

A faint, light gray background graphic consisting of a network of interconnected circles and lines, resembling a molecular structure or a data network, spanning the entire slide.

RAPID7

insightIDR

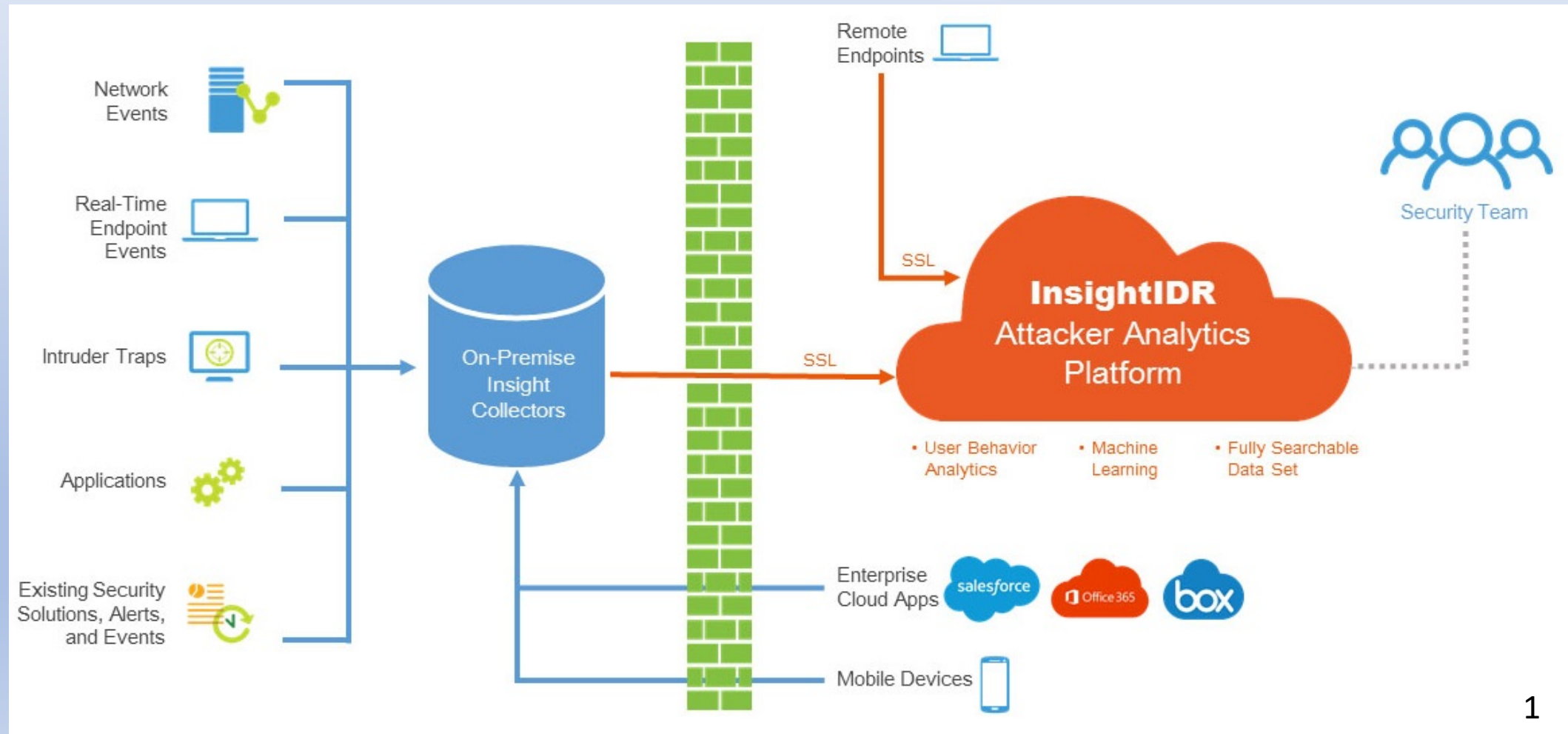
ECE 8496
Sean Carroll

Outline

- What is InsightIDR?
- InsightIDR Specifications
- DFIR Use Case
- Experience Report
- Consumer Reviews
- Key Takeaways

What is InsightIDR?

Rapid7's security solution that combines UEBA, SIEM, and EDR to help users focus on efficient incident detection and response (IDR).



InsightIDR Specifications

Add Event Source

User Attribution

Tie actions to the users and assets involved. It is highly recommended that you configure these event sources as they are necessary to tie the actions back to the users and assets involved.

LDAP

Active Directory

DHCP

Auto Configure

Discover and Configure event sources automatically. Auto Configure supports Active Directory, LDAP, DHCP and DNS.

Auto Configure

Endpoint Monitoring

Empower effective incident detection and investigation.

Endpoint Scan

Insight Agent

Mac Endpoint Monitor

Security Data

Enable Search and Analytics across your entire environment.

DNS

Firewall

IDS

Advanced Malware

VPN

Web Proxy

Email & ActiveSync

Cloud Service

Virus Scan

Data Exporter

Ingress Authentication

Raw Data

Send any machine data and make it available for search.

Generic Syslog

Generic Windows Event Log

Custom Logs

Database Audit Logs

Third Party Alerts

Integrate alerts from other products.

AWS GuardDuty

Carbon Black Response

Darktrace

insightIDR

RazorDemo

Type to search...

🔍

🔔

🔧

🌐

👤 Spencer Engelson

Home

Log Search

Dashboards

Users & Accounts

Assets & Endpoints

Investigations

Report Archive

Data Collection

Settings

1,673

Users

As of Now

152M

Events Processed

↑ 17.8M (43.36%) Last 24 Hours

4,338

Notable Behaviors

↑ 2,790 (48.78%) Last 24 Hours

1

New Alerts

↓ 1 (50%) Last 24 Hours

28.2k

Endpoints Monitored

As of Now

15

Data Collection Issues

As of Now

10

Honeypots

As of Now

Users

Last 28 days

Risky

Watchlist

1

Tabitha McLaughlin

Business Development Representative

📈 5133

📉 2

2

Irving Mathis

Director of Operations

📈 1750

📉 4

3

guest null

📈 813

📉 26

4

Lucia Parsons

Network Security Consultant

📈 599

📉 1

5

administrator

📈 487

📉 26

6

Carlo Anez

📈 282

📉 16

7

veeam_admin3 null

📈 160

📉 5

8

Pat Chandler

IT Engineering Manager

📈 154

📉 6

9

Tina Gonzales

Partner Relations Manager

📈 126

📉 8

10

Sean Laing

📈 122

📉 1

More >

Alerts by attack chain

Last 28 days

14

All alerts

0

Insidious

0

Exploit detection

4

Initialisation and reconnaissance

1

Reconnaissance

6

Lateral movement

3

Mission target

Ingress Locations

Last 24 hours

+

-

● success

● failure

More >

Latest Processes

Last 28 Days

Unique

Rare

1password 7

First Seen: Jul 16, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

1password extens

First Seen: Jul 16, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

__go_build_rapid7_bootstrap_go

First Seen: Jul 17, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

agent

First Seen: Jul 17, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

assetcacheagent

First Seen: Jul 15, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

attackpolicygenerator.exe

First Seen: Jul 17, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

cfnetworkagent

First Seen: Jul 17, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

com.apple.preferences.internetaccounts.remotese...

First Seen: Jul 17, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

com.apple.siri.acousticidsignature

First Seen: Jul 17, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

com.apple.accounts.accounts...

First Seen: Jul 17, 2018 8:00:00 PM

Last Seen: Jul 18, 2018 8:00:00 PM

🔔 1

DFIR Use Case

insightIDR
Simulation Lab

Type to search

Spencer Engleson

Investigation Details

MalDoc - Word Spawns Executable From Users Directory

Last accessed Oct 9, 2018 8:19 AM

Add data

Assign

Notes (0)

Export to PDF

Close investigation

Take action

ALL

RESET

Date range

Oct 9, 2018 to Oct 9, 2018

Alerts

ALL

MalDoc - Word Spawns Executable From Users Directory

Malicious documents - Filename Known

Bad

End

Oct 9, 2018

Malicious documents - Filename Known Bad

8:18:56 AM

Evidence

MalDoc - Word Spawns Executable From Users Directory

8:18:56 AM

Evidence

Start

Malicious documents - Filename Known Bad

```
"value": "fd904238e4f18ac631ed34f9bdc84ee6bce91",
{
  "algo": "md5",
  "value": "b554d9ae15d716a23b8b8d6dc4be513f"
},
"signingDetails": [],
"current": {
  "pid": 3992,
  "username": "rryan",
  "productName": null,
  "companyName": null,
  "commandLine": "C:\\Program Files\\Microsoft Offi",
  "processName": "WINWORD.EXE",
  "executablePath": "C:\\Program Files\\Microsoft O",
  "hashes": [
    {
      "algo": "sha1",
      "value": "3326210..."
```

MalDoc - Word Spawns Executable From Users Directory

Last accessed Oct 9, 2018 8:28 AM

Assign

Notes (0)

Export to PDF

Reopen investigation

Take action

New network data has been requested to be added. This may take some time to load, but the items in the right bar will stop spinning when complete.

ALL

RESET

Date range

Oct 8, 2018 to Oct 9, 2018

Alerts

ALL

MalDoc - Word Spawns Executable From Users Directory

Malicious documents - Filename Known

Bad

Network Access for Threat

Network Access for Threat

Network Access for Threat

Network Access for Threat

Detection Evasion - Event Log Deletion

Blacklisted Authentication

Restricted Asset Authentication - New User

End

Oct 9, 2018

Started Disable User in Active Directory

8:28:50 AM

This action was taken on Rusty Ryan.

View Details

Finished Quarantine Asset

8:24:30 AM

This action was taken on win7s4.akbar.trap.

View Details

Undo Quarantine

Started Quarantine Asset

8:24:25 AM

This action was taken on win7s4.akbar.trap.

View Details

Undo Quarantine

Hide actors

Asset Authentication

Users


Rusty Ryan

Assets

win7s4.akbar.trap

Experience Report

InsightIDR Data Collection Alert

 insight_noreply@rapid7.com
Today, 9:51 AM
Sean Carroll

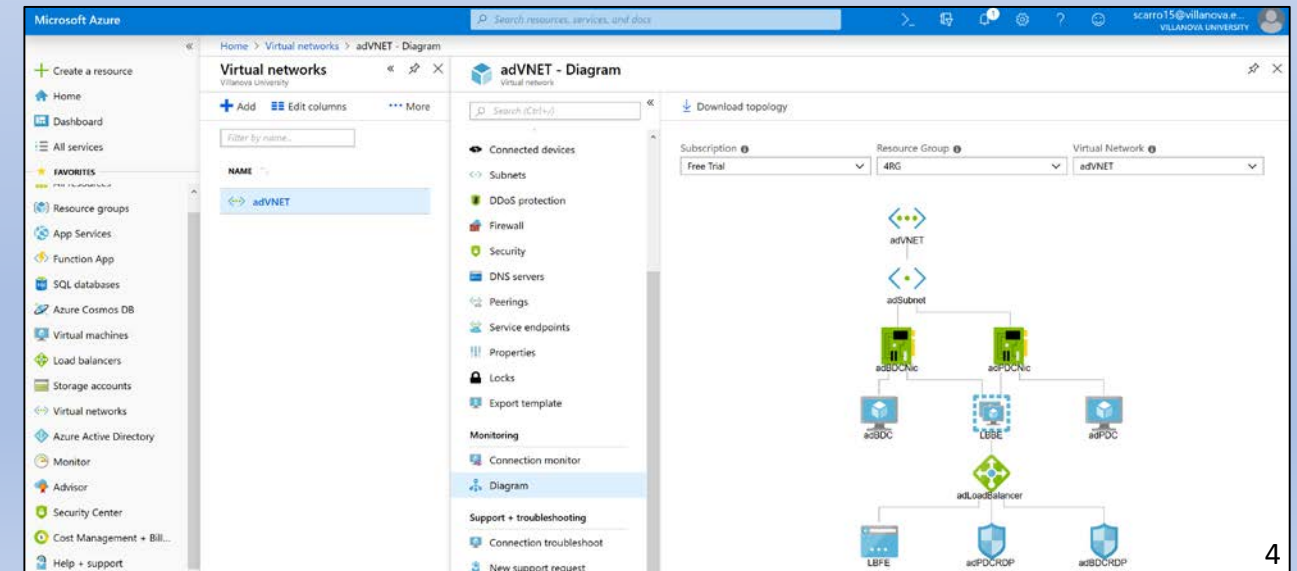
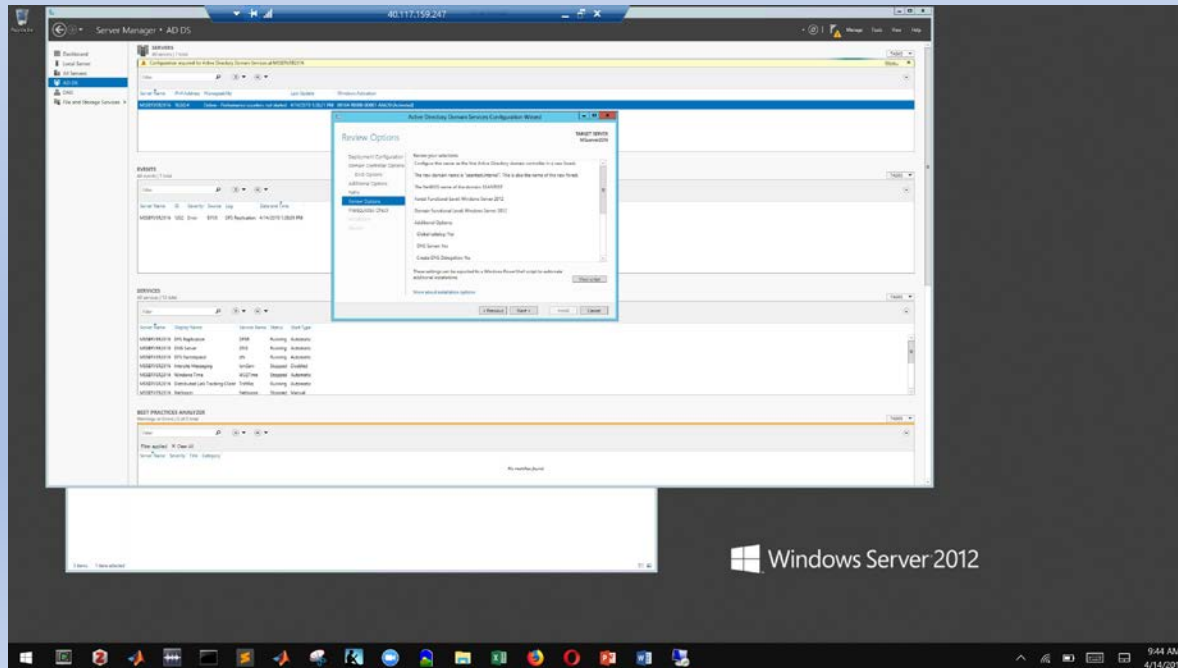
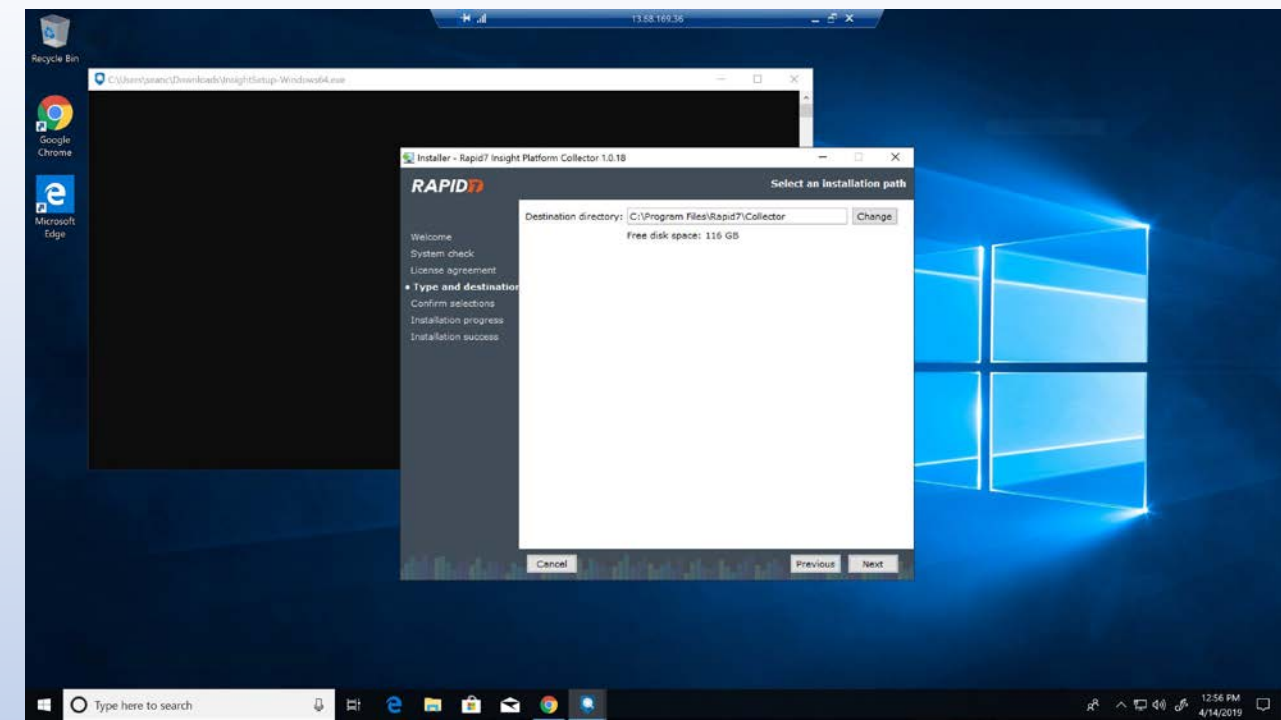
COLLECTOR ISSUE

Collector 'w10main', running at IP address 10.0.0.5, has encountered following issue at Sun Apr 14 13:29:17 UTC 2019:

Collector has been inactive for 22 minutes

For details, see the [data collection page](#).

The InsightIDR Team



Consumer Critical Reviews

- “Everything they are building is cloud based...we could not at this time justify **sending out all of our vulnerabilities** and all of our logs to an outside company.”⁶
- “The interface was **not customizable** (dashboards), and there are a limited amount of event sources that are pulled, especially from **Windows endpoints**. Additionally the automated event correlations presented more **false positives than actual benefits**.”⁶
- “[Rapid7 developer said] the product wasn't designed to run against **dynamic cloud-based sites**, wasn't designed to work well with **web application firewalls** that we're on a shared platform, and that they weren't going to fix it.”⁶
- “We had to disable it on a lot of machines because the background scanning **service slowed them down** a lot.”⁶

Key Takeaways

- InsightIDR can be a useful tool for Incident Response if company does not already have a SoC
- InsightIDR integrates UEBA, SIEM, ERD into a streamlined platform so that IDR can be further automated.
- InsightIDR has integration with other Rapid7 cloud products
- Other Products: IBM, Logrhythm, Splunk, Dell (RSA), and Exabeam

References

1. https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-insightidr-product-brief.pdf
2. https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-technology-brief-insight-agent.pdf
3. <https://reprints.forrester.com/#/assets/2/1336/RES142217/reports>
4. https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure-fall2018.pdf/
5. <https://castbox.fm/app/castbox/player/id476645/id81539471?v=4.1.190412&autoplay=0>
6. https://www.reddit.com/r/sysadmin/comments/78fu0v/anyone_using_rapid7_insightidr/
7. <https://www.youtube.com/watch?v=e15qkgK8Gtk&feature=youtu.be>
8. <https://insightidr.help.rapid7.com/docs/insightidr-overview>
9. <https://embed.vidyard.com/share/eUPMwbRT1j2BjPowCa6VL9>
10. <https://azure.microsoft.com/en-us/>

Images

1. <http://spireind.com/wp-content/uploads/2016/10/Rapid7-InsightIDR.png>
2. [https://files.readme.io/a0ee579-InsightIDR Tech Deep Dive.png](https://files.readme.io/a0ee579-InsightIDR_Tech_Deep_Dive.png)
3. <https://www.youtube.com/watch?v=e15qkgK8Gtk&feature=youtu.be>
4. <https://azure.microsoft.com/en-us/>