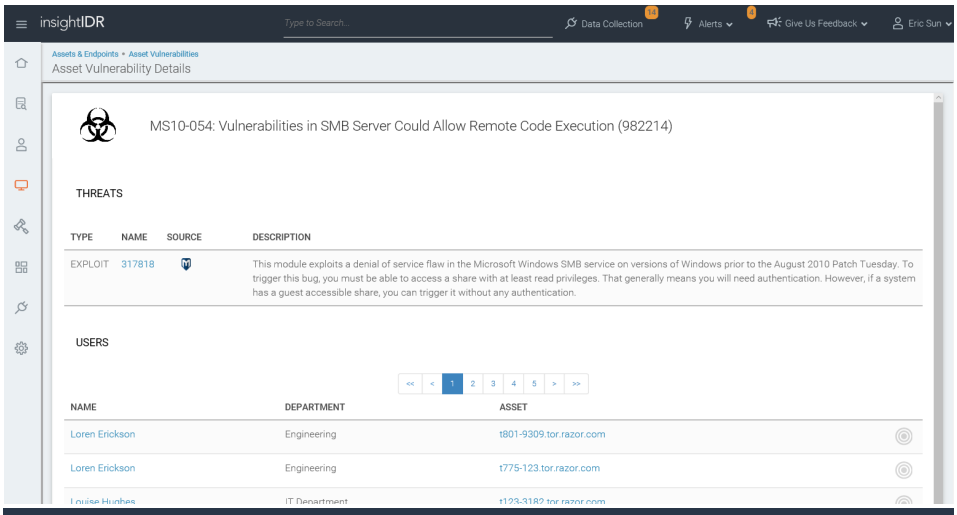
SOLUTION BRIEF

InsightIDR and Nexpose
Integrate for Total User and Asset Security Visibility

Rapid7's Incident Detection and Response and Vulnerability Management solutions, InsightIDR and Nexpose, integrate to provide visibility and security detection across assets and the users behind them.

Nexpose identifies and prioritizes weak points on your network, while InsightIDR relentlessly hunts threats by combining user behavior analytics, SIEM, and endpoint capabilities all in one. In combination, you detect malicious behavior earlier in the Attack Chain and expose user and asset risk, prioritized based on our knowledge of the attacker. This allows you to measurably reduce your attack surface, detect "unknown-unknowns" in real-time, and save time by knowing where to hunt.

Figure 1. For any exploitable vulnerability, see the exact users at risk.



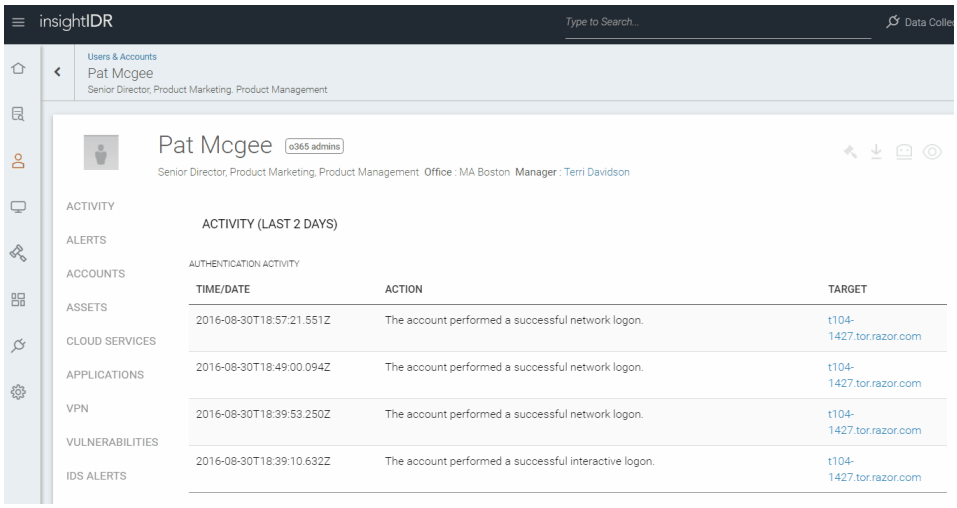
TWO BENEFITS OF PAIRING INSIGHTIDR AND NEXPOSE:
1. Put faces to your vulnerabilities.
2. Automatically place vulnerable assets under greater scrutiny.

Benefit 1: User Context for Your Vulnerabilities

InsightIDR integrates with your existing network and security infrastructure to create a baseline of your users' activity. It correlates all activity to the users behind them and alerts you of hard-to-detect attacks such as compromised credentials and lateral movement.

With the integration, InsightIDR ingests Nexpose vulnerability scan results and adds vulnerabilities to users' profiles. When you search by employee name, asset, or IP address, you'll get a complete look at their user behavior (Figure 2).

Figure 2. Searching for any user in InsightIDR brings up a full dossier of their activity.



You save time by:

- Seeing who is affected by what vulnerability to prioritize remediation
- Having instant context on the user(s) behind an asset to accelerate incident investigations and see if the attacker laterally moved beyond that endpoint
- Reducing your exposed attack surface by verifying that key players are not vulnerable

Benefit 2: Automatic Security Detection for Critical Assets

In Nexpose, you can dynamically tag assets as critical. Combined with InsightIDR, that context extends to the users accessing these assets. Assets tagged as critical are labeled as Restricted Assets when ingested into InsightIDR. This integration automatically places vulnerable assets under greater detection scrutiny.

Examples of restricted asset alerts:

- First authentication from an unfamiliar source asset: Instead of just alerting on an IP address, InsightIDR shows the exact users involved whenever possible.
- An unauthorized user attempts to log in: This can include a contractor or compromised employee attempting to access a financial server.
- A unique or malicious process hash is run on the asset: An Insight Agent deployed on your endpoints performs both vulnerability scanning and endpoint detection to find intruders earlier in the attack chain. This includes identifying every process running on your endpoints. These process hashes are automatically run against the wisdom of 50 virus scanners to identify malicious processes, as well as identify unique processes for further investigation.
- Lateral movement (both local and domain): Once inside your organization's network, intruders typically run a network scan to identify high-value assets. They then laterally move across the network, leaving behind backdoors and stealing higher privilege credentials.
- Endpoint log deletion: After compromising an asset, attackers look to delete system logs in order to hide their tracks. This is a high-confidence indicator of compromise.
- Anomalous admin activity, including privilege escalation: Once they've gained access to an asset or endpoint, attackers use privilege escalation exploits to gain admin access, allowing them to dump creds or attempt pass-the-hash. We identify and alert on anomalous admin activity across your ecosystem.

Configuring the InsightIDR | Nexpose Integration

If you have InsightIDR and Nexpose, setting up the Event Source is easy.

1. In Nexpose, set up a Global Admin.
2. In InsightIDR, on the top right Data Collection tab, go to Setup Event Source, and then Add Event Source.
3. Add the information about the Nexpose Console (Server IP & Port).
4. Add the credentials of the newly created Global Admin.

Learn more about Rapid7 InsightIDR and Nexpose at:

www.rapid7.com/insightIDR
www.rapid7.com/nexpose