP Enterprise Threat Detection using UDP or TCP.

To integrate data from non-standard log providers, SAP Enterprise Threat Detection includes two tools that enable you to create rules for parsing and interpreting the log data without the need for development expertise: a log learning tool that teaches SAP Enterprise Threat Detection how to interpret and normalize logs using runtime rules, and a knowledge base tool referenced by the log learning tool that stores metadata about new types of logs, the events they include, and various predefined attributes. By combining these tools, which have been enhanced with SP03, with a runtime adapter that can serve as a single connector for multiple log providers, you can very quickly connect diverse sources to SAP Enterprise Threat Detection.

There are some log formats that the log learning tool cannot yet handle, however — for example, logs with deep structure, such as logs in XML format, and logs with events spread over multiple lines, such as Microsoft Windows error logs. You can create your own custom SAP ESP projects to handle these types of logs, or if you have specific monitoring needs, such as monitoring performance, you can create a specific SAP ESP adapter for that purpose.[4]

[4] Detailed information on creating custom SAP ESP projects for this purpose is available in the SAP Enterprise Threat Detection implementation guide and in the SAP ESP documentation.

An Updated Data Model

In its initial release, SAP Enterprise Threat Detection focused primarily on connecting to ABAP systems. Accordingly, the data model for storing log entries in SAP HANA for analysis reflected an ABAP-dominated format, with a header table containing some of the most-used attribute fields for ABAP, network, and system logs, and a corresponding details table for storing additional information.

With the newest release, the data model reflects the expanded scope of SAP Enterprise Threat Detection, with a less heavy focus on ABAP and a significantly expanded header table that contains all the allowed attributes. With all attributes now in the header table, the details table is no longer necessary and has been dropped, making the process of log learning and maintenance of the knowledge base simpler, and making it easier to work with the events in the forensic lab — the main tool in SAP Enterprise Threat Detection, where threats are analyzed and attack detection patterns are created. Additionally, this has a positive effect on the sizing of the SAP HANA database, making it possible to keep log events for longer periods of time.

The knowledge base and log learning tools provide a useful illustration of the changes to the data model introduced with SP03. In the knowledge base tool (see **Figure 5** on the next page), events and log types remain freely definable, the list of predefined attributes has been expanded, and roles are now incorporated into the ATTRIBUTES tab instead of appearing separately on their own tab.

In the log learning tool, the STAGING ENTRY TYPES tab shows where the attributes listed in the knowledge base are used (see **Figure 6** on the next page). To give you an idea of how the application learns to normalize logs,[5] let's take a closer look at some of the key areas of this tab:

- **Markup:** The tool automatically generates the markup using the sample log file that you upload, which is taken from a source log in the monitored system and should contain examples of the various events to be identified. SAP Enterprise Threat Detection will use the markup as its basis for identifying log events.

[5] Note that the finer points of adding annotations to the log, which the log learning tool uses to automatically generate the runtime rules for interpreting the log, is beyond the scope of this article. Details are available in the SAP Enterprise Threat Detection implementation guide.

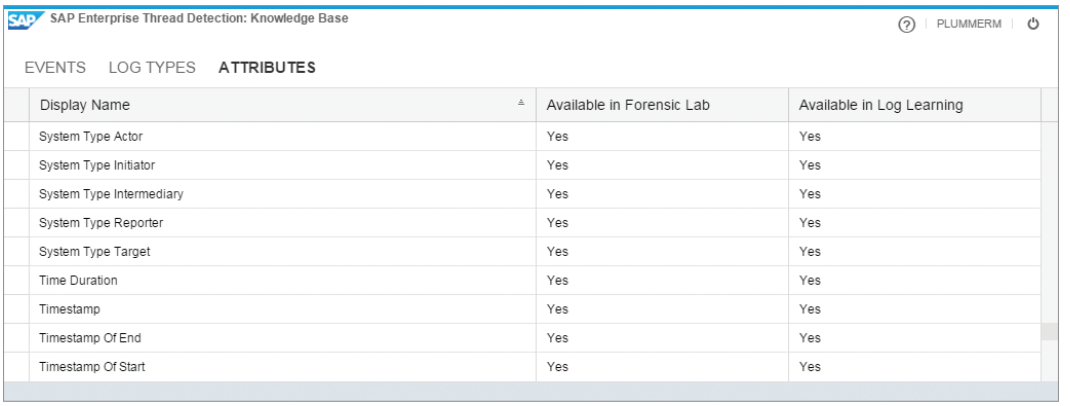

Figure 5 The new data model reflected in the knowledge base tool

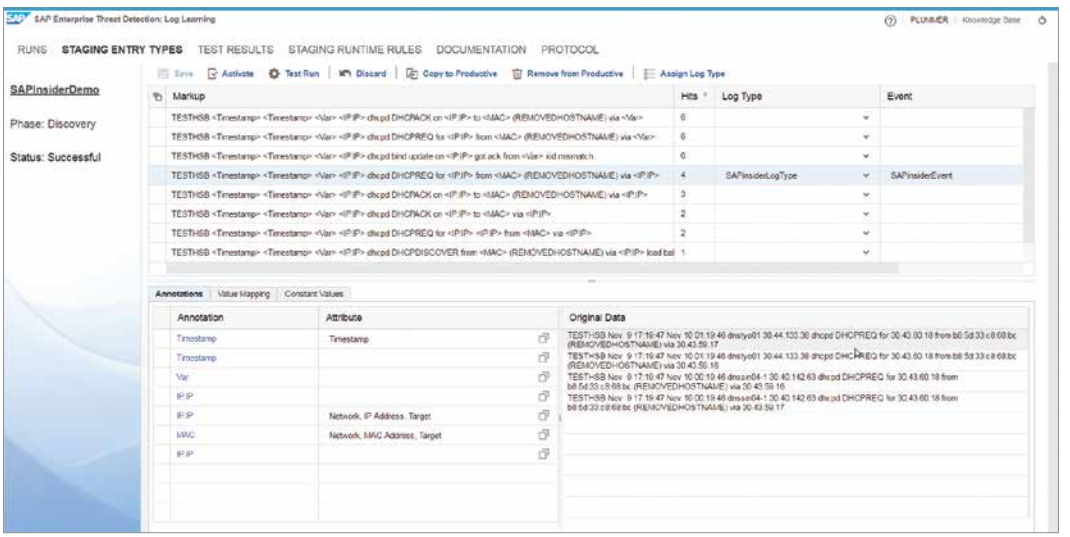

Figure 6 The log learning tool

- **Log Type and Event:** For each line of markup, you tell the tool what type of event it corresponds to. The sample log file may contain events from different log types (for example, the source log might be an amalgamation of various logs).
- **Annotations:** This is where you specify the parts of the markup that correspond to particular attributes in the knowledge base, such as Timestamp and IP address. The annotations made here will be available for analysis in the forensic lab of SAP Enterprise Threat Detection — or, looking at it another way, if you are not interested in storing part of an event, you can leave that section un-annotated.
- **Original Data:** Here, you can see the original data from the uploaded file that corresponds to the selected markup. You can use this to help with your annotation of the markup.

In the example shown here, only the events that correspond to the highlighted markup would be identified, and the annotated timestamp and the annotated IP address would be extracted and stored.

Summary

With the release of SP03 for SAP Enterprise Threat Detection 1.0, adjustments to the data model have not only made working with log data easier, they have also significantly improved performance and sizing. Integration with third-party tools and log providers has been eased considerably, particularly via interfaces for accessing and publishing alerts, allowing you to consider scenarios that leverage all the useful security tools in your landscape, and enabling you to benefit from actionable, understandable analysis in real time. Learn more at **http://scn.sap.com/docs/DOC-58501** and **http://help.sap.com/sapetd**. ■