RAPID7 + okta

INTEGRATION BRIEF

Manage and Monitor User Identities

With Okta and Rapid7 InsightIDR

Solution Overview

Sixty-six percent of employees report they can still access corporate data on cloud services after leaving the corporation.[1] If that is a problem, what about stealthy attacks using compromised credentials? With the security perimeter now at the individual user and extending far beyond the corporate network, Okta's Identity Management and Rapid7's InsightIDR combine to provide coverage for your entire network ecosystem, from the endpoint to the cloud.

This integration allows security analysts to provision simple, secure access to cloud applications and monitor user activity for low-noise, high-value alerts on stealthy intruder attacks. This includes the top two attack vectors behind breaches: stolen credentials and malware.

Okta Identity Management

Okta's Identity Management is a class leading SaaS solution which helps enterprises enable their workforce to adopt the cloud. It integrates with the hundreds of cloud applications you use today, saving time and adding security for both IT and your end-users. This is done through easy account provisioning through Active Directory (AD), a seamless Single Sign On (SSO) experience, and secure Two Factor Authentication (2FA).

Rapid7 InsightIDR

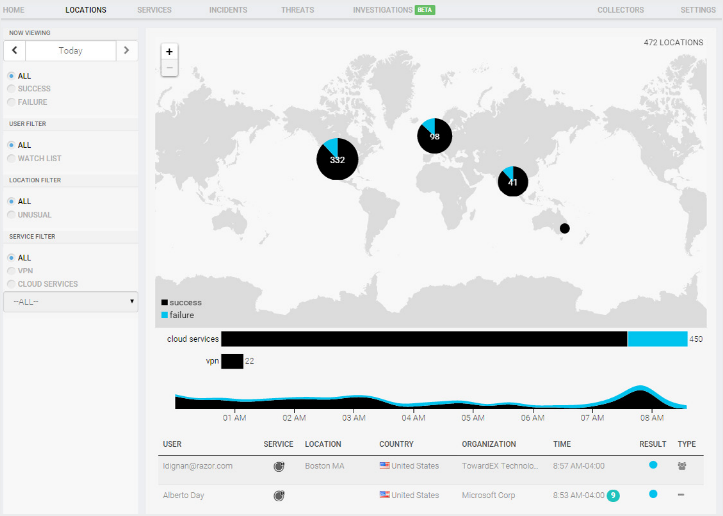
Rapid7 InsightIDR is an intruder analytics solution that gives you the confidence to detect and investigate security incidents faster. Only InsightIDR gives you quality alerts without the noise, enables your entire team to investigate an incident, and adds user context to your monitoring solutions. Unlike other solutions, InsightIDR monitors activity not just on your network, but across endpoints, mobile devices, and the cloud. InsightIDR 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.

Integration Benefits

1. Complete visibility into your users' authentication activity, inside and outside the network perimeter
2. Detect the attacks you're missing across the entire network ecosystem, from the endpoint to the cloud
3. Intelligent Single Sign On (SSO) and Two-Factor Authentication (2FA)
4. Automatically detect compromised credentials, the number one attack vector
5. Monitor Okta Administrator authentications and activity

[1] http://mobileenterprise.edgl.com/news/Employees-Go-Rogue-with-Data97211

Bring Confidence Into Your Cloud Architecture



NOW VIEWING
Today
● ALL
○ SUCCESS
○ FAILURE

USER FILTER
● ALL
○ WATCH LIST

LOCATION FILTER
● ALL
○ UNUSUAL

SERVICE FILTER
● ALL
○ VPN
○ CLOUD SERVICES
--ALL--

USER	SERVICE	LOCATION	COUNTRY	ORGANIZATION	TIME	RESULT	TYPE
ldignan@razor.com		Boston MA	United States	TowardEX Technolo...	8:57 AM-04:00	●	
Alberto Day			United States	Microsoft Corp	8:53 AM-04:00 9	●	—

Figure 1: Visualize your organization’s cloud authentications

How It Works

Rapid7 InsightIDR uses Okta’s direct API to ingest the authentication data for users across the organization. These logs are analyzed and combined with network, endpoint, mobile, and attacker methodology to detect intruders and risky internal behavior. Incident alerts are automatically generated in InsightIDR.

1. Set up Rapid7 InsightIDR
2. Forward Okta logs to InsightIDR’s collector

What You Need

Rapid7 InsightIDR	Okta Identity Management

About Okta

Okta is an integrated identity and mobility management service. Built from the ground up in the cloud, Okta securely and simply connects people to their applications from any device, anywhere, at anytime. Okta integrates with existing directories and identity systems, as well as thousands of on-premises, cloud and mobile applications, and runs on a secure, reliable and extensively audited cloud-based platform.

About Rapid7

Rapid7 is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. 7,400 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations.

Support

Please contact Rapid7 for support or assistance at +1.866.380.8113, or through our Customer Portal.

Customer Portal