

How to **Detect & Prevent** Attacks on **SAP S/4HANA**?

Sandip Dholakia, SAP
October 20, 2022

PUBLIC



Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Agenda

Detecting a possible attack

Ask what logs can do for you

- Importance of logging
- Raw materials for detection & investigation

Logging for Security in SAP S/4HANA

- Challenges in SAP S/4HANA logging
- What to look for in SAP S/4HANA logs

Tools for the Trade

- SAP Enterprise Threat Detection
- SAP Data Custodian
- SAP UI Data protection Logging

Key Takeaways & Resource

The damage related to
Cybercrime
is projected to hit
\$6 trillion USD
by 2022

Detecting a possible attack

- Unrecognized login / Multiple login attempts
- Unknown use/change to data or application
- Multiple requests from the same IP
- Change of permission by non-admin account
- Access from unknown location



**Malicious insider or
an external attack ?**

How can we find out & prevent?

Answer: Logs

**Logs can help identify, possibly
prevent and investigate the attacks**

Ask what logs can do for you!

- Logging can give detailed information about -
 - suspicious activities
 - configuration changes within the system.
- Different log sources can provide a comprehensive view onto the activities.
- You can learn to improve your current security setup based on the events you discover in the logs.
- The security detection process becomes more agile.
 - If logging is taken seriously you could provide quicker response time to security events and better security program effectiveness.

Open Web Application Security Project - OWASP

Security Logging and Monitoring Failures
is the 9th Vulnerability
on the OWASP Top 10
Vulnerability list of 2021!

Insufficient Logging Vulnerability
was
number 10 in 2017

It moved up in ranking!!

Use logs to detect or investigate an attack

- Timestamped logs are MUST in investigation
- Aggregating logs into centralized repository
- Create the baseline
- Generate Alerts
- Right tools for the trade

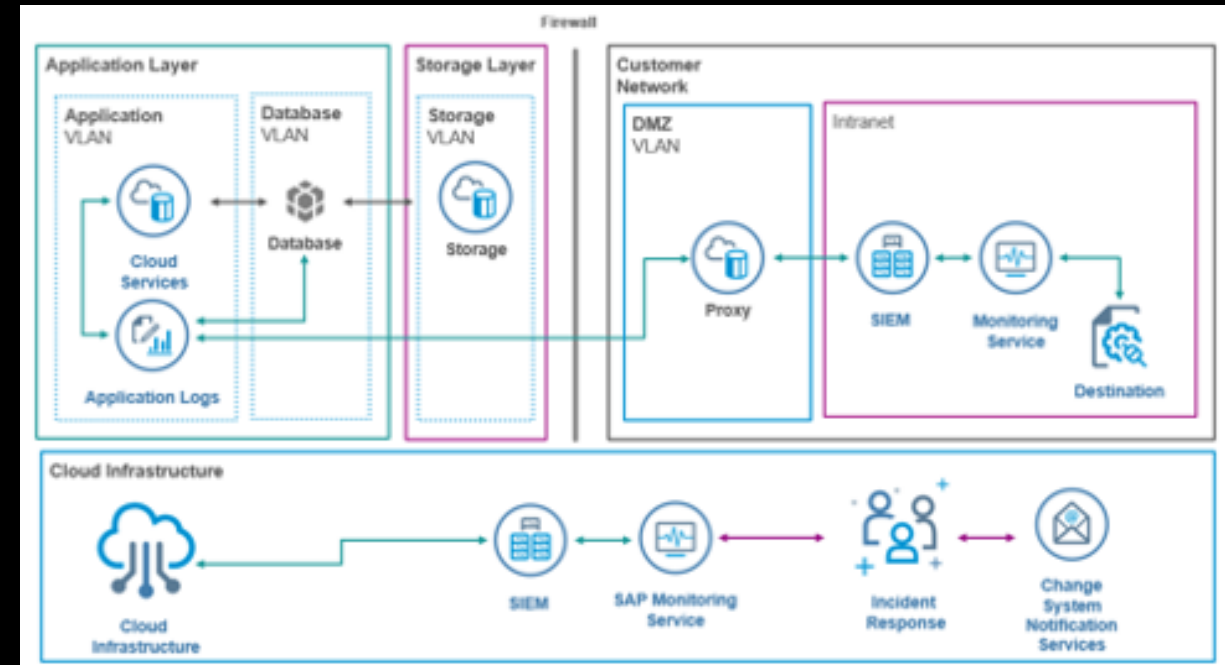
Raw Materials for Investigation

- **Timestamp**
- **Aggregation**
 - **Alerts**
 - **Tools**



Logging for Security in SAP S/4HANA

- Is (*somewhat*) challenging!!
- Many different logs are available
- SAP logs are complex and user must know the system to evaluate
- Traditional SIEM (Security Information & Event Management) tools do not work well
- Not all logs are enabled by default



Examples of Logs in SAP S/4HANA

- Security Audit logs
- System logs
- SAP Web Dispatcher logs
- ICM logs
- Security logs, HTTP access logs, Gateway logs
- Business transaction logs
- Application specific change logs
- Change document logs
- User change logs
- Read access logs

Logs we focus on

Security audit logs

Read access logs

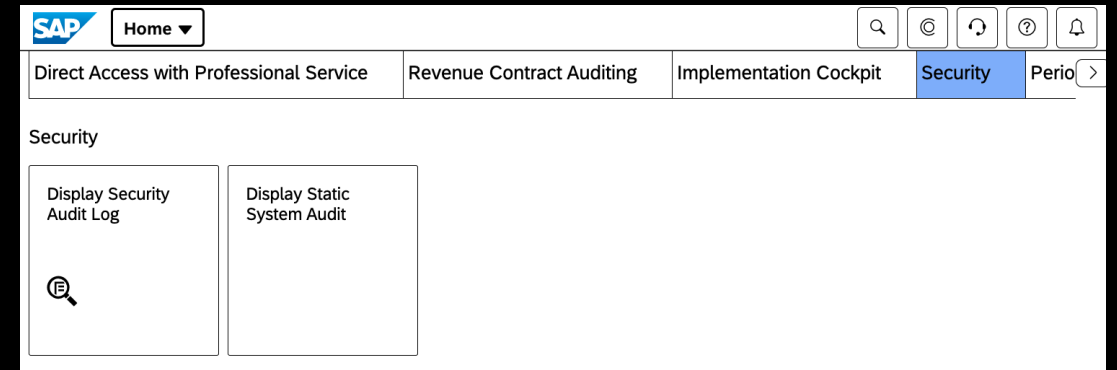
User change logs

Business transaction logs

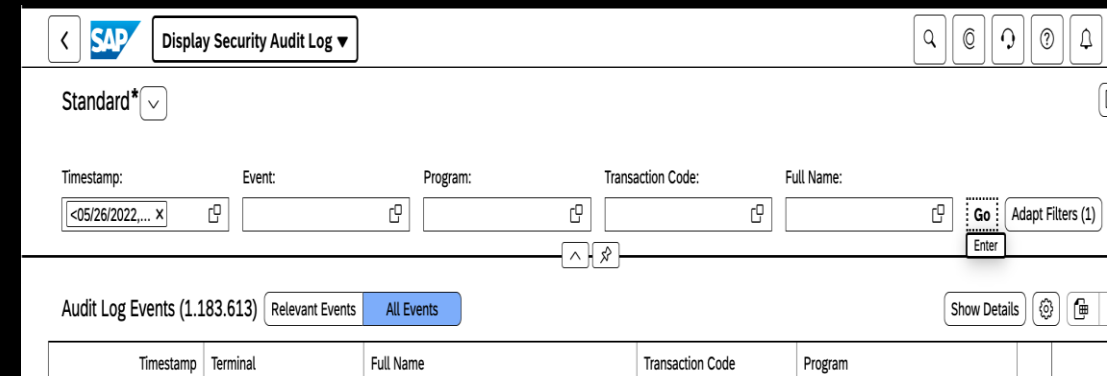
Security Audit Logs

- Captures security relevant information
 - Successful and unsuccessful logins
 - Starting and stopping of an app by a user
 - Changing data fields while debugging sessions
 - Download of files from backend
 - RFC calls to function modules
 - Successful and unsuccessful transaction starts
 - Changes to the security audit logs configuration
- Who can access SAL?
 - External auditor
 - Administrator
 - Data privacy specialist

Display Security Audit Logs



What to look for in SAL?



Read Access Logs

- Logs access to sensitive data
 - Who is trying to read the sensitive information?
 - Who is accessing employees' personal information?
 - Which employees are accessing the company's financial information?
 - Who is accessing trade secrets of the business?
- Read Access Logging: Configuration
- Read Access Logging: Monitoring
- Who can access RAL?
 - Administrator
 - Data privacy specialist

RAL Configuration

The screenshot shows the 'Read Access Logging Configuration' page in SAP. At the top, there's a navigation bar with the SAP logo and the title 'Read Access Logging Configuration'. Below this, the 'Channel' is set to 'Web Service'. The 'Search Criteria' section includes fields for 'Object Type', 'Interface Name', 'Namespace', 'Operation Name', 'Description', and 'State', each with a dropdown menu and a search icon. The 'Maximum Number of Hits' is set to 100. There are 'Search', 'Clear', and 'Reset' buttons. A 'Saved Search' dropdown is also present. At the bottom, there's a toolbar with buttons for 'Create', 'Activate', 'Deactivate', 'Check', 'Delete', and 'More...'. Below the toolbar is a table with columns: 'Actions', 'Owner', 'Description', 'Object Type', 'Interface Name', 'Interface Namespace', 'Operation Name', 'State', and 'Software Component'.

RAL Monitoring

The screenshot shows the 'Read Access Logging Monitor' page in SAP. At the top, there's a navigation bar with the SAP logo and the title 'Read Access Logging Monitor'. Below this, the 'Data Source' is set to 'Expanded Database'. The 'Search Criteria' section includes fields for 'Channel', 'Date / Time', 'User Name', 'System ID', 'Client', 'Field Value', 'Log Domain', and 'Log Domain With Value', each with a dropdown menu and a search icon. The 'Maximum Number of Hits' is set to 100. There are 'Search', 'Clear', and 'Reset' buttons. A 'Saved Search' dropdown is also present. At the bottom, there's a 'Search Result' section with a 'View' dropdown set to 'Default', a 'Download' button, and 'Hits: 0'. Below this is a table with columns: 'Created At (Loc...', 'User Name', 'System ID', 'Client', 'Channel', 'Direction', 'Logging Purpose', 'Channel Status', and 'Status Text'. A message at the bottom states: 'The table does not contain any data'.

User Change Logs

- Records changes to users and authorization
 - User password
 - User type
 - User group
- User Change Log can identify:
 - ☐ User creeping,
 - ☐ Privilege escalation, and
 - ☐ Other changes to user information within the system
- Useful in identifying whether the user is acting beyond the given scope

Not to confuse with IAM.

The user changes included here are not part of IAM or central user access, but rather are local to the SAP S/4HANA system.

How to use User Change Logs?

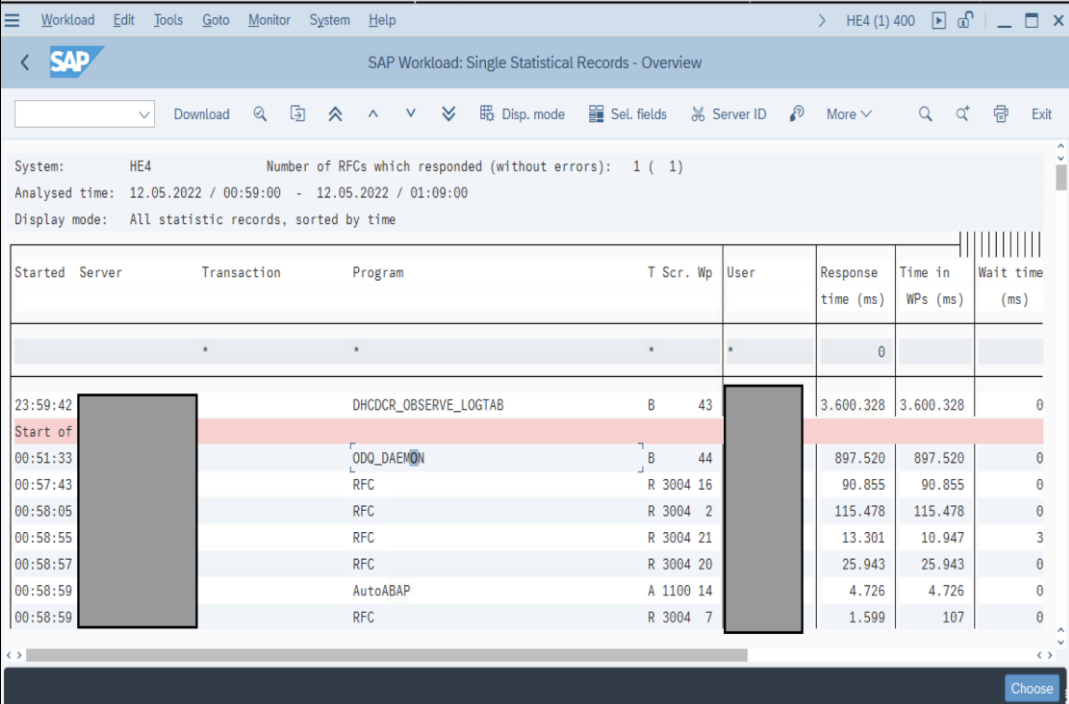
The user change log is a useful tool in the incident response as well as in forensic analysis. The logged data could provide evidence of user misbehaviors, if any.

The screenshot displays the SAP User Change Log interface. At the top, there are filters for 'Changed On' (09.05.2022 - 09.05.2022), 'Business User ID' (empty), and 'Action' (a dropdown menu). A 'Go' button and 'Adapt Filters' link are also present. Below the filters, a table titled 'Change Documents' is shown. The table has columns for 'Business User ID', 'Change Category', 'Attribute/Object', 'Action', and 'Value From'. The table is currently empty, with 'No data' displayed. To the right of the table, there are links for 'Download' and 'Changed By'. A dropdown menu for the 'Action' filter is open, showing a list of actions with checkboxes: 'User created', 'User deleted', 'Password changed', 'Lock changed', 'Validity period changed', 'Alias changed', 'Business roles changed', 'Business roles added', 'Business roles removed', and 'Changes due to technical reasons'.

Business User ID	Change Category	Attribute/Object	Action	Value From
No data				

Business Transaction Logs

- Contains primary events related to business transactions within the system
- Provides statistical data for all the transactions and programs
- The business transaction logs provides:
 - Server name
 - Program or transaction
 - User
 - Response time
 - Wait time and
 - Many other details for any given transaction



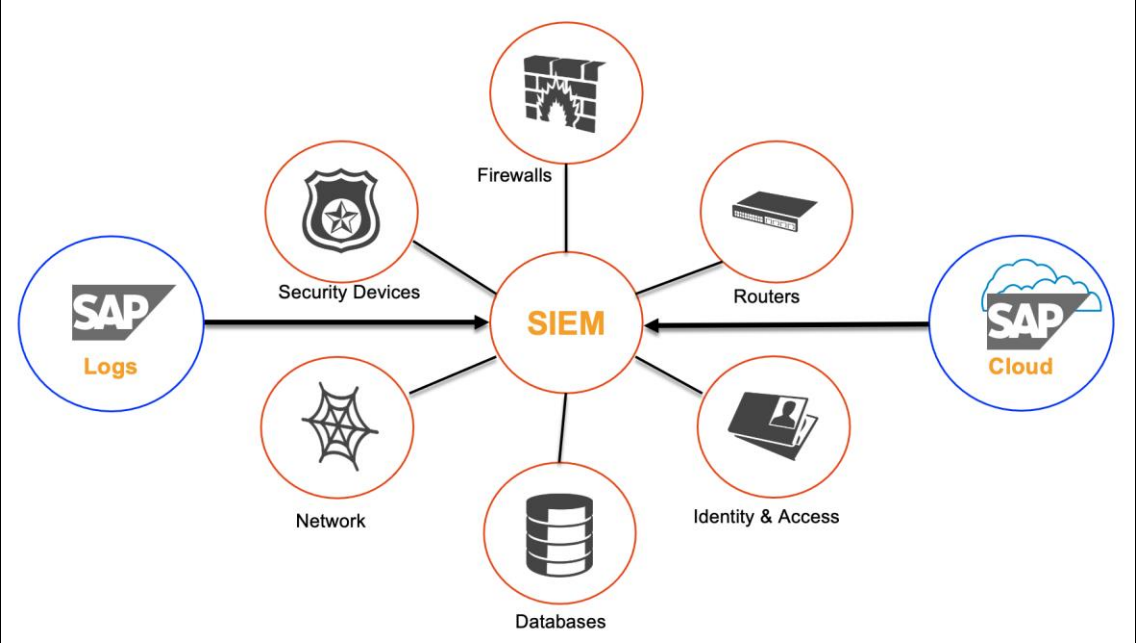
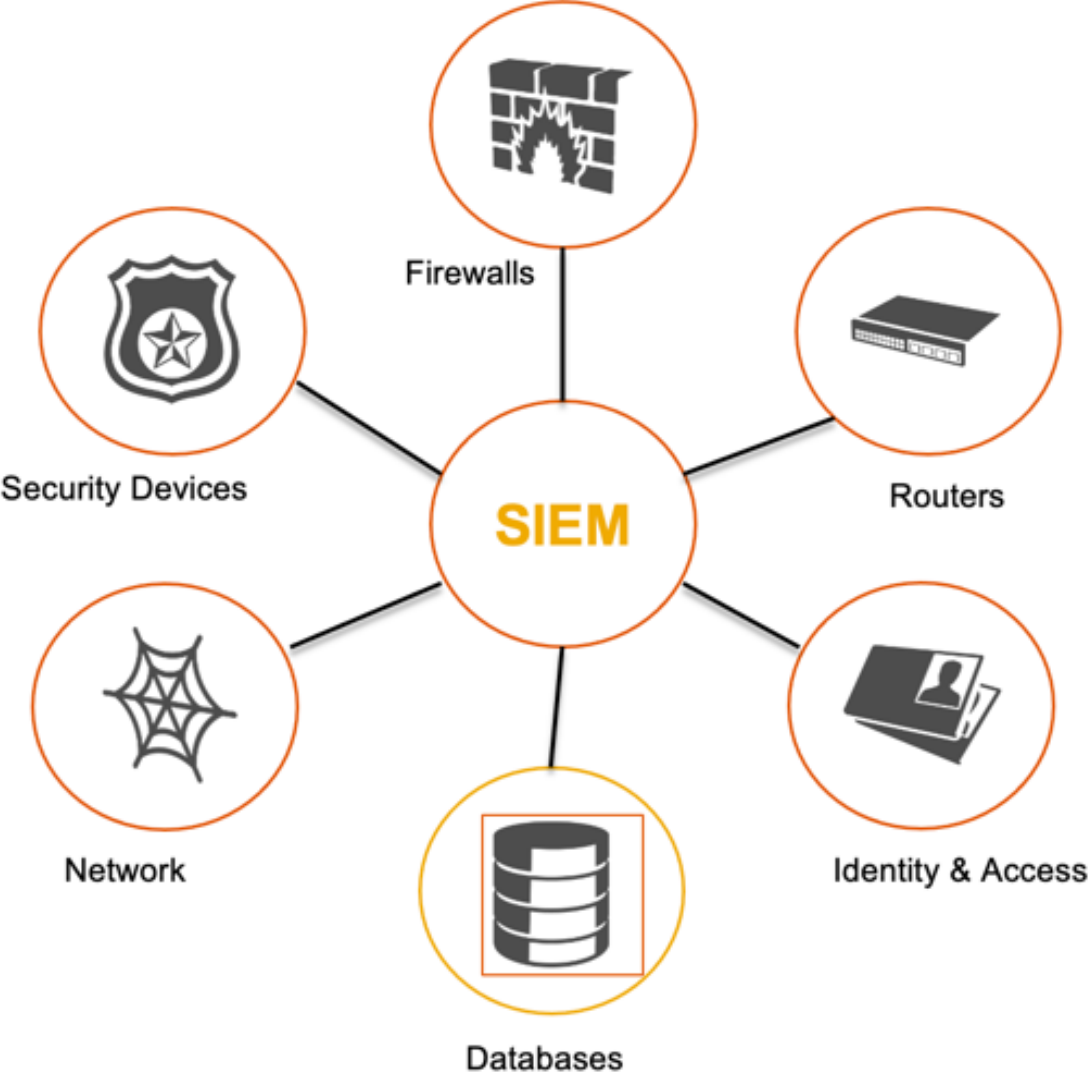
The screenshot shows the SAP Workload: Single Statistical Records - Overview interface. The table displays transaction statistics for system HE4, analyzed from 12.05.2022 / 00:59:00 to 12.05.2022 / 01:09:00. The display mode is set to 'All statistic records, sorted by time'.

Started	Server	Transaction	Program	T Scr.	Wp	User	Response time (ms)	Time in WPs (ms)	Wait time (ms)
		*	*	*		*	0		
23:59:42			DHCDOR_OBSERVE_LOGTAB	B	43		3.600.328	3.600.328	0
Start of									
00:51:33			ODQ_DAEMON	B	44		897.520	897.520	0
00:57:43			RFC	R	3004 16		90.855	90.855	0
00:58:05			RFC	R	3004 2		115.478	115.478	0
00:58:55			RFC	R	3004 21		13.301	10.947	3
00:58:57			RFC	R	3004 20		25.943	25.943	0
00:58:59			AutoABAP	A	1100 14		4.726	4.726	0
00:58:59			RFC	R	3004 7		1.599	107	0

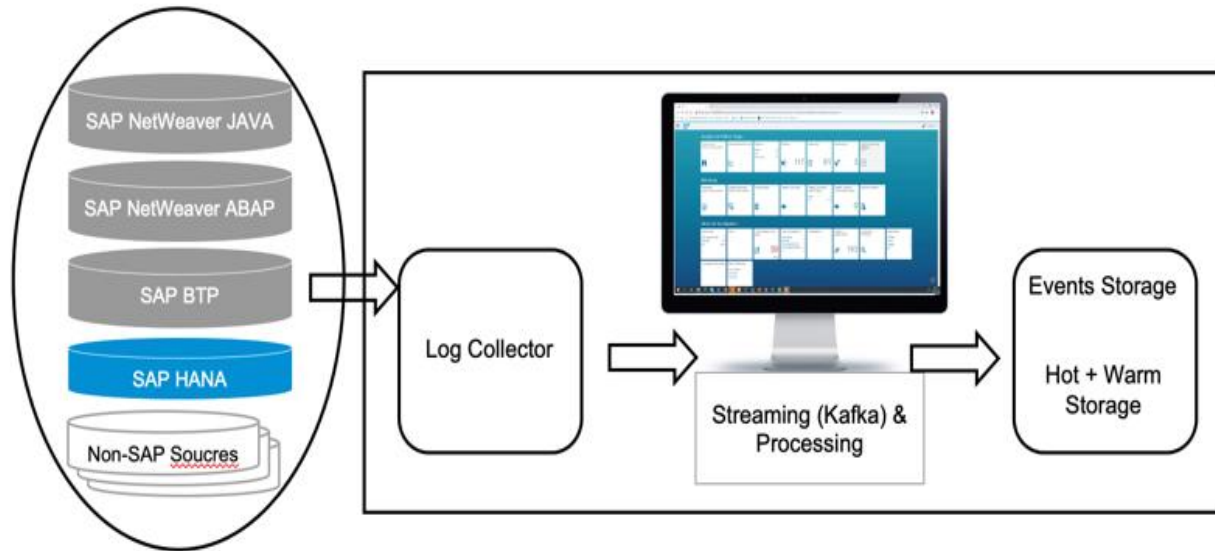
Use of BTL in investigation

In the event of an attack, BTL can provide information such as which RFC call was executed in a certain time period.

SAP Enterprise Threat Detection



SAP Enterprise Threat Detection



- The heart of the SAP Enterprise Threat Detection is to provide the ability to configure, analyze, and process log data or log events.
- You can define the baseline pattern, configure alerts, or investigate and create tickets.

Which logs are ingested from S/4HANA?

- System log
- Security audit log
- Business transaction log
- HTTP server log
- Gateway log
- User change log
- Change document log
- Read access log/UI log
- SOAP-based web services log
- HTTP access log
- Security log

SAP Data Custodian

- SAP Data Custodian provides two services:
 - Transparency and Control Service (TCS)
 - Key Management Service (KMS)
- Transparency and Control Service (TCS)
 - Identify any anomalies or misuse of the data through transparency
 - Protects the data through control by applying policies through the transparency and control service.

Transparency & Control Service

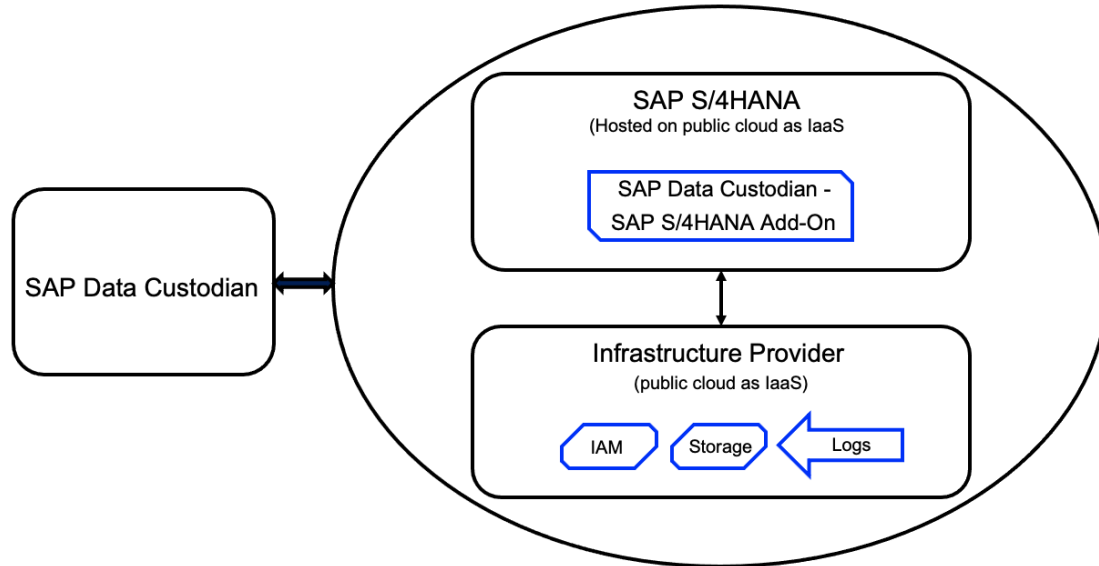
- Activity monitoring
- Policy definition
- Contextual access control
- Compliance management
- Data governance
- Audit reporting

Advance monitoring
&
complete control
over the
data and resources
in the cloud.

SAP Data Custodian

- Key Management Service

- key management service lets customers keep complete control over the encryption key
- Customers can manage the complete key life cycle and assign or revoke access as needed.
- The key can be accessed and managed through the user interface or using REST APIs.
- The key management service is available globally.

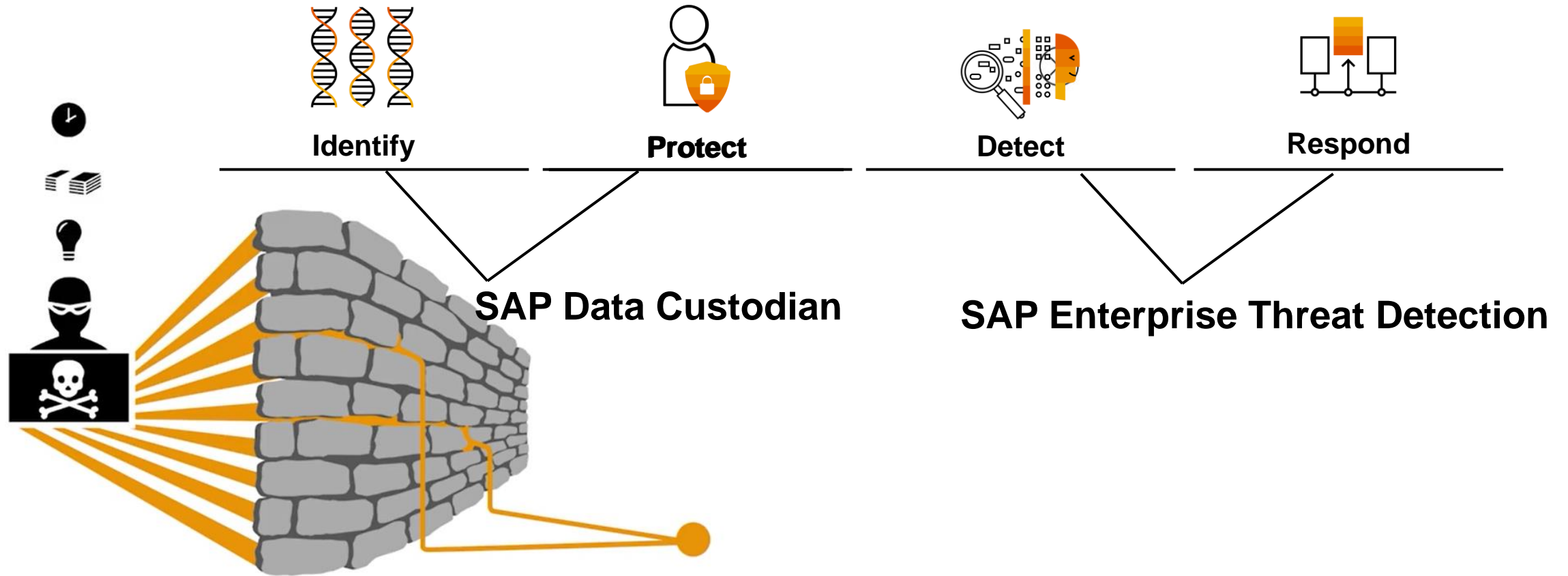


Key management service

Customers can generate keys or can bring their own key (BYOK) from their on-premise hardware security module (HSM) to encrypt data in public cloud, hybrid cloud, or on-premise environments.

SAP Data Custodian's key management service also offers an export feature that allows customers to export to key to encrypt their other resources.

NIST's Cybersecurity Risk Framework



NIST = National Institute of Standards & Technology

User Interface (UI) Data Protection Logging

- Logs data at the user interface
- Logs all data that is presented to the user as well as entered by the user
- Rich in features
 - Alerting
 - **Basic logging**
 - **Change logging**
 - **Conditional logging**
 - **Data transfer with adjustments**
 - **Log analyzer**
 - **Integration with SAP Enterprise Threat Detection**
 - **Pseudonymization**

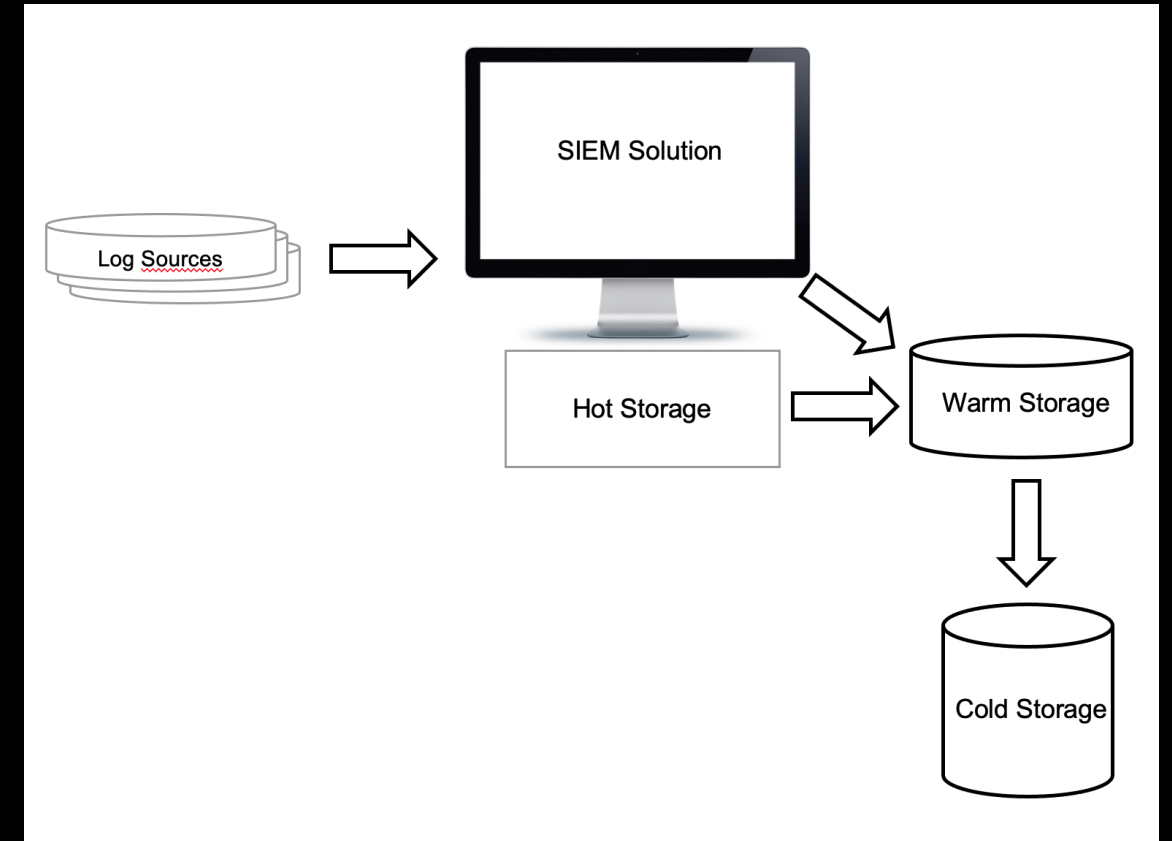
What UI data protection logging can do for you?

Offers very robust protection from insider threats

Although it does not prevent malicious users proactively, it definitely helps indirectly because users are less likely to commit wrongdoing if they know they are being watched.

Best Practices

- Blueprint
- Access Control
- Format
- Timestamp
- Storing, retaining & Deleting the logs




Resources

- [SAP Help Portal](#)
- [Whitepaper: Log Management Guide](#)
- [Logging for SAP S/4HANA Security – SAP Press](#)
- [SAP Trust Center](#)


Key Takeaways



Logs are very important to security -
helps detecting & investigating attacks



Centralized logging helps in
identifying & responding



Proper configuration, baseline & retention
are the key to successful logging

Thank you.

Contact information:

Sandip Dholakia
Sandip.dholakia@sap.com



Follow us



www.sap.com/contactsap

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/copyright for additional trademark information and notices.

