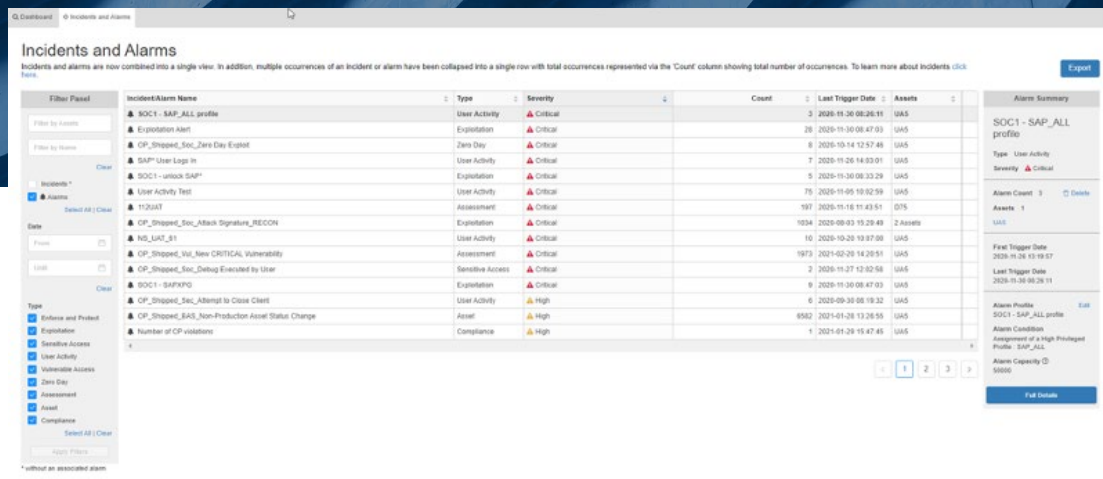


# ONAPSIS DEFEND

## Continuous Threat Detection and Response for Mission-Critical Applications



Incident/Alarm Name	Type	Severity	Count	Last Trigger Date	Assets
SOC1 - SAP_ALL profile	User Activity	Critical	3	2020-11-20 08:26:11	UAS
Exploitation Alert	Exploitation	Critical	26	2020-11-20 08:47:03	UAS
OP_Shipped_Soc_Zero Day Exploit	Zero Day	Critical	8	2020-10-14 12:57:46	UAS
SAP* User Login In	User Activity	Critical	7	2020-11-20 14:03:01	UAS
SOC1 - unlock SAP*	Exploitation	Critical	5	2020-11-20 08:33:29	UAS
User Activity Test	User Activity	Critical	75	2020-11-05 10:02:59	UAS
112UAT	Assessment	Critical	197	2020-11-18 11:43:51	075
OP_Shipped_Soc_Attack Signature_RECON	Exploitation	Critical	1034	2020-09-03 15:29:49	2 Assets
NO_UAT_S1	User Activity	Critical	10	2020-10-20 10:07:08	UAS
OP_Shipped_Vul_New CRITICAL Vulnerability	Assessment	Critical	1973	2021-02-26 14:29:51	UAS
OP_Shipped_Soc_Debug Executed by User	Sensitive Access	Critical	2	2020-11-27 12:02:58	UAS
SOC1 - SAPFPO	Exploitation	Critical	6	2020-11-20 08:47:03	UAS
OP_Shipped_Soc_Alternate to Close Client	User Activity	High	6	2020-09-28 08:19:32	UAS
OP_Shipped_Soc_Non-Production Asset Status Change	Asset	High	8582	2021-01-26 13:26:55	UAS
Number of CP violations	Compliance	High	1	2021-01-26 15:47:45	UAS

**Alarm Summary**

**SOC1 - SAP\_ALL profile**

Type: User Activity  
Severity: Critical

Alarm Count: 3 Details

Assets: 1

First Trigger Date: 2020-11-20 10:10:17

Last Trigger Date: 2020-11-20 08:26:11

Alarm Profile: SOC1 - SAP\_ALL profile

Alarm Condition: Engagement of a High Privileged Profile: SAP\_FPO

Alarm Capacity: 50000

Full Details

### Threat Detection And Response

Onapsis Defend enables real-time threat alerts so organizations can respond quickly to unauthorized changes, misuse, or cyberattacks targeting mission-critical applications hosted in cloud, hybrid and on-premises environments.

Defend helps organizations enable more effective threat monitoring and gives security teams unprecedented visibility into critical applications.

Onapsis Defend continuously monitors mission-critical applications hosted in cloud, hybrid and on-premises environments for internal and external threats, including changes, critical transactions and user activity that introduce risk, exploit a vulnerability or take the organization out of compliance. Intelligent, research-driven capabilities reduce and prioritize incidents so organizations can focus on actionable, probable events.

Real-time notifications and integrations with SIEMs allow Security Operations Center (SOC) and Incident Response Teams to respond quickly to active threats, determine root cause analysis and use Defend as a compensating control until the issue can be resolved.

## SUPPORTED SYSTEMS



ORACLE®

salesforce

### Onapsis Defend Provides Real-time Visibility and Threat Detection

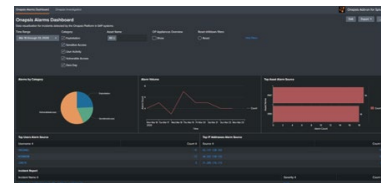
Automatically monitor for 3,000+ threat indicators, including:

- Inappropriate privilege escalation
- Authorization misuse and abuse (e.g., functions that would expose sensitive information, data downloads)
- System and interface misconfigurations
- Indicators of compromise or known exploits
- User activity and logins
- Dangerous RFC or program executions
- User Access misuse and abuse
- Create, customize and assign alarms for specific stakeholders to receive threat indicator alerts most relevant to their risk posture
- Custom alarms workflow enables notifications to be sent through the product, via email, or to a SIEM depending on existing workflows and the preferences of SOC and Incident Response teams
- Improve response capability with detailed alarm notifications that include in-depth threat intelligence, detailed explanation of business risk and, contextual attack notifications with success probabilities
- Enhance root cause analysis with integration to SIEMs, bringing mission-critical application threat information into the SOC so it can be correlated with other system logs

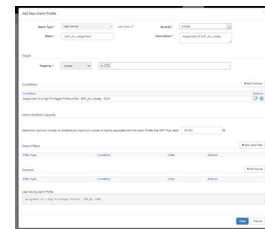
### Onapsis Defend In Action



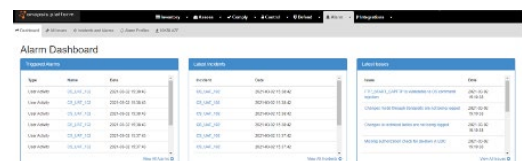
*Defend dashboard showcases latest threat indicators and incidents and alarms by category*



*Example of Defend SIEM integration: Onapsis Alarm Dashboard in Splunk shows alarms by category, over time, by asset, and more*



*Create custom alarms so you only receive alerts for threat activity relevant to your security posture*



Triggered Alarms			Latest Threat Indicators			Latest Issues		
Type	Name	Date	Type	Name	Date	Type	Name	Date
User Admin	10.1.1.1	2019-01-10 10:00:00	User Admin	10.1.1.1	2019-01-10 10:00:00	Issue	10.1.1.1	2019-01-10 10:00:00
User Admin	10.1.1.1	2019-01-10 10:00:00	User Admin	10.1.1.1	2019-01-10 10:00:00	Issue	10.1.1.1	2019-01-10 10:00:00
User Admin	10.1.1.1	2019-01-10 10:00:00	User Admin	10.1.1.1	2019-01-10 10:00:00	Issue	10.1.1.1	2019-01-10 10:00:00
User Admin	10.1.1.1	2019-01-10 10:00:00	User Admin	10.1.1.1	2019-01-10 10:00:00	Issue	10.1.1.1	2019-01-10 10:00:00
User Admin	10.1.1.1	2019-01-10 10:00:00	User Admin	10.1.1.1	2019-01-10 10:00:00	Issue	10.1.1.1	2019-01-10 10:00:00

*Alarm dashboard shows triggered alarms, latest threat indicators, and latest issues with the ability to click through for more details.*

**50%**

Reduced forensic time thanks to detailed alarm explanations and resolution guidance

**100%**

SAP log forwarding enables correlation with other system logs to provide context and help determine response strategy

**75%**

Improved incident times by integrating with SIEMs and having all information in one place

## Key Features of Onapsis Defend

- Out-of-the-box integrations with SIEMs (e.g., Splunk, QRadar, ArcSight, Exabeam, Sentinel) and generic connectors available (e.g., Syslog) give SOC teams visibility into threats against mission-critical applications and incorporate context into incident response processes
- Alarms and Investigation dashboards provide detailed information, such as root cause of the alarms and next steps to resolve the incident
- 3,000+ out-of-the-box threat indicators and 24 pre-configured alarms provide a base level of threat monitoring upon installation
- Incident workflow and alarm profiles ensure that the proper audience receives the correct notifications when incidents occur
- Defend is automatically updated to include the latest threats, including Zero-day issues from the Onapsis Research Labs



## Powered By The Onapsis Research Labs

The award-winning Onapsis Research Labs is a team of cybersecurity experts who combine in-depth knowledge and experience to deliver security insights and threat intel affecting mission-critical applications from SAP, Oracle, Salesforce and others. They have discovered over 800 zero-day vulnerabilities and multiple critical global CERT alerts have been based on their novel research.

Onapsis automatically updates its products with the latest threat intelligence and other security guidance from the Onapsis Research Labs. This provides customers with advanced notification on critical issues, comprehensive coverage, improved configurations and pre-patch protection ahead of scheduled vendor updates. The ongoing discoveries from the Onapsis Research Labs keeps the Onapsis Platform ahead of ever-evolving cybersecurity threats.

# THE ONAPSIS PLATFORM

Threat detection and response is just one component of protecting your mission-critical applications. Onapsis provides a suite of products, built on the Onapsis Platform, to support security, compliance, threat monitoring, secure application development, and change management.

## Assess

Identify vulnerabilities, understand risk, prioritize remediation

## Defend

Continuously monitor for threats and misuse; integrate with SIEMs

## Comply

Evaluate configurations and controls against policies;  
automate audit processes

## Control for Code

Scan custom code for security, compliance, and quality  
issues in real-time or before release

## Control for Transports

Inspect SAP transports to avoid import errors, outages,  
downgrades, security vulnerabilities, and compliance violations



## ABOUT ONAPSIS

Onapsis protects the business-critical applications that power the global economy including ERP, CRM, PLM, HCM, SCM and BI applications from SAP®, Oracle® and leading SaaS providers. Onapsis proudly serves more than 300 of the world's leading brands including 20% of the Fortune 100 and partners with leading consulting and audit firms such as Accenture, Deloitte, IBM, PwC and Verizon. The Onapsis Research Labs is responsible for the discovery and mitigation of more than 800 zero-day business-critical application vulnerabilities. For more information, visit [www.onapsis.com](http://www.onapsis.com).