RAPID7

PRODUCT BRIEF

InsightIDR Deception Technology

Deceiving malicious actors beyond just the honeypot

Deception technology is a defense technique that deploys false entities - or decoys made to imitate genuine assets - across an organization's infrastructure. Once they are configured and deployed (i.e "set and forget"), no one should be interacting with the false entities, ever. If malicious behavior is executed, the decoys will trigger high-fidelity alerts. This not only provides security teams an effective method for detecting, analyzing, and defending against attackers, it dramatically increases attacker efforts (e.g. time spent and confusion due to misdirection) which impacts their chances for successfully attacking an organization.

With InsightIDR, Rapid7's cloud-native SIEM and XDR, security teams can quickly create a multitude of false entities (based on Rapid7's extensive knowledge of attacker behavior), to identify malicious behavior earlier in the attack chain which include: honeypots, honey users, honey credentials, and honey files.

Break the attacker's kill chain with honeypots

Honeypots are fake systems that appear legitimate, which are deployed in a network to gather information. They work to divert malicious traffic away from important systems, identify anomalous network scans, and reveal information about attackers and their methods. Honeypots are part of InsightIDR's deception technology suite. Users can quickly and easily install, configure, and deploy - making honeypots an effective and quick defense to get up right away with InsightIDR. In addition to slowing down attackers, they are straightforward and low-maintenance, and help test incident response processes.

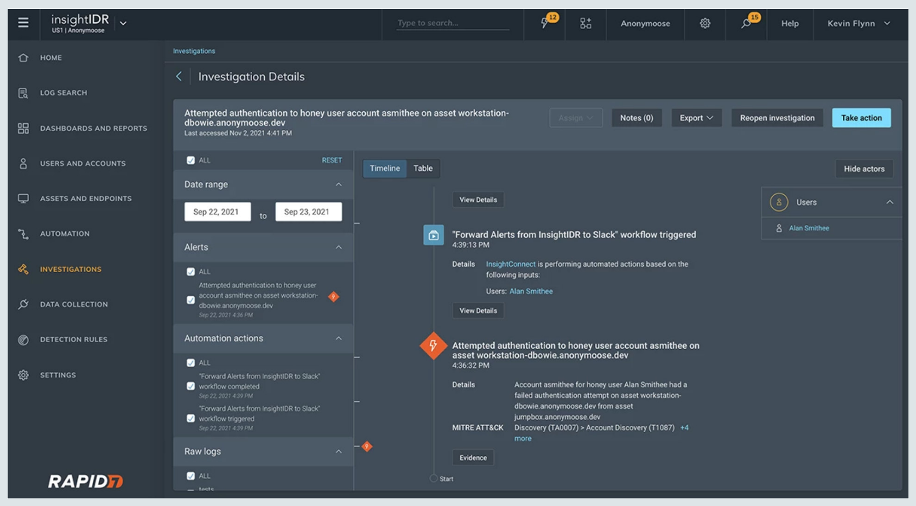
Thwart account access with honey users

Similar to honeypots, honey users are fake user accounts that are deployed within Active Directory (and replicated to all domain controllers). They detect and alert on brute-force attacks (password-guessing attempts from malicious actors) that are executed. Honey users are indistinguishable from actual accounts and never used for any valid authentication - meaning when an attacker mistakenly begins leveraging these accounts, you and your team can be certain this is a real threat and take action quickly and confidently.

Get Started

Stop malicious attacks earlier in the attack chain. Leverage deception technology, from InsightIDR, to help security teams detect compromise early.

Experience Deception Technology and InsightIDR, start your free trial today: www.rapid7.com/try



Attempted authentication to honey user account asmithee on asset workstation-dbowie.anonymoose.dev
Last accessed Nov 2, 2021 4:41 PM

Sep 22, 2021 to Sep 23, 2021

☑ ALL

☑ Attempted authentication to honey user account asmithee on asset workstation-dbowie.anonymoose.dev
Sep 22, 2021 4:36 PM

☑ ALL

☑ "Forward Alerts from InsightIDR to Slack" workflow completed
Sep 22, 2021 4:39 PM

☑ "Forward Alerts from InsightIDR to Slack" workflow triggered
Sep 22, 2021 4:39 PM

☑ ALL

tests

"Forward Alerts from InsightIDR to Slack" workflow triggered
4:39:13 PM

Details: InsightConnect is performing automated actions based on the following inputs:
Users: Alan Smithee

Attempted authentication to honey user account asmithee on asset workstation-dbowie.anonymoose.dev
4:36:32 PM

Details: Account asmithee for honey user Alan Smithee had a failed authentication attempt on asset workstation-dbowie.anonymoose.dev from asset jumpbox.anonymoose.dev
MITRE ATT&CK: Discovery (TA0007) > Account Discovery (T1087) +4 more

Catch the use of stolen credentials with honey credentials

Once an attacker compromises an endpoint, they will apply the obtained passwords across the organization to try and access other resources on the network. Honey credentials help combat this by serving as fake credentials injected onto the endpoint via the Insight Agent within InsightIDR. If an attacker tries to authenticate with a honey credential, an alert is immediately generated. Honey credentials also show a clear trail of an attacker moving laterally across a network, helping identify the steps that were taken across an attack.

File-level visibility with honey files

Honey files are legitimate files that act as decoys (it is strategy in placement, and lucrative in naming convention to draw attention to potential attackers). When a honey file is manipulated, it sends an alert (similar to the other deception technologies) letting your team know that a likely intruder is engaging with the fake file(s). With InsightIDR, you can deploy honey files on any network file share – including critical directories which can help create a stronger early warning system when an attacker is potentially targeting valuable company information. All actions taken on the file are monitored, giving file-level visibility alongside the native file integrity monitor (FIM) capabilities included with InsightIDR.

Using deception technology alongside other security solutions security teams can strengthen defenses and help detect compromise early.

PRODUCTS

insightCloudSec | insightIDR | Threat Command

insightVM | insightAppSec | insightConnect

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

SUPPORT

Customer Portal | Call +1.866.380.8113

RAPID7