# Rapid7 InsightIDR Brings User Context to Palo Alto Networks WildFire™ Alerts

Integration Brief

## INTEGRATION BENEFITS

- Add user context to Palo Alto Networks alerts
- Facilitate investigations into advanced malware alerts
- Seamless integration through a lightweight collector

## Solution Overview

Advanced attacks are not point in time events. Adversaries deliver attacks persistently, often using non-standard ports, protocols, or encryption for subsequent attack stages. There are only a few times when the attacker is at a disadvantage: when they first land on and scan the network, when they phish users, and when they look to laterally move between accounts.

Monitoring solutions report findings by IP address, making it difficult to investigate, assess impact, and build a timeline of events. Understanding the user context of the alert is critical to respond with confidence.

This combined solution allows your IT teams to map findings from Palo Alto Networks WildFire to the user context provided by Rapid7 InsightIDR. This provides coverage to your entire ecosystem, even as users are assigned changing IP addresses, use various on premise and cloud service accounts, and access e-mail on mobile devices.

## Palo Alto Networks WildFire

WildFire simplifies an organization's response to the most dangerous threats—automatically detecting unknown malware and quickly preventing threats before organizations are compromised. Unlike legacy security solutions, WildFire quickly identifies and stops these advanced attacks without requiring manual human intervention or costly Incidence Response (IR) services after the fact.

## Rapid7 InsightIDR

Rapid7 InsightIDR is an intruder analytics solution that gives you the confidence to detect and investigate security incidents faster. Only InsightIDR gives you quality alerts without the noise, enables your entire team to investigate an incident, and adds user context to your monitoring solutions. Unlike other solutions, InsightIDR monitors activity not just on your network, but across endpoints, mobile devices and the cloud, and it gives you instant visibility into user activity across your infrastructure and monitoring solutions. Rapid7's unique understanding of attacker methodologies is the key for producing these highly accurate analytics.

# “74% of security professionals claim incident investigation solutions lack integration with existing security products.”

- Ponemon Institute, 2014 Industry Report

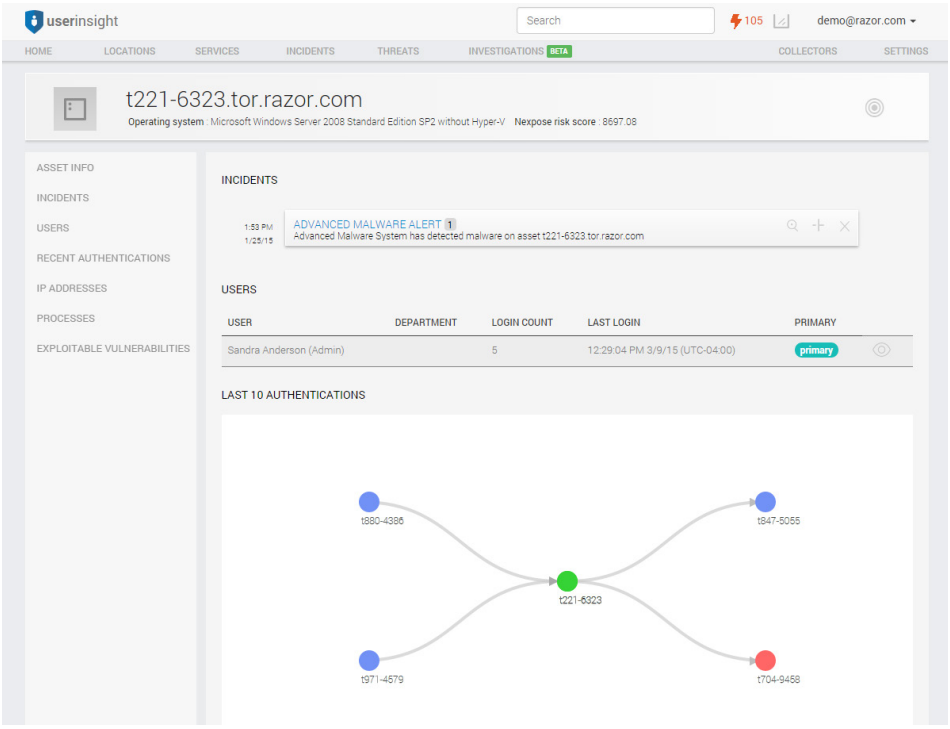


Figure 1: A user-attributed alert using combined information from InsightIDR and Palo Alto Networks WildFire

## HOW IT WORKS

Once you have set up Palo Alto WildFire and Rapid7 InsightIDR, take the following steps:

1. Configure the InsightIDR collector to consume data from WildFire.

2. Data is automatically imported into InsightIDR to enable investigations in the user context.

3. InsightIDR provides detection of compromised credentials in addition to the malware alerts provided by WildFire, giving you complete incident detection.

## WHAT YOU NEED:

- Rapid7 InsightIDR
- Palo Alto Networks WildFire

## SUPPORT

Please contact Rapid7 for support or assistance at +866.380.8113 or support@rapid7.com

## About Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today’s dynamic computing environments: applications, users, and content. Find out more at www.paloaltonetworks.com.

## About Rapid7

Rapid7’s IT security data and analytics software and services help organizations reduce the risk of a breach, detect and respond to attacks, and build effective IT security programs. With comprehensive real-time data collection, advanced correlation, and unique insight into attacker techniques, Rapid7 strengthens an enterprise’s ability to defend against everything from opportunistic drive-by attacks to advanced threats. Unlike traditional vulnerability management and incident detection technologies, Rapid7 provides visibility, monitoring, and insight across assets and users from the endpoint to the cloud. To learn more about Rapid7, visit www.rapid7.com.