JOINT SOLUTION REPORT

Palo Alto Networks and Radiflow

The Challenge

The growing digitization in industrial automation applications has introduced critical cybersecurity threats into traditional industrial applications, including targeted attacks on OT devices and processes as well as IT attacks that span into OT networks. These risks are apply especially to distributed SCADA networks that span multiple remote sites, where an attack can result in catastrophic disruption of national infrastructure services.

Radiflow iSID

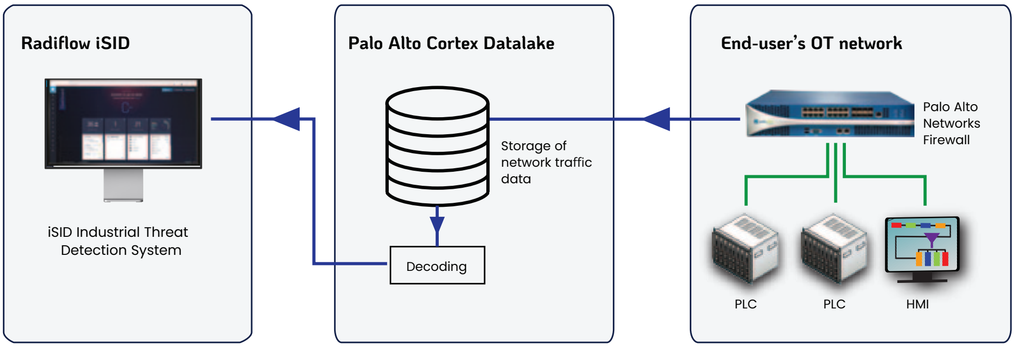
Radiflow iSID is a threat detection system for ICS/SCADA networks. It enables monitoring of industrial networks by mapping the IT and OT assets, and then providing situational awareness as well as real-time alerts on any behavioral anomalies.

iSID uses multiple security engines in parallel, each applying to a different OT operational aspect. These engines detect potential anomalies, such as changes in network topology in the session used between devices, use of known exploits, deviations from predefined DPI policies for M2M sessions and changes in PLC configurations.

Palo Alto Networks Cortex

Palo Alto Networks'® Cortex prevents successful cyberattacks through intelligent automation. Cortex combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection and prevent cyber breaches.

Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks and mobile devices, natively providing the right capabilities at the right place across all stages of the attack lifecycle.


Radiflow iSID
iSID Industrial Threat Detection System
Palo Alto Cortex Datalake
Storage of network traffic data
Decoding
End-user's OT network
Palo Alto Networks Firewall
PLC
PLC
HMI

Basic elements and workflow of the combined solution

ISID-PA For Palo Alto Networks Application Framework

iSID-PA is an industrial threat detection app for the Palo Alto Networks' Cortex Framework. The use of Cortex Framework apps enables organizations to quickly deploy new security capabilities without needing to provision additional hardware or software.

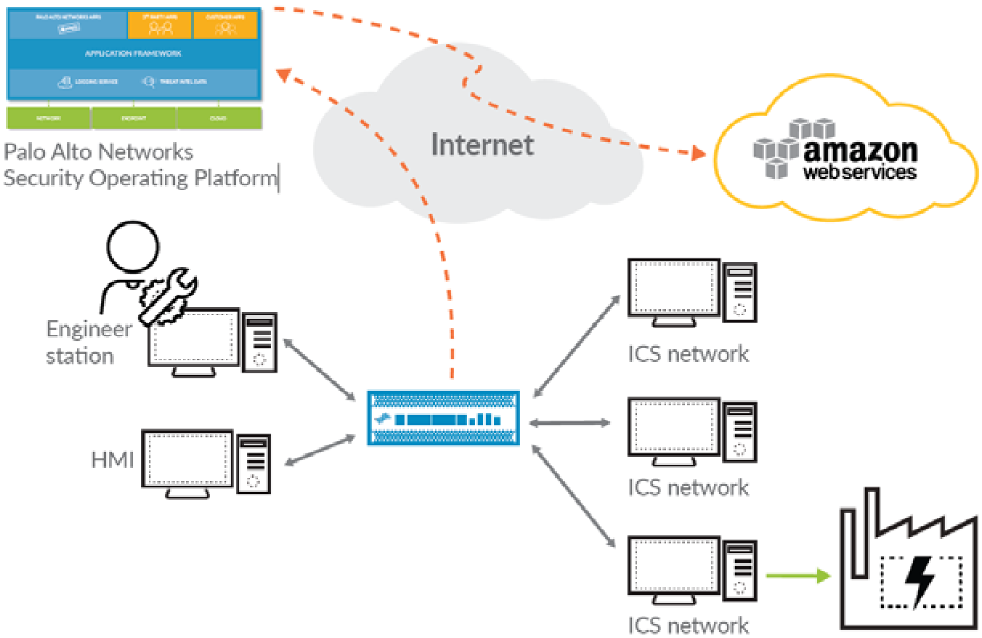
The Cortex Framework also offers a suite of APIs that developers can use to connect innovative apps with rich data, threat intelligence and enforcement points. In this way, organizations can gain immediate security value from apps developed by an open ecosystem of trusted innovators.

USE CASE NO. 1

Challenge: Logic change in industrial controllers is inadequately protected.
Solution: Monitor maintenance sessions on each controller and validate each change process.
Benefit: Radiflow iSID understands the maintenance protocols of the industrial controllers. It monitors and raises alerts on suspicious operations, in addition to validating the content of any firmware or logic change.

USE CASE NO. 2

Challenge: No up-to-date inventory information for industrial assets and their vulnerabilities.
Solution: Radiflow iSID monitors the operational parameters published by each controller and compares them to known vulnerabilities.
Benefit: Up-to-date, accurate OT asset inventory, with complete properties for each asset.



iSID monitoring an ICS network via the Application Framework

About Radiflow

Radiflow is an OT Cyber Security company that develops unique tools to secure digital assets for the long term. The company works directly with Managed Security Service Providers to overseethe discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its' field-proven solutions are installed in over 6000 sites around the globe.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers.
Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of changemakers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices. Find out more at www.paloaltonetworks.com.

Radiflow | For more info: **radiflow.com**