



HOW **XDR** AND **SOAR** GET YOU UP AND RUNNING FASTER

Senior Security Solutions Engineer

October 2022

Scales are tipped in **attackers' favor.**



**DIGITAL
TRANSFORMATION**



**NO
PERIMETER**



**NOISE &
COMPLEXITY**



**RESOURCE &
SKILLS GAP**

Teams **don't have time to do it all.**

What if it could be **different?**

Less noise. More time. Faster detection and response.

The right detection and response approach can help.

Relevant insights, not aggregated noise.



RAPID7 XDR**RAPID7** MDR24/7 Global
SOC Expertise

insightIDR

Unified Next-Gen
SIEM & XDR

Threat Command

External Threat
Intelligence & Response

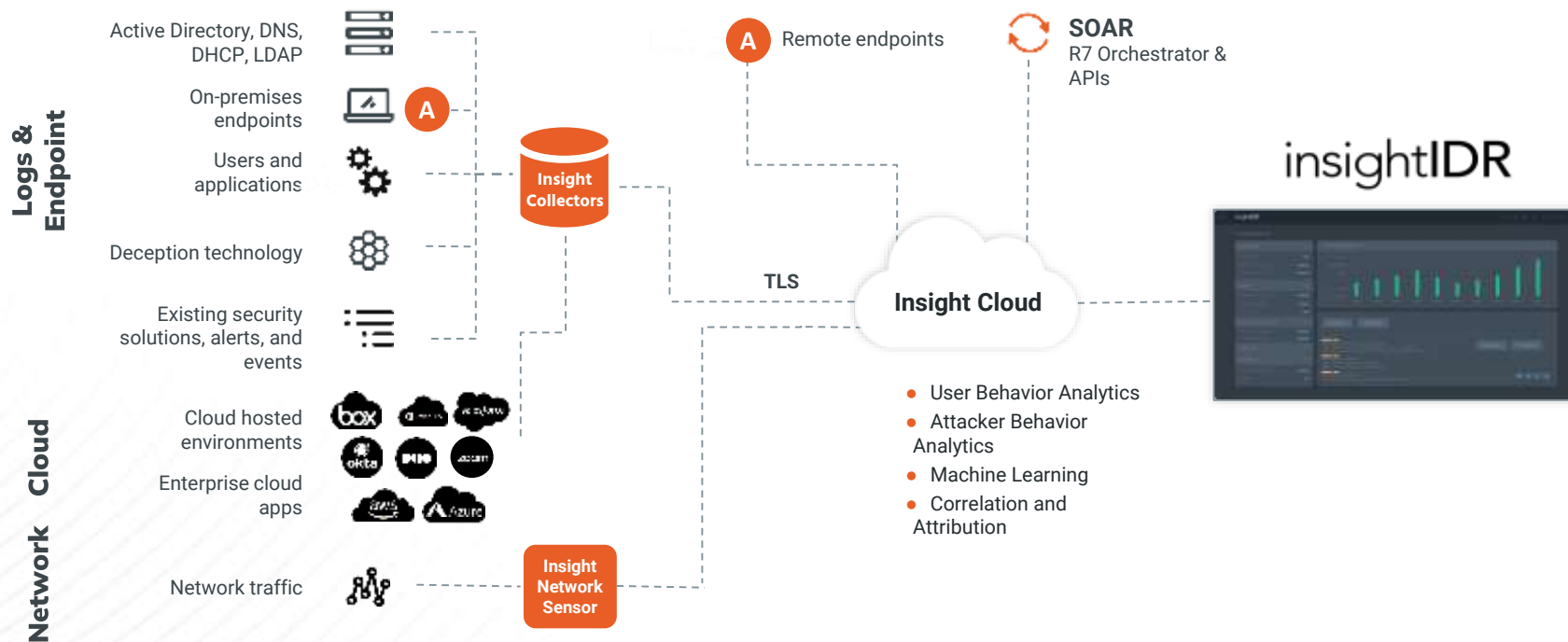
insightConnect

Accelerated Response &
Connected Ecosystem

Velociraptor

Crowdsourced
DFIR

InsightIDR Architecture





Home

Overview

Security Operations Activity

1,379

Users

As of Now

611.3k

Events Processed

↓ 303.4K (-53.17%) Last 24 Hours

4,036

Notable Behaviors

↓ 293 (-4.77%) Last 24 Hours

10

New Alerts

↓ 5 (-53.33%) Last 24 Hours

9

Endpoints Monitored

Last 15 Days

4

Data Collection Issues

As of Now

2

Honeypots

As of Now

Investigations by Priority

Last 28 days

30 Investigations



2 Critical



4 High



17 Medium



7 Low



0 Unspecified

Users

Last 28 days

Risky

1 Catherine Howard

22009

2 Anne Boleyn

21959

3 soconnor

4052

4 Chris Martin

4013

5 Ed Sheeran

4000

6 David Bowie

3886

7 Amy Winehouse

3881

Watchlist

Ingress Locations

Last 24 hours



Latest Processes

Last 28 Days

Unique

Rare

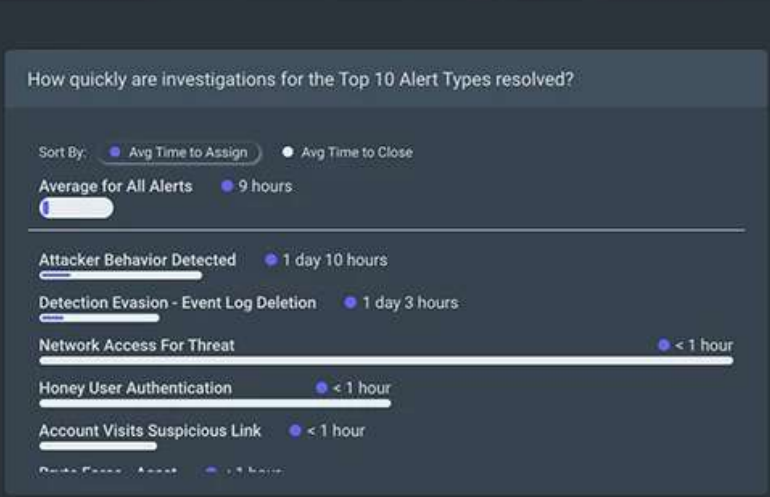
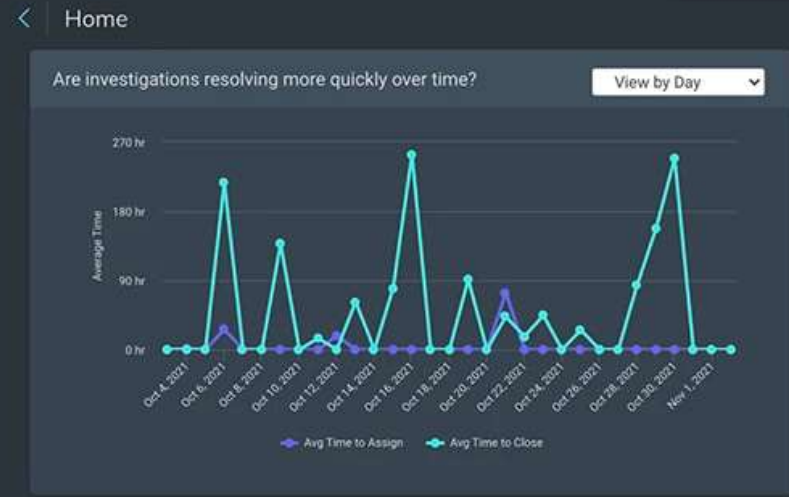


We don't see any data for Unique Processes at this time.

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.

[Setup](#)



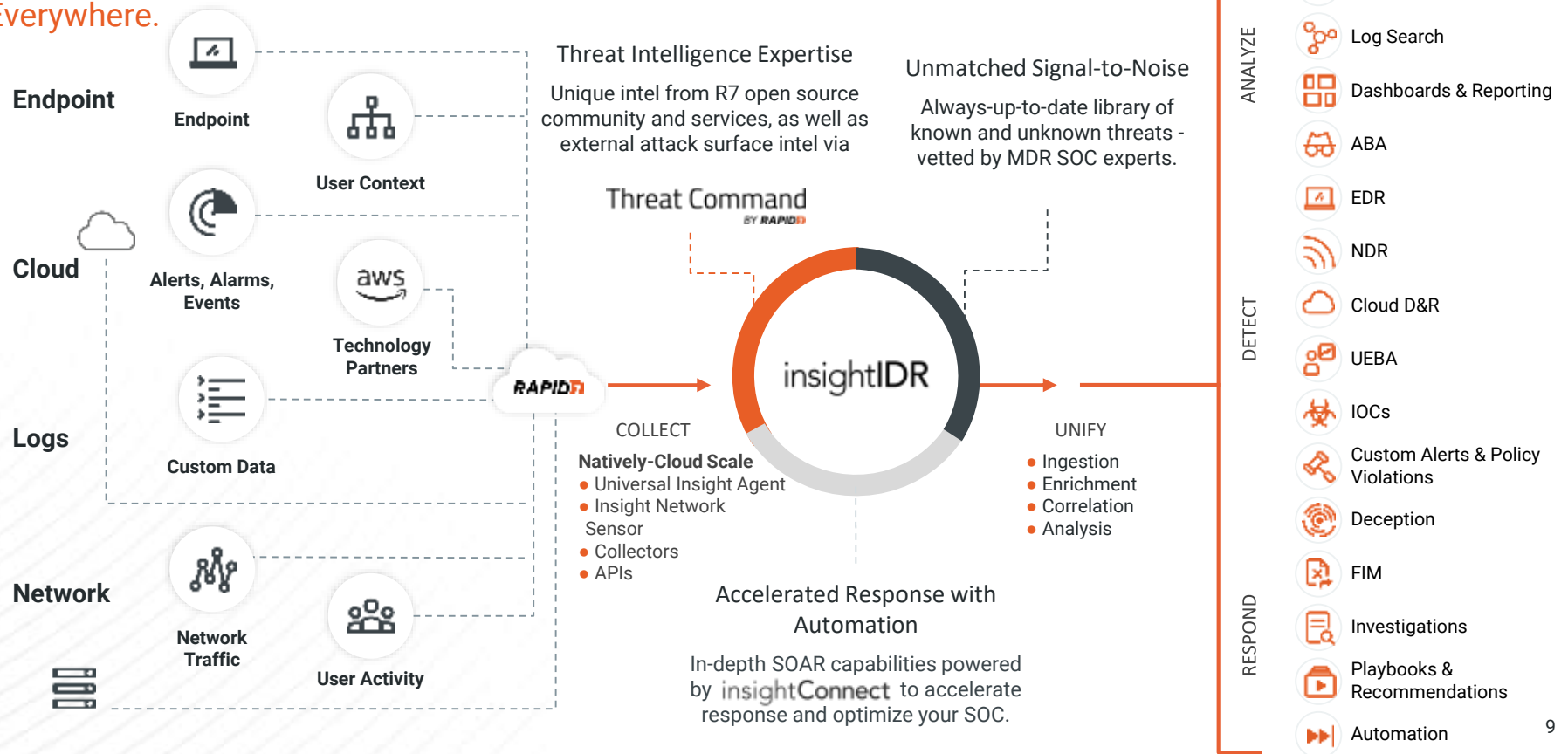
Attack Trends

To better understand the attack vectors inbound, break down the alerts into categories to see trends and their impacts to reach Mission Target.



Rapid7 insightIDR

Detect Faster. Respond Smarter. Secure Everywhere.



Detection Rules

Attacker Behavior Analytics | User Behavior Analytics | MITRE ATT&CK Matrix | Alert Modifications | Custom Alerts | Community Threats

Here you'll find a view of the MITRE ATT&CK framework's tactics, techniques and sub-techniques. Click into any tactic, technique or sub-technique to see a description and mitigations recommended by MITRE. Techniques and sub-techniques that are covered by Rapid7 detection rules are indicated by a green bar, and expand to show associated detection rules. [Read the documentation.](#)

Jump to: Reconnaissance

Tactics and techniques shown: All Covered by Rapid7

Search techniques and rules

Reconnaissance

10 techniques - 16 detection rules

Expand All

Gather Victim Identity Information T1589

Gather Victim Network Information T1590

Gather Victim Org Information T1591

Gather Victim Host Information T1592

Search Open Websites/Domains T1593

Search Victim-Owned Websites T1594

Active Scanning (1 rules) T1595

Search Open Technical Databases T1596

Search Closed Sources T1597

Phishing for Information (15 rules) T1598

Resource Development

7 techniques - 1144 detection rules

Expand All

Acquire Infrastructure (534 rules) T1583

Compromise Infrastructure (534 rules) T1584

Establish Accounts T1585

Compromise Accounts T1586

Develop Capabilities T1587

Obtain Capabilities (76 rules) T1588

Stage Capabilities T1608

Initial Access

9 techniques - 157 detection rules

Expand All

Valid Accounts (90 rules) T1555

Replication Through Remote Services T1582

External Remote Services T1585

Drive-by Compromise (1 rule) T1586

Exploit Public-Facing Application T1592

Supply Chain Compromise T1594

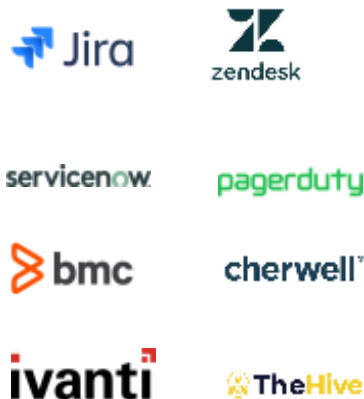
Trusted Relationship T1600

Hardware Additions T1601

Phishing (57 rules) T1590

Plugin Integrations With insightIDR

Bi-Directional Ticketing & Incident Tracking



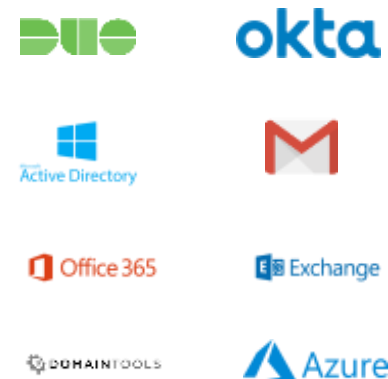
Network & Endpoint Containment



Threat Intelligence & Alert Enrichment






































User Management & Phishing Investigations



Find out more → extensions.rapid7.com

Use Cases for SOC Automation

Use Case	InsightIDR		InsightConnect
Contain Endpoints	 	+	     
Contain Users	 	+	  
Custom Escalation Pathways & Approval Chains		+	     
Enrich with Threat Intel	 	+	    
Block Senders			 
Block IPs with Firewall			     
Blacklist Hash			      
Create & Manage Incident Tickets	 	+	    

Automation Playbook

Take your SOC to the next level with SOAR!



Auto-Enrich Alerts



**Customize Alerting &
Escalation Pathways**



Auto-Contain Threats

Auto-Enrich Alerts

Let Machines Do The Heavy Lifting

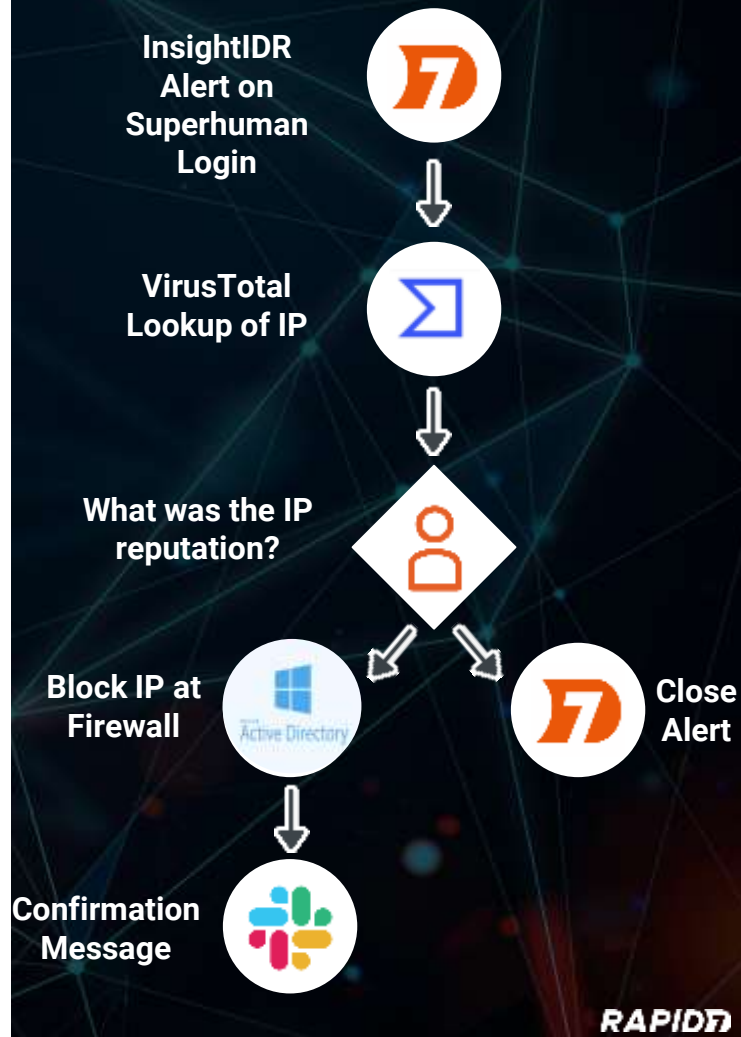
Eliminate the manual effort it takes to enrich indicators in your SIEM alerts. By the time you get to investigating, all hashes, IP addresses, domains, and more will have already been **cross-checked across several threat intelligence sources**.

Reduce Alert Fatigue

Have InsightConnect do the hard work of **aggregating threat intel and data correlation** to bubble up suspicious alerts and reduce false positives. Connect as many threat intel sources you need to arm your analysts with the right information to be lethal.



and more...



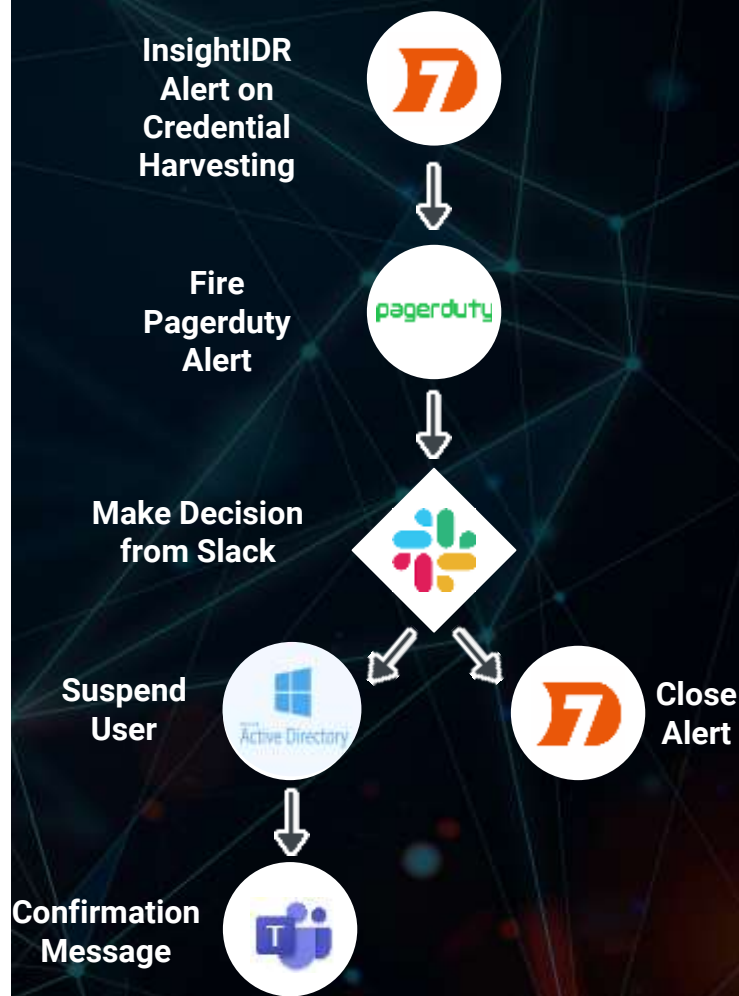
Customize Alerting & Escalation Pathways

Next Level Your Security Processes

Work the way your team wants to! Define **different communication & approval chains** based on the type or severity of alert. Automate as you go and systematically cut your alert queue down by eliminating false positives and **building a playbook for every situation**.

Take Your Work on the Go

Maintain **24/7 uptime** with tools like Microsoft Teams, Slack, or Pagerduty without having to be physically present in the SOC. **Make it easier for your team** to respond to alerts **without staring at a screen**.



Auto-Contain Threats

Drop your Meantime to Containment

Give your teams a leg up on attackers by **containing threats immediately after they are discovered**. Be **proactive about defense** by taking action if a team member is unable to make the call in a timely manner.

Stop Attackers at Multiple Layers

Orchestrate your entire stack to **stop attackers at every turn!** Leverage integrations with EDR, Firewall, and IAM tools to **block IP addresses, ban hashes, and quarantine assets** before threats have the ability to spread throughout your organization.



and more...



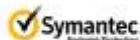
Eradicate & Mitigate Threats

Drop your Meantime to Containment

Give your teams a leg up on attackers by **containing threats immediately after they are discovered**. Be **proactive about defense** by taking action if a team member is unable to make the call in a timely manner.

Stop Attackers at Multiple Layers

Orchestrate your entire stack to **stop attackers at every turn!** Leverage integrations with EDR, Firewall, and IAM tools to **block IP addresses, ban hashes, and quarantine assets** before threats have the ability to spread throughout your organization.



and more...



RAPID7

Connect Security & IT

Streamline Operations

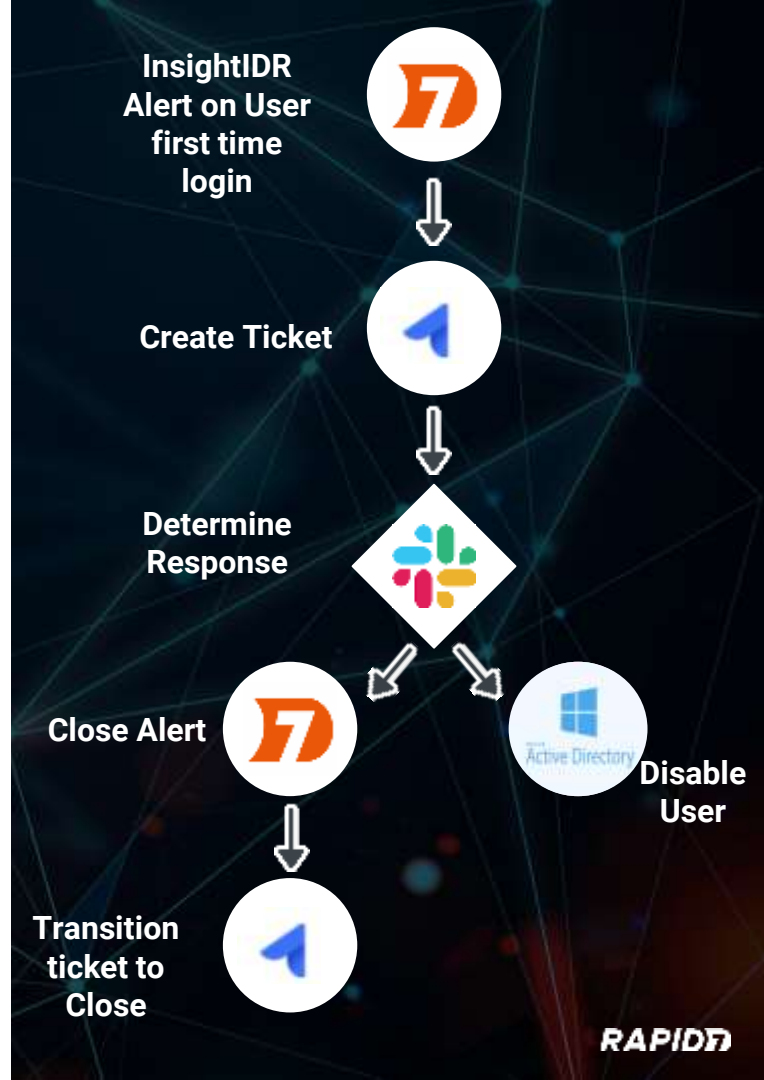
Improve cross team collaboration with other business units by tagging them in on tasks that may be outside of your role or responsibilities. Create, track, and get notified when tasks are closed by building in actions with your ITSM solution with SOAR.

Track the Incident Lifecycle

Build in compliance strategies to your automated workflows by adding actions to **create, update, and transaction tickets** as the alert at hand advances to an incident, or just confirming a false positive. Either way, gather all of the tails needed to stay within your organization's regulations.



and more...



Top Use Cases Customers are Automating Today



Off Hours Alert
Response



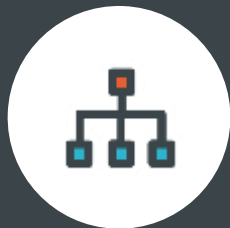
Push Updates to
Firewall



Confirm Multi-
Country Auth



Alert Data
Enrichment



Distributed Alerting



Automated
Assignment of High
Risk Investigations

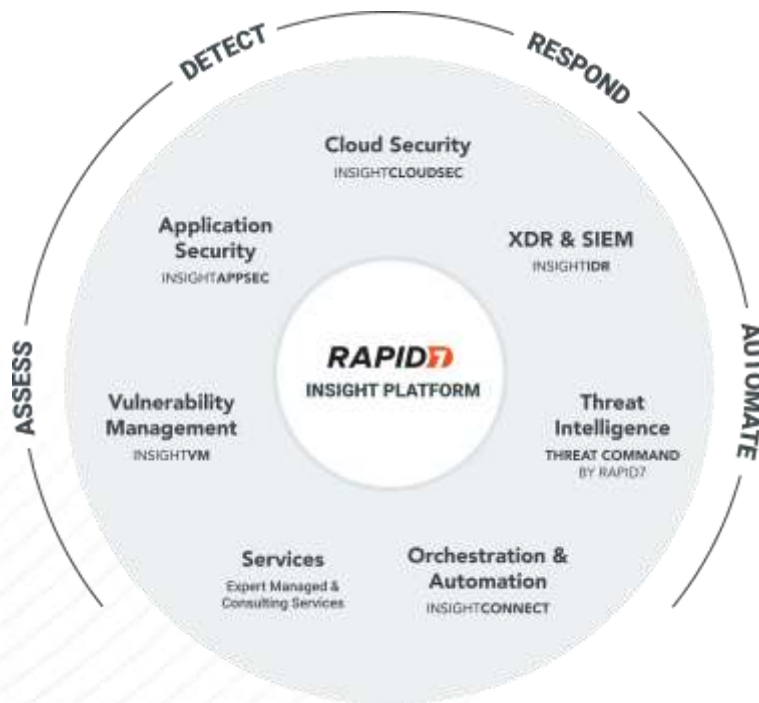


Suspicious
Endpoint
Containment



And Much More!

Comprehensive security that powers your business.



Technology

Best-in-Class Portfolio
Unified Platform Services
Plug and Play Integrations
Intelligent Automation

Expertise

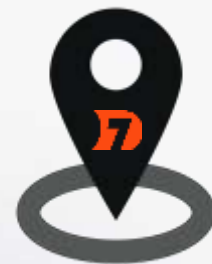
Security Research
Open Source Community

Differentiators

Flexible Product and Managed
Services Mix
Time to Value
Vendor Consolidation

RAPID7

Thank You.



Halle: 7

Stand: 529