InsightVM and InsightIDR

Integrate for total user and asset visibility

Rapid7's vulnerability management and incident detection and response solutions, InsightVM and InsightIDR, integrate to provide visibility and protection across your assets and the users behind them.

InsightVM identifies and prioritizes weak points in your environment, while InsightIDR relentlessly hunts threats by combining User Behavior Analytics, SIEM, and endpoint capabilities all in one tool. Combining these solutions enables you to detect malicious behavior across the ATT&CK Chain, expose user and asset risk, then prioritize that risk based on our unique knowledge of attacker tactics and mindsets. This allows you to measurably reduce your attack surface, find both common and targeted attacks, and save time by knowing where to hunt.

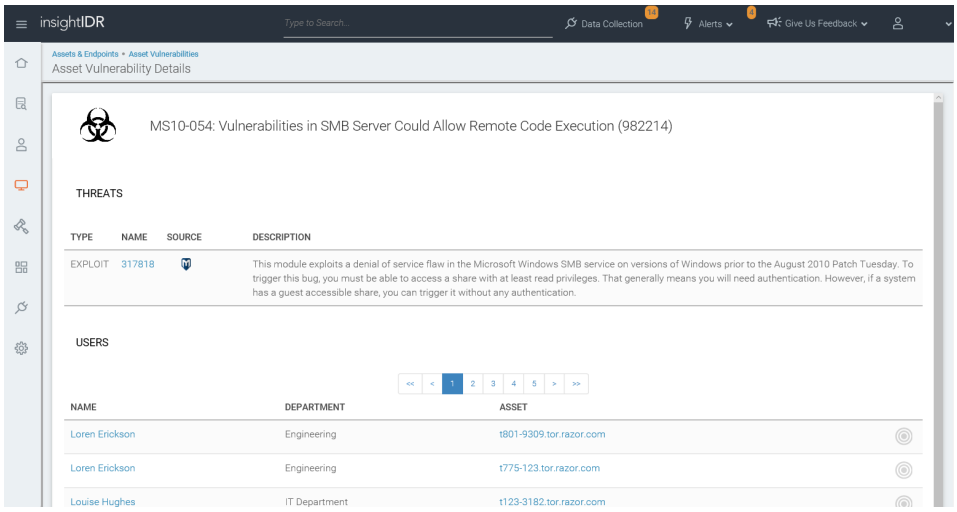

Figure 1: For any exploitable vulnerability, see the exact users at risk.

Benefit 1: User Context for Your Vulnerabilities

InsightIDR easily ingests data from your existing network and security infrastructure to baseline user activity across the modern network. With industry-leading User Behavior Analytics, you can easily retrace user activity and be alerted to hard-to-detect attacks, such as the use of compromised credentials or lateral movement.

InsightIDR integrates with InsightVM to ingest vulnerability scan results and add vulnerabilities to users' profiles. When searching by employee name, asset, or IP address, you'll get a complete look at their user behavior (Figure 2). Get your time back by:

- Seeing who is affected by what vulnerability to prioritize remediation
- Leveraging instant context on the user(s) behind an asset, speeding up alert triage and investigation (e.g. Did the attacker then move laterally?)
- Preventing and detecting with direct visibility into both vulnerabilities and real-time user behaviors

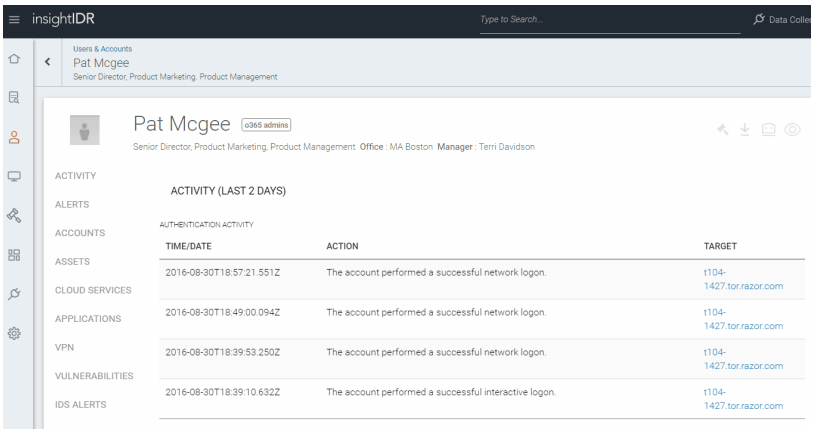

Figure 2: Searching for any user in InsightIDR brings up a full dossier of their activity.

Benefit 2: Automatic Detection for Critical Assets

In InsightVM, you can dynamically tag assets as critical (or other severities as appropriate). 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, and those identified as vulnerable can be automatically put under greater detection scrutiny.

Examples of restricted asset alerts:

- **Authentication from an unfamiliar source asset:** Instead of just highlighting authentication stemming from an IP address, InsightIDR shows you the assets and users involved whenever possible.
- **Logins from unauthorized users:** InsightIDR will alert if a contractor account or compromised employee account is attempting to access a restricted asset.
- **A unique or malicious process hash is run on the asset:** By deploying the Insight Agent on your endpoints, you can both collect vulnerability data and perform endpoint detection to find malware and anomalous behaviors. 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 any unique ones running across your endpoints.
- **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 often delete system logs in order to hide their tracks. This is a high-confidence indicator of compromise detectable by InsightIDR.
- **Anomalous admin activity, including privilege escalation:** Once attackers have gained access to an asset, various techniques are used to gain persistence or escalate privileges. The Attacker Behavior Analytics (ABA) leveraged in InsightIDR specifically find malicious micro-behaviors (such as anomalous Powershell commands or volume shadow copy tampering), and alert you as they happen. You can investigate these threats and take containment actions from within InsightIDR. This includes disabling user accounts, killing malicious processes, and quarantining assets from your network.

Configuring the integration

If you have InsightIDR and InsightVM, setting up the event source is simple:

- In InsightVM, set up a Global Admin.
- In InsightIDR, on the top right Data Collection tab, go to Set Up Event Source, then Add Event Source.
- Add the details for the InsightVM Console (Server IP & Port).
- Add the credentials of the newly created Global Admin.

Get Started

To learn more about InsightVM and InsightIDR, start your free trial today:

www.rapid7.com/try

About Rapid7

Rapid7 (Nasdaq: RPD) 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. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations.

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