RAPID7 **okta**

Manage and Monitor User Identities

With Okta and Rapid7 InsightIDR

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

- Complete visibility into your users' authentication activity, inside and outside the network perimeter

- Detect the attacks you're missing across the entire network ecosystem, from the endpoint to the cloud

- Intelligent Single Sign On (SSO) and Two-Factor Authentication (2FA)

- Automatically detect compromised credentials, the number one attack vector

- Monitor Okta Administrator authentications and activity

[1] http://mobileenterprise.edgl.com/news/Employees-Go-Rogue-with-Data97211
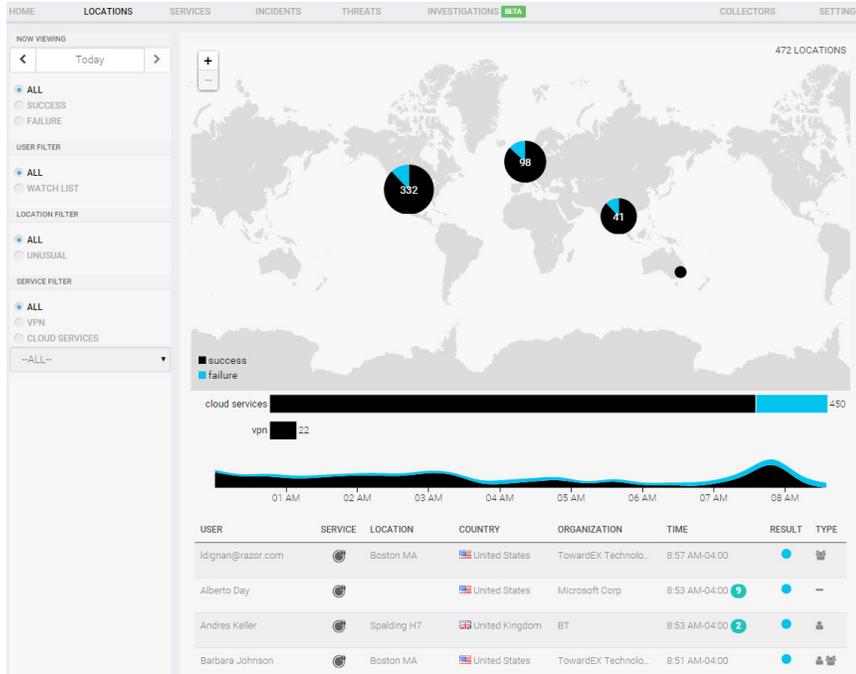
Bring Confidence Into Your Cloud Architecture

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.

- Step 1: Set up Rapid7 InsightIDR
- Step 2: Forward Okta logs to InsightIDR's collector

What You Need

- Rapid7 InsightIDR
- Okta Identity Management

SUPPORT

Please contact Rapid7 for support or assistance at +1.866.380.8113 or support@rapid7.com

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 a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cybersecurity. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks.

To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.