ONAPSIS

Onapsis Defend

Threat Detection and Response for Business-Critical Applications

Continuously Monitor and Protect Your Most Important Assets from Threats

The Challenge

Your Window to Defend Your Business-Critical Applications Is Shrinking

Digital transformation initiatives have left business-critical applications more exposed than ever, and this increased exposure hasn't gone unnoticed. Threat actors are targeting business-critical applications through a variety of attack vectors and at a faster pace than ever before.

Attempting to monitor for threat activity by manually reviewing system logs is inefficient and requires extensive internal knowledge. Given the speed at which threat actors operate, this leaves far too much time for successful attacks to take place. To protect their critical business operations and data, organizations need continuous threat monitoring designed specifically for these applications. They need to identify potential threats in real-time and understand the risk they pose, so they can prioritize incident response.

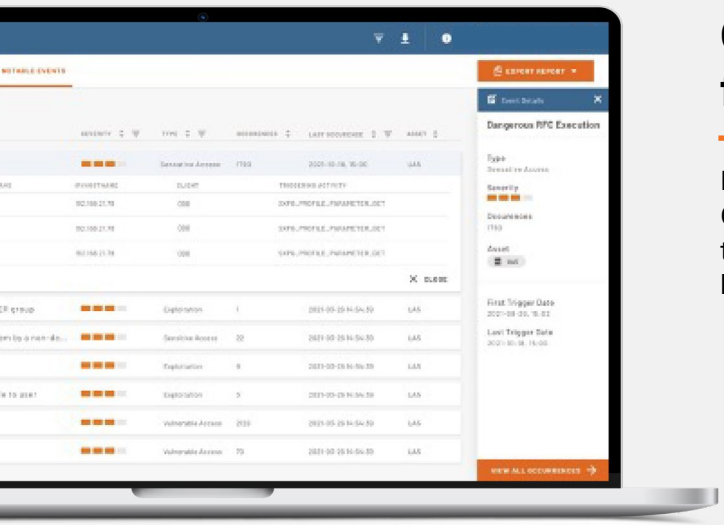
<3 hours

for the first exploit attempt on an unprotected system coming online[1]

<72 hours

between release of a patch and first exploit attempts[1]

[1] SAP and Onapsis Threat Report



The Solution

Continuous Threat Monitoring for SAP with Onapsis Defend

Powered by research and insights from the Onapsis Research Labs, Onapsis Defend uniquely provides the visibility and context security teams need to respond faster and smarter to threats targeting their business-critical applications.

- Over 2,000 detection rules specific for SAP, including zero days to protect applications from threats prior to patch release
- Understand root cause and how to mitigate
- Integrate with SIEMs for SOC visibility and cross-system analysis
- Get the latest threat intelligence from Onapsis Research Labs

Understand Threats to Your Critical Systems

Automatically Detect
Eliminate the need for manual log reviews and in-house SAP security expertise to identify threats

Start Monitoring Immediately
2,000+ detection rules and 24 pre-configured alarms provide a base level of threat monitoring upon install

Correlate with Other Systems
Pull SAP threat information into SIEMs for cross-system correlation and enhanced root cause analysis

> ***We're saving 20 hours a week compared to manual log reviews***
>
> *– F500 Financial Institution*

> ***We're saving 20 hours of week addressing security controls around user access***
>
> *— F500 Consumer Good Company*

Respond Faster and Smarter

Reduce Investigation Time
Receive real-time alerts with detailed explanations, including root cause, severity, and business context

Accelerate Incident Response
Incident workflows and SIEM integrations ensure timely notifications and reduce time to resolution

Gain Prioritization Capabilities
Understand where to focus efforts and don't waste time on activity that doesn't pose a risk

Reduce Risk to Critical Systems

Shrink Exposure Window
Preemptively protect applications before patches are released (zero day vulnerabilities) or have been applied

Get the Latest Threat Intel
Receive the latest vulnerability and threat research, including zero-day issues, from Onapsis Research Labs

Implement Compensating Controls
Monitor for potential exploit activity until the appropriate patch or fix can be applied

> ***We're confident our most important assets are protected from zero-days and other emerging threats***
>
> *— F500 Chemical Company*