InsightIDR User and Entity Behavior Analytics (UEBA)

Detect and Eliminate Stealthy Unknown and Insider Threats

InsightIDR—Rapid7's cloud-native SIEM and XDR—delivers highly efficient, accelerated detection and response. With built-in User and Entity Behavior Analytics (UEBA), InsightIDR has developed rich, finely tuned analytics and machine learning to quickly understand the baselines of your unique environment and alert you to risky behavior. Teams work smarter and faster with InsightIDR's frictionless SaaS deployment experience, hyper-intuitive interface, robust out-of-the-box detections, and actionable automation.

A UEBA solution is a critical component of a multi layered, integrated IT and information security strategy to prevent attacks and investigate threats. InsightIDR's UEBA is an incredibly powerful tool to provide visibility into user activity, mitigate risks, and stop threats beyond what is flagged by traditional perimeter monitoring tools.

Key SOC challenges:

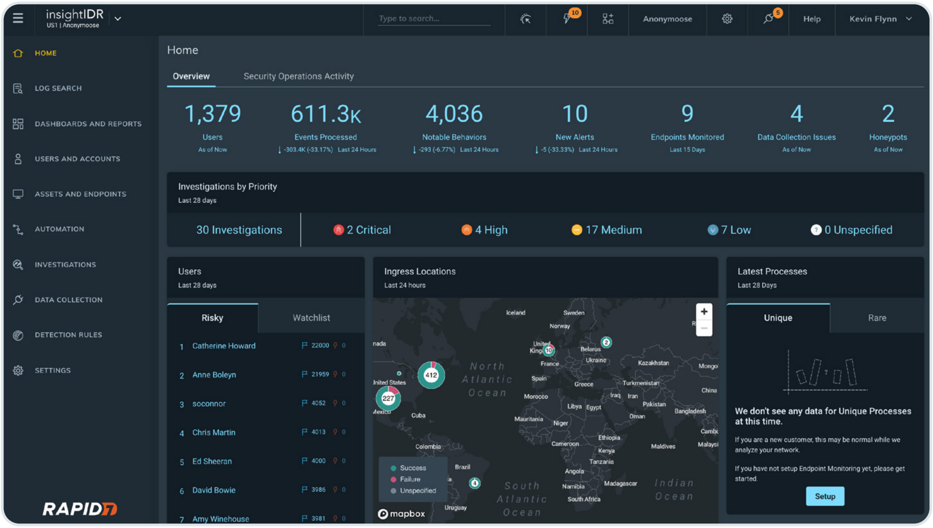
- **Limited visibility into user behaviors** makes it difficult to detect and stop insider threats before they make an impact.
- **Unactionable alerts and false positives** create tedious and time-consuming manual work for time-strapped security professional.
- **Labor-intensive investigation processes** are required to retrace user activity across accounts, assets, and cloud services.

Earlier, more reliable threat detection and response UEBA from InsightIDR

Unmatched visibility of your environment with continuous monitoring of users and credentials

InsightIDR continuously baselines healthy user activity in your organization, quickly catching anomalies and distinguishing between real threats vs. outliers. InsightIDR establishes this baseline within two weeks of deployment–driving immediate insights and value out of the gate. By creating a baseline for each user, device, application, privileged account, and shared service account, InsightIDR provides near real-time alerts as soon as it detects a deviation from the norm.

To visualize your user data, you don't have to go further than the InsightIDR homepage. There you will find prebuilt dashboards with relevant, contextual insights around ingress activity, risky users, and notable behaviors. InsightIDR automatically ranks risky users based on notable behaviors over the last 28 days. This, combined with customers' own watch list users, mean those most vulnerable to attack are monitored more closely and have adjusted thresholds for alerting to identify threats earlier in the kill chain.



1 Catherine Howard 22000 0
2 Anne Boleyn 21959 0
3 soconnor 4052 0
4 Chris Martin 4013 0
5 Ed Sheeran 4000 0
6 David Bowie 3986 0
7 Amy Winehouse 3981 0

We don't see any data for Unique Processes at this time.

If you are a new customer, this may be normal while we analyze your network.

If you have not setup Endpoint Monitoring yet, please get started.

User visibility extends into log search and investigations as well. The InsightIDR Attribution Engine tracks users and assets as they move around a network, auto-enriching every log line with user and asset details for stronger correlation and more complete visibility. All investigations detail impacted user and asset details as well. Analysts save time not having to piece together this story themselves and instead have this rich detail at their fingertips to make informed decisions immediately.

> **InsightIDR saves time when time is crucial. Once notified of a threat, it is easy to track down movement and quickly create a ticket for my team so they can immediately remediate the issue.**
>
> Gartner Peer Insights Review

Expertly-vetted detections ensure highly relevant and actionable alerts - not false positives

InsightIDR UEBA identifies anomalous, risky, and malicious behaviors that may stem from unintentional negligence or real insider threats. These are the stealthy, unknown threats that can often be hard to anticipate or defend against. Oftentimes, UEBA products will be configured too simply - creating noisy alerts that are impossible to manage. Every UEBA detection within InsightIDR is created leveraging insights and intelligence from our open source community research projects and our MDR SOC to ensure analysts receive only relevant, actionable alerts - not an overwhelming amount of false positives.

InsightIDR UEBA Detections

Specific behaviors foreshadow every breach — and we know them reliably.

Detect Insider Threats	Detect Unknown Threats
• Data Exfiltration Attempts • Policy Violations • Endpoint Monitoring • Unauthorized Data Access	• Brute-Force Attack • Compromised Credentials • DDoS • Detection Evasion

Protect your most sensitive data and intelligence

Your organization's intellectual property and proprietary information are critical to secure - making it a prime target for advanced attackers. The UEBA engine leverages data from across foundational event sources, Active Directory, the Insight Agent, and the Insight Network Sensor to provide a complete picture of all user activity and identify these more advanced threats. For example, with the native Network Sensor, access additional Anomalous Data Transfer (ADT) detections that alert you to data exfiltration attempts to detect transfer activity and identify large or unusual data moving outside your network.

Triage and investigate faster with correlated user data and built-in automation

Every alert in InsightIDR generates a high context investigation and correlated timeline of all relevant events and evidence. All alerts come with a detailed recommended response action - vetted by the Rapid7 MDR SOC to help analysts at any level respond like an expert.

From the investigations panel, analysts can leverage prebuilt automation workflows to respond to threats with just a couple of clicks. Automatically contain threats on an endpoint or suspend user accounts to address threats faster - before attackers have an opportunity to carry out their plans or move laterally across the network.

> “
> **Rapid7 InsightIDR has been a wonderful tool that gives us insight into our user behaviors, as well as clearly alerting us to potential threats that exist in our network. Our team has become more efficient with fewer false positives and improved investigation times.**
>
> Josh Petrucka, Security Analyst, Conexus Credit Union via Techvalidate

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: **https://www.rapid7.com/try/insight/**