RAPID7

SIEM USE CASE

Rapid7 InsightIDR

The SIEM You Always Wanted, Incident Detection You'll Always Need

Two decades ago, SIEMs were born from the need to manage and analyze all of the rich data being generated by security programs. However, intelligently correlating this data to detect compromises and risky behavior has long been an afterthought. Is your security team trapped under a mountain of vague alerts? You're not alone. From shadowing and collaborating with security teams, we were guided to create the UBA-powered SIEM you always wanted—or would have built yourself, if you weren't spending so much time weeding out false positives—InsightIDR.

Why InsightIDR is the SIEM you always wanted

InsightIDR is purpose-built for Incident Detection & Response (IDR) and is equipped with live log search and custom compliance cards. Turn a week's worth of legwork into an hour: By integrating with your existing network and security stack, InsightIDR reliably detects compromise as it occurs, accelerating investigations. No more prolonged deployments, consulting, and support—you can get visibility from endpoint to cloud and meet SIEM requirements without it becoming a second full-time job.

Unify your data

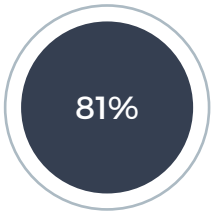
- Centralize, search, and visualize all of your logs—no data degree required.
- Track authentication for all users across assets and services, including cloud.

Intelligent incident detection

- Pre-built detections alert you of intruder presence at each step of the attack chain.
- Deception technology is included to expose attacker behaviors that never appear in log data.

Prioritize your search

- Automatically identify risky users and misconfigurations after adding in data sources.
- Build compliance dashboards that meaningfully highlight company risks and progress.



81% hacking-related breaches leveraged stolen and/or weak passwords.

- 2017 Verizon Data Breach Investigations Report

83% of compromises take weeks or longer to discover.

- 2016 Verizon Data Breach Investigations Report

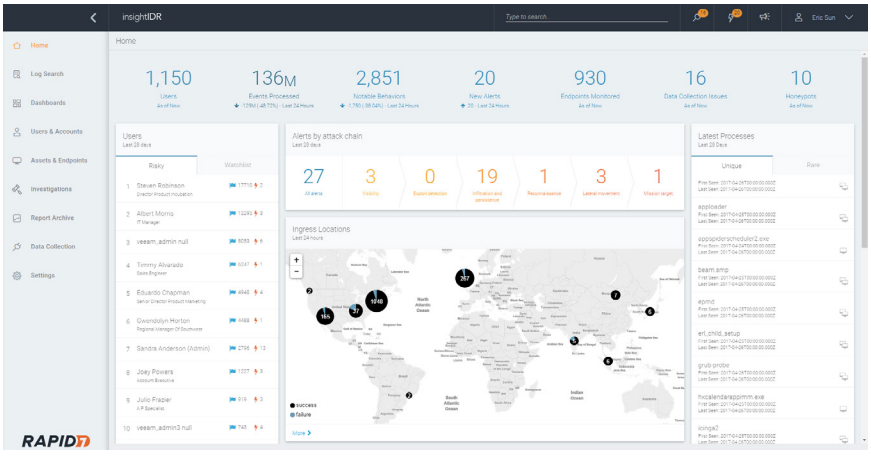
How InsightIDR arms you with the insight to detect attacks earlier

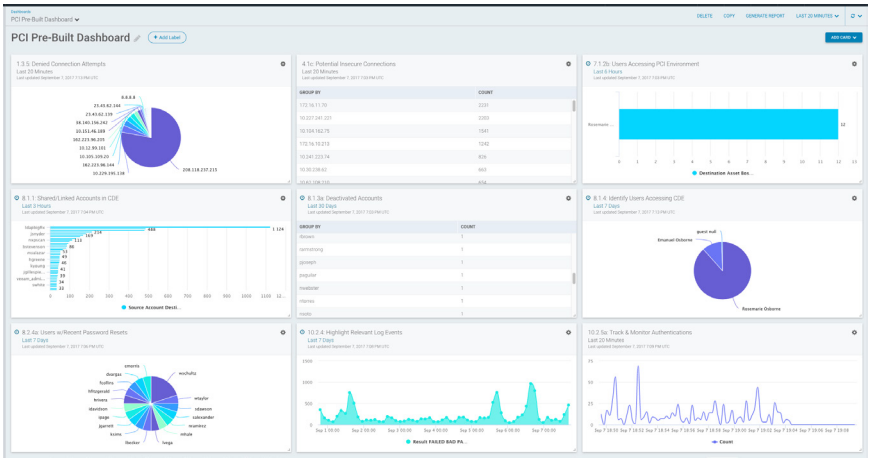
At Rapid7, we obsessively focus on detecting and stopping intruders anywhere they go in your ecosystem. Our team's extensive knowledge and exploration of attacker methodology allows us to go beyond analyzing log data to reliably detect intruders earlier in the attack chain.

How can InsightIDR disrupt an attack?

INFILTRATION & PERSISTENCE	EXPLORE NETWORK	LATERAL MOVEMENT	MISSION TARGET	MAINTAIN PRESENCE
DETECT PHISHING ATTEMPTS DETECT MALWARE AND UNIQUE PROCESSES ALERT ON LEAKED CREDENTIALS MONITOR INBOUND CONNECTIONS	DETECT NETWORK SCANS DETECT PASSWORD GUESSING ATTEMPTS	IDENTIFY COMPROMISED CREDENTIALS ACROSS LOCAL/ DOMAIN/CLOUD ACCOUNTS IDENTIFY PRIVILEGE ESCALATIONS DETECT PASS THE HASH ATTACKS	DETECT SUSPICIOUS ACCESS TO CRITICAL DATA MONITOR DATA TRAFFIC AND CLOUD USAGE	DETECT MALWARE AND UNIQUE PROCESSES

Above: InsightIDR brings together asset, user, and behavioral data into a single view.
Below: Meet your compliance needs with real-time reporting, flexible search, and user behavior analytics.





MANAGED DETECTION AND RESPONSE (MDR) SERVICES

Rapid7 Managed Detection and Response is an extension of your security team and combines our InsightIDR technology and proprietary tools with real-time threat intelligence and world-class analysts to monitor your network 24/7, 365.

Our team proactively hunts for known and unknown threats—even our most junior analysts have responded to hundreds of threats. If a threat is discovered, the team will shift to incident response and guide remediation efforts. The result: Rapid7's team of cyber guardians augmenting your people, process, and technology, from detection to response.

INCIDENT RESPONSE SERVICES

Has your network been compromised? Our Incident Response team is available for immediate assistance: 1-844-RAPID-IR

IR Program Development, Tabletop Exercises (TTX), Breach Readiness Assessments, and flexible retainer agreements are available for your needs. Learn more below: www.rapid7.com/IR-services

Why we're different: The Rapid7 Approach

Traditional Approach	InsightIDR Approach	Details
Expanding hardware deployment	Cloud-based architecture	Our secure, multi-tenant cloud architecture means you spend less time managing your security data and more time benefiting from blazing fast search, constantly updated detections, and reassurance that your log data is out of attackers' hands.
Alert fatigue	An average of 10-15 alerts daily	More than 60% of organizations get more alerts than they can feasibly investigate.[1] InsightIDR doesn't alert on every anomaly; each alert comes with meaningful context and highlights network happenings you want to know about.
Rule-based detection	Deception technology	Not all signs of an intruder are found in log files. With InsightIDR, you'll detect stealthy attacker behaviors with our purpose-built traps: honeypots, honey users, honeyfiles, and honey credentials.
Events-per-second pricing	Asset-based pricing	As your company expands, your log and machine data also balloons. Avoid data overage surprises with our simple, clean asset-based pricing model.
Sluggish time to value	Cloud-deployed detections, pre-built analytics	SIEM deployments take months, then specialized expertise and time must be spent to test and tune detection rules. With our pre-built analytics, you'll reliably detect the top attack vectors behind breaches—no data degree required.
Strict correlation rules	User behavior analytics core	In 2017, 81% of confirmed breaches involved the misuse of stolen or weak credentials.[2] Armed with our visionary user behavior analytics (UBA), you'll detect the use of stolen credentials and expose misconfigurations across your environment.
On-premise endpoint visibility	Choice of Insight Agent and endpoint scans	Securing your endpoints can be a challenge, especially for remote workers off of the corporate network. InsightIDR arms you with visibility, detection, and the ability to proactively hunt for answers. Both the Insight Agent and endpoint scans alert you of malware, local lateral movement, and even custom rules, like "Has anyone stuck a USB key in me?" Unlike EDR tools, we'll also identify malicious behavior around embedded devices, such as printers and routers.
Limited visibility into cloud services	Direct API integrations with leading cloud service providers	50% of ex-employees still have access to corporate applications.[3] Through integrations with Office 365, Google Apps, Salesforce, and more, you'll be notified of unusual authentications across local, domain, and cloud accounts.
Alert validation	Full network context	Spending too much time weeding through false positive alerts? By integrating with your existing network and security stack, including endpoint and cloud services, you slash investigation times by getting the full context for every alert.
Lengthy, tedious investigations	Automatic event-to-user attribution	Retracing your users' activity between IPs, assets, and services is tedious. InsightIDR takes the millions of events your company generates every day, highlights notable behavior, and attributes these events directly to the users and assets involved.

STAY READY, AND STAY SECURE

Get started for free with InsightIDR—no strings attached: www.rapid7.com/try-InsightIDR

GOT QUESTIONS?

Learn more about our Incident Detection & Response solutions: www.rapid7.com/solutions/incident-detection-and-response

[1] 2015 Rapid7 Incident Detection & Response Survey

[2] 2017 Verizon Data Breach Investigations Report

[3] 2017 OneLogin IT Survey