

# Threat Briefing

**MTC Advanced - May 2024**

# Agenda

---

- Service Status Update
- New Features, Improvements, & Fixes
- Vulnerability Trends
- Updates & Recommendations
- Workshops & Webinars
- 2024 Q1 - Incident Response Data
- Q&A

# Rapid7 Managed Services Contact Information

Issue	Escalation Path	Contact Methods	Additional Notes
<b>Security Related Emergency</b>	MDR Team	Managed Services Emergency Hotline us: +1 844-777-7637 uk: +44 800-088-5859 sg: +65 800-852-3321 au: +61 2-4734-7032	In an emergency, call the hotline to speak with an Managed Services Representative. Alternatively, submit a case via the platform. Include any applicable information in request (i.e.- Alert, Activity, Hostnames, Users, Time, etc)
<b>Non-Emergency Managed Inquiries</b>	Primary Customer Advisor	<a href="#">Platform</a>	Non-urgent questions related to Alerts, Tuning, Product, Reporting or the Managed Service. If Alert related, include Alert, Activity, Hostnames, Users, Time, etc
<b>Product or Support Issue</b>	Primary Customer Advisor	<a href="#">Platform</a>	Please provide as many details as possible to include screenshots, steps already taken, assets affected, potential impact, etc.
<b>Overall Account Inquiries and Information</b>	Customer Success Manager	name@rapid7.com	Licensing, Renewals, Webinars and Training Opportunities

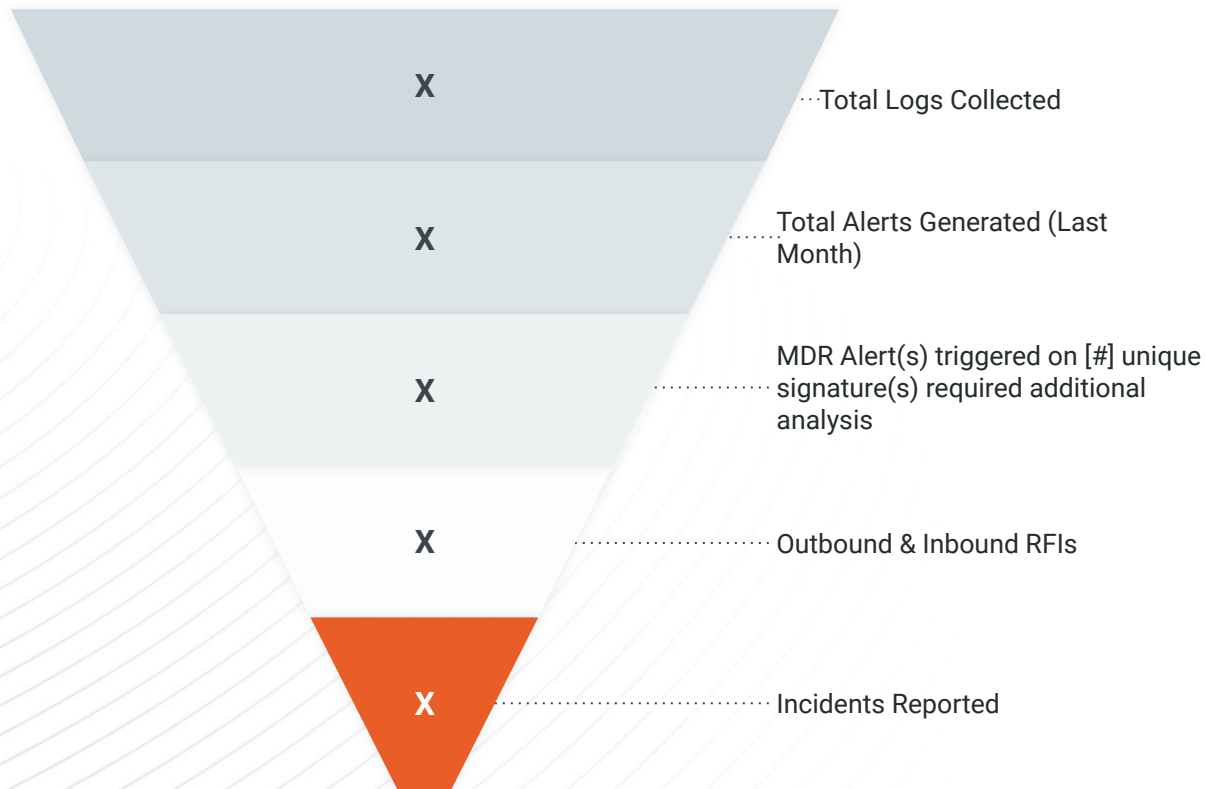
If the MDR team needs to reach you, they will call from the following number:

**+1(617) 906-7121**  
**+1(617) 247-1717**

Please be sure to save this number to your phone and allow through Do Not Disturb

# Service Status Update

# Alerts, RFIs, & Incident Reports



	Closed Alerts by Priority	Incident Reports
High	[#]	[#]
Medium	[#]	[#]
Low	[#]	[#]

# New Features, Improvements & Fixes

# Insight Agent Update

May 1, 2024

## Sysmon and Events Monitor Update

- The [Sysmon Installer component](#) improved its ability to detect system crashes. The Sysmon Installer component manages the Sysmon service installation and monitors for system crashes in order to uninstall the Sysmon service if a crash occurs. It uninstalls the Sysmon service to protect the asset from recurring system crashes. However, this has led to the Sysmon Installer to uninstall Sysmon unnecessarily, even if Sysmon did not cause the crash. Now, version 1.10 of the Sysmon Installer enables Sysmon to continue to run and will not uninstall Sysmon if it fails to read the crash dump due to a system shutdown. In all other scenarios, the Sysmon Installer will uninstall Sysmon as a protective measure to ensure the safety of the endpoint.

## Fixed

- We fixed an issue within [Sysmon Installer component's](#) ability to detect system crashes.
- We fixed an issue with the Darwin installer file bundle that prevented Velociraptor from installing or updating on MacOS endpoints.
- We fixed an issue that could prevent Velociraptor from communicating with the Agent Core sub-component if the Agent Core sub-component restarted while Velociraptor was running.

# New IDR Features

**Cloud Event Sources:** In the past, you had to deploy a collector in your network to collect log data. This took time to set up and manage. Cloud-based event sources provide you with a quick and easy way to ingest your security events without setting up a collector. You can set up the cloud event source, add your credentials, and log data will flow into Log Search within 10 minutes. Here's a list of the cloud event sources:

- Cisco Umbrella
- Proofpoint TAP
- Mimecast
- Okta
- Duo
- Zoom
- Salesforce

**Add a threshold and average line to a dashboard card:** For cards that leverage a single query, you can now switch on a threshold line and an average line. To add these lines to your card, select Edit and navigate to the Chart tab. For now, this is only available to bar charts (vertical and horizontal), line charts, and area charts. This update gives our users greater flexibility in monitoring trends and anomalies. These new reference lines, especially the threshold line, makes it easier for you to identify and act on critical insights.

[See the full list of New Features](#)



# IDR Improvements

---

- **Log Search sorting:** We removed a constraint on the order of search results. Previously, it was restricted to searches within the last 30 days. You can now search beyond this limit to the log retention when ordering by newest log first.
- **Additional log set context:** We added the log set name to the results displayed when you run a groupby(#log) query. By providing this additional information, you now have more context when you want to determine the relative activity across different logs.
- **Remove old logs:** We added the ability to remove old logs with the log selector interface in Log Search. Provided the criteria for removal is met, an icon appears adjacent to the name in Log Search. This allows you to remove redundant and stale logs (where a collector, event source, or network sensor has already been deleted) and means you can focus their queries on relevant logs with live data.
- **Word clarification:** We updated the wording on the Investigation Management and Detection Rules pages from Alerts to Detection Rules for clarity.
- **Event source counts:** We updated Event Source filtering to recalculate Event Source counts after selecting filters.

[See the full list of Improvements](#)

# IDR Bug Fixes

---

- We fixed an issue where filters in Investigation Details for Ingress Authentication data were not filtering data correctly.
- We fixed an issue where users were being notified of an error after editing an event source when no error had occurred.
- We fixed an issue where the search results for Event Sources was blank when the list was empty rather than displaying contextual information.
- We fixed an issue where users could elect that a collector-based event source can be cloud-based.
- We fixed an issue where some timestamps in Investigation Details and Alert Triage pages weren't following user preferences.

# InsightVM Release Notes

5/22/2024: [6.6.253](#)

## New

- **CIS benchmark coverage.** We added built-in support for CIS SQL Server 2022 benchmark, version 1.1.0.

## Improved

- **Asset Search - Customer Requested.** We improved the communication between the Security Console and the Insight Platform, improving data consistency.
- **Java Runtime Environment (JRE).** We improved the InsightVM's security posture by upgrading the JRE included with the Scan Engine and Security Console to Zulu OpenJDK version 1.8.0\_412.

## Fixed

- CIFS/SMB credentials are no longer incorrectly reported as not supplied (NO\_CREDS\_SUPPLIED) when authentication fails. Now, failure to authenticate is correctly reported as SUPPLIED\_FAILED.
- We fixed an issue affecting credential elevation when using the CyberArk integration where the Test Credential was successful on the Site Configuration page but unsuccessful during the scan.
- We fixed an issue affecting the SQL Export Report feature that prevented some SQL queries from executing due to false validation errors.
- We updated the error messages that are generated when a user attempts to edit and save Discovery Connections to be more relevant.
- We updated our CIS SQL Server 2019 benchmark to resolve an issue that prevented the policy from being copied.

5/15/2024: [6.6.252](#)

## New

- **Microsoft Patch Tuesday coverage.** This release includes new Microsoft Patch Tuesday content for updated scan coverage for May 2024. Check out our blog post for details.
- **CIS benchmark coverage.** We added built-in support for CIS Oracle Linux 9 benchmark.

# New IDR Features

## Updated Reports Experience, Including Custom Reports:

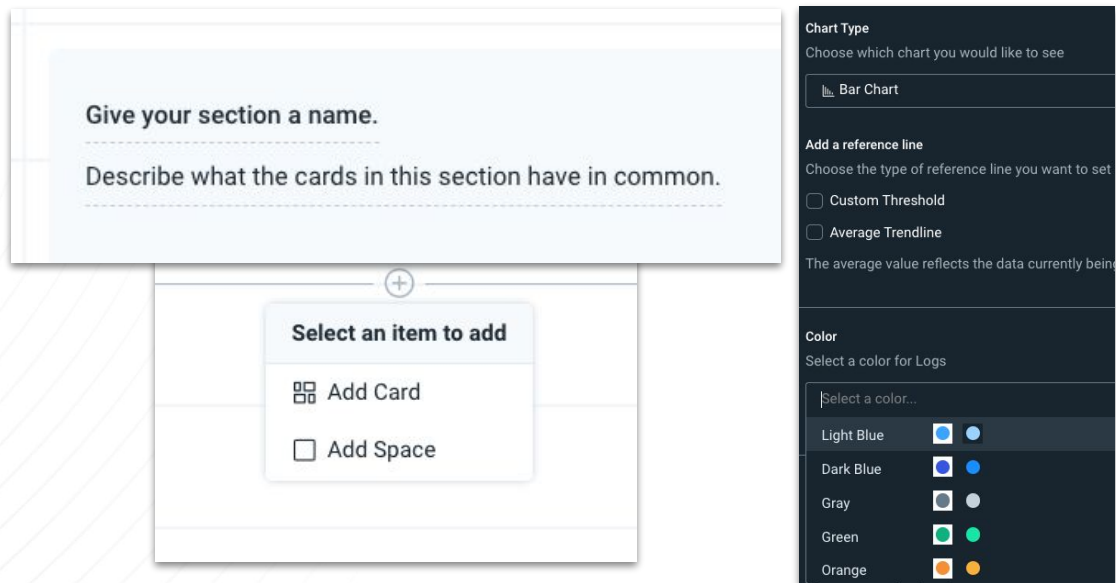
We added new customizations to reports to help you tell a better story with your data.

- Add items to the report in real-time by hovering over the report and clicking the + that appears.
- Edit section names and descriptions.
- Change the layout. You can now drag and resize all items on the report to be the way you want.
- Edit the visualization and color of individual cards. (Changes to cards on the report will not be reflected on the dashboard)

### Note:

You can add cards to the report from the card library and dashboards.

To customize the layout of your report you can add a blank space.



The image shows a screenshot of the IDR report editor interface. It features a light blue background with a grid pattern. A central panel displays two text input fields for section customization:

- Give your section a name.** (with a dashed line below for input)
- Describe what the cards in this section have in common.** (with a dashed line below for input)

Below these fields is a plus sign icon (+) and a dropdown menu titled "Select an item to add" with two options:

- Add Card
- Add Space

On the right side, a dark-themed sidebar shows configuration options for a chart:

- Chart Type:** Choose which chart you would like to see. A "Bar Chart" option is selected.
- Add a reference line:** Choose the type of reference line you want to set. Options include "Custom Threshold" and "Average Trendline".
- Color:** Select a color for Logs. A color palette is shown with options: Light Blue, Dark Blue, Gray, Green, and Orange.

# MTC Intel Dashboard

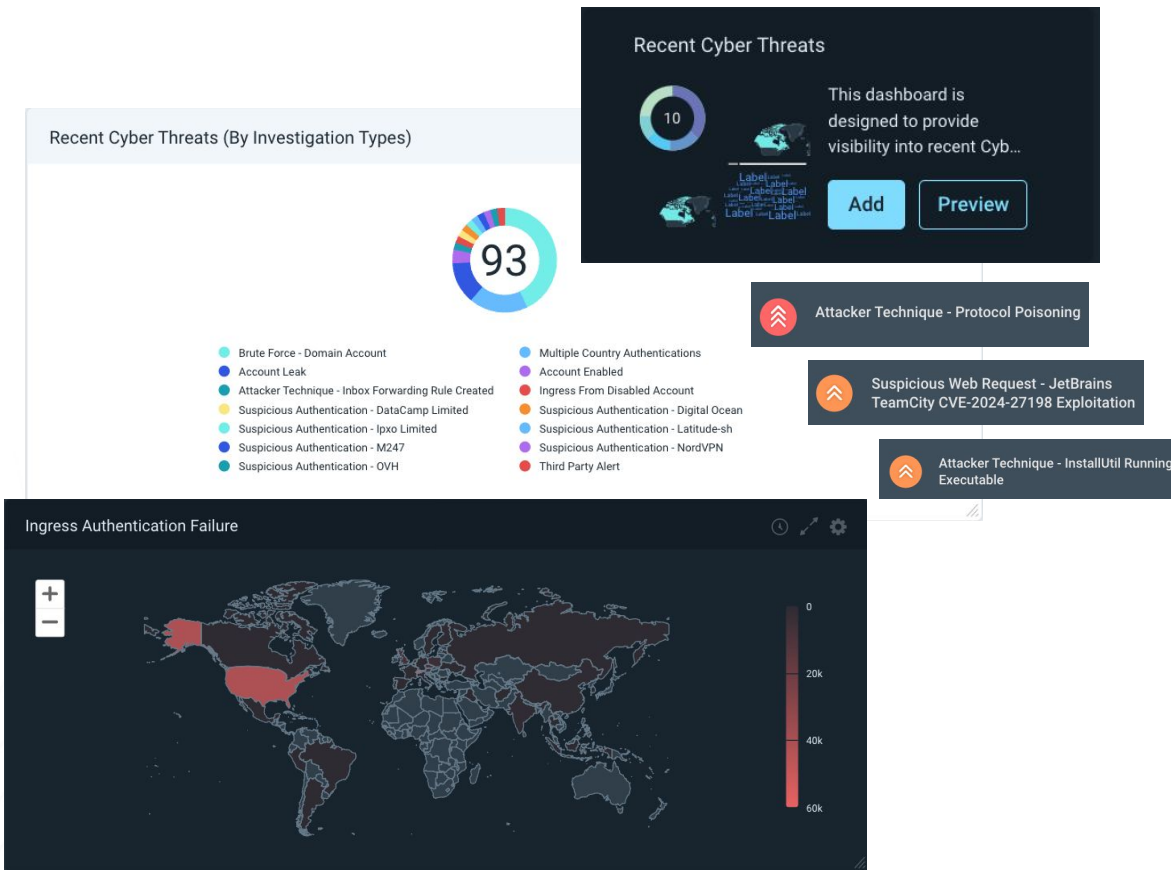
## WHY

Cyber situational awareness from various types of investigations and data that allows you to review, hunt, explore activity of interest based today's cyber threats that may be lurking in your environment

- CA, Customer, and MDR SOC review of alerts and threats from various log sources
- Expanded insight for potential new investigations, monitoring and response in your environment

## WHAT

Event Source(s) to allow for Rapid7 MDR direct triage and investigation for MTC customers



# Vulnerability Trends

# Threat Landscape - Microsoft - May 2024

## May 2024 Patch Tuesday

Microsoft is addressing 61 vulnerabilities this [May 2024 Patch Tuesday](#). Microsoft has evidence of in-the-wild exploitation and/or public disclosure for 3 of the vulnerabilities published today

### Windows DWM: zero-day EoP

- [CVE-2024-30051](#) - **Windows DWM Core Library Elevation of Privilege Vulnerability** - An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.

### MSHTML: zero-day security feature bypass

- [CVE-2024-30040](#) - **Windows MSHTML Platform Security Feature Bypass Vulnerability** - The advisory states that an attacker would have to convince a user to open a malicious file; successful exploitation bypasses COM/OLE protections in Microsoft 365 and Microsoft Office to achieve code execution in the context of the user.
- As Rapid7 has [previously noted](#), MSHTML (also known as Trident) is still fully present in Windows — and unpatched assets are thus vulnerable to CVE-2024-30040 — regardless of whether or not a Windows asset has Internet Explorer 11 fully disabled.

### Visual Studio: zero-day DoS

- [CVE-2024-30046](#) - **Visual Studio Denial of Service Vulnerability** - Only Visual Studio 2022 receives an update, so older supported versions of Visual Studio are presumably unaffected.

### SharePoint: critical post-auth RCE

- [CVE-2024-30044](#) - **Microsoft SharePoint Server Remote Code Execution Vulnerability** - allows an authenticated attacker with Site Owner permissions or higher to achieve code execution in the context of SharePoint Server via upload of a specially crafted file, followed by specific API calls to trigger deserialization of the file's parameters.

### Excel: arbitrary code execution

- [CVE-2024-30042](#) - **Microsoft Excel Remote Code Execution Vulnerability** - Successful exploitation requires that an attacker convince the user to open a malicious file, which leads to code execution, presumably in the context of the user.

# Threat Landscape - Apple

## Apple Security Updates

Safari 17.5

macOS Sonoma 14.5

macOS Ventura 13.6.7

macOS Monterey 12.7.5

iOS 17.5 and iPadOS 17.5

iOS 16.7.8 and iPadOS 16.7.8

## Recently addressed critical vulnerabilities

### WebKit - CVE-2024-27834

- **Impact:** An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication
- **Description:** The issue was addressed with improved checks.

### Kernel - CVE-2024-27818

- **Impact:** An attacker may be able to cause unexpected app termination or arbitrary code execution
- **Description:** The issue was addressed with improved memory handling.



# Threat Landscape - Emergent Threats

## Emergent Threats

Emergent Threat Response (ETR) is a cross-team effort to deliver fast, expert analysis and first-rate security content for the highest-priority security threats to help customers understand their exposure and act quickly to defend their networks.

In InsightVM, these ETR vulnerabilities are consolidated in the "Rapid7 Critical" category (vulnerability.categories IN 'Rapid7 Critical'). This category includes all ETR vulnerabilities as well as other critical vulnerabilities from before the formal ETR process was created.

[AttackerKB](#)

[Blog RSS Feed](#)

## Recent Threats

### [CVE-2024-24919: Check Point Security Gateway Information Disclosure](#)

On May 28, 2024, Check Point published an advisory for CVE-2024-24919, a high-severity information disclosure vulnerability affecting Check Point Security Gateway devices configured with either the "IPSec VPN" or "Mobile Access" software blade.

### [CVE-2024-4978: Backdoored Justice AV Solutions Viewer Software Used in Apparent Supply Chain Attack](#)

Justice AV Solutions (JAVS) is a U.S.-based company specializing in digital audio-visual recording solutions for courtroom environments. According to the vendor's website, JAVS technologies are used in courtrooms, chambers and jury rooms, jail and prison facilities, and council, hearing, and lecture rooms. Their company website cites over 10,000 installations of their technologies worldwide.

### [Ongoing Social Engineering Campaign Linked to Black Basta Ransomware Operators](#)

Rapid7 has identified an ongoing social engineering campaign that has been targeting multiple managed detection and response (MDR) customers. The incident involves a threat actor overwhelming a user's email with junk and calling the user, offering assistance.

# Updates & Recommendations

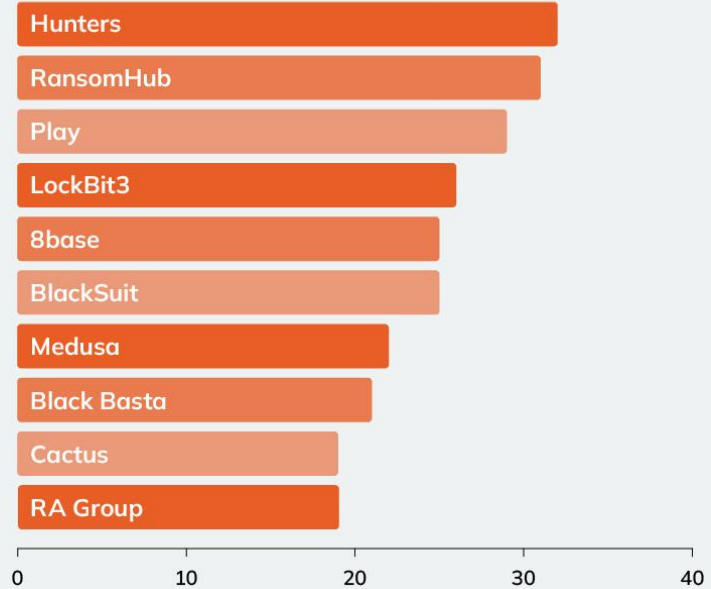
**RAPID7**

# Top 10 Ransomware Groups

by Number of Extortion Attempts

**APRIL 2024**

Number of Posts by Group



# Updates

---

Rapid7 has identified an **ongoing social engineering campaign** that has been targeting multiple managed detection and response (MDR) customers. The incident involves a threat actor overwhelming a user's email with junk and calling the user, offering assistance. **The threat actor prompts impacted users to download remote monitoring and management software like AnyDesk or utilize Microsoft's built-in Quick Assist feature in order to establish a remote connection.** Once a remote connection has been established, the threat actor moves to download payloads from their infrastructure in order to harvest the impacted users credentials and maintain persistence on the impacted users asset.

While ransomware deployment was not observed in any of the cases Rapid7 responded to, the indicators of compromise we observed were previously linked with the **Black Basta ransomware** operators based on OSINT and other incident response engagements handled by Rapid7.

Rapid7 recommends:

- Baselining your environment for all installed remote monitoring and management solutions and utilizing application allowlisting solutions, such as AppLocker or Microsoft Defender Application Control, to block all unapproved RMM solutions from executing within the environment.
- Blocking domains associated with all unapproved RMM solutions. A public GitHub repo containing a catalog of RMM solutions, their binary names, and associated domains can be found [here](#).
- Ensuring users are aware of established IT channels and communication methods to identify and prevent common social engineering attacks.
- Ensuring users are empowered to report suspicious phone calls and texts purporting to be from internal IT staff.

Read more on our Rapid7 Blog: [Ongoing Social Engineering Campaign Linked to Black Basta Ransomware Operators](#)

# Security Recommendations

## Remediating Imposter Domain Names

Rapid7 recommends reviewing and blocking identified imposter domains if they serve no business need.

<https://dnstwist.it/> is a free tool that generates a list of domain names similar to a given domain name and performs DNS queries for them (A, AAAA, NS and MX). For MX records it checks whether there is an active mail server which could be used to intercept misdirected emails.

**Dnstwist** checks for copycat/imposter domains. Most of the time these domains are owned by domain squatters that hope an organization will purchase it. However, when malicious actors set up an imposter domain for abcbank[.]com such as acbbank[.]com, they will use the imposter domain to host malicious payloads or to try and trick customers into giving up their credentials.

### Our Recommendations:

1. Block outbound web traffic to the websites you don't own as a precaution.
2. Check the Monthly MDR Service Report and **dnstwist[.]it** every month for new entries and block if needed.
3. Check your outbound web traffic, start with the top 10 sites, and run those through **dnstwist[.]it**.
  - a. Block THOSE imposter domains on your outbound firewall. (The danger isn't that an employee of abcbank will mistype their own company site and end up at an imposter; the danger is when an employee is trying to check their paystub, or Netflix, or their 401k, or cat memes, and "fat-fingers" a key.)
  - b. Employers can't control what other companies do, so employees may end up at a malicious site on their company device.
  - c. If your top-visited domain on the outbound web traffic is adp[.]com – run **dnstwist** for that. Then block those imposter domains with your web filter.
4. Create a survey.
  - a. Send it out to every department and every executive and ask them for their top 10 vendors, business websites, and external people (email addresses) they deal with.
  - b. Same thing as above: **dnstwist** them and block the imposters.
5. Write a script that pulls this data monthly and add the new ones to your web filter.

# Detection Updates for April 2024

**104**

Total # of Detections  
Reviewed

**58**

New Third party  
Detections Created

**19**

New R7 Detections  
Created

**9**

Detections With Rule  
Logic Updated

**11**

Detection Priorities  
Updated

**7**

Detections RETIRED

# Hot New Detections Highlights

---

- **Suspicious Process - Notepad Launching CMD or PowerShell via RDP (High - MDR)**  
This detection identifies Notepad.exe Spawning CMD or Powershell child process in an RDP Session. This technique is used by malicious actors for post-exploitation activities.
- **Suspicious Service - Execution of a Service in a Shared Drive (High- MDR)**  
This detection identifies the execution of a service in a shared drive. Malicious actors has been observed copying and executing malicious DLL and executable files in a shared drive in order to maintain persistence.
- **Suspicious Process - Possible Gootloader Malware (High - MDR)**  
This detection identifies a JavaScript file being run from a Temp or Download directory. The JavaScript file name contains key words that has been identified to be used in Gootloader family of malware. Gootloader utilizes Search Engine Optimization (SEO) poisoning to ensure potential victims navigate to compromised sites to download malicious payloads.
- **Attacker Technique: Renamed EWSPProxy in Non-Standard Location (High - MDR)**  
This detection identifies the execution of a renamed copy of the HP Embedded Web Server tool 'EWSPProxy'. This technique is used by malicious actors for network scanning. Threat actors has also been observed using a renamed version of 'EWSPProxy' to evade detection.
- **Attacker Technique: Renamed AnyDesk Binary in Non-Standard Location (High - MDR)**  
This detection identifies the execution of a renamed copy of the Remote Desktop Utility 'AnyDesk'. This technique is used by malicious actors to evade detection and prevent the blocking of this utility using the name of the process.
- **Suspicious Process: A Single Character Executable in Root Intel Directory (High - MDR)**  
This detection identified the execution of a single character executable file under a directory "Intel". The Intel folder is where various Intel graphic drivers used to be stored. Threat Actors have abused this folder location to drop malicious binaries.

# Hot New Detections Highlights

---

- **Attacker Technique - Windows Backup Admin Saves Backup to Remote ProgramData (Medium - MDR)**

This detection identifies the Windows Backup Admin utility being used to create backups to remote ProgramData Directory. Malicious Actors were observed creating this backups to include sensitive files including NTDS.dit, and later extract credentials.
- **Suspicious Authentication - MS Office 365 Cloud Service - "Impossible Travel" Activity (Medium - Customer)**

This detection identifies an "Impossible Travel" anomaly from an Office 365 Cloud Service user. An "Impossible Travel" activity is an authentication anomaly wherein a user tried to login from two different countries within a period of time that is much faster than the actual time a user can travel between those countries. When such activity happens, it is an indication that the user has been compromised.
- **Suspicious Authentication - Multiple Bad Password Login Failure From A Remote Host (Medium - MDR)**

"This detection identifies several or multiple failed authentications due to wrong password, from a single host to multiple hosts within a very short period of time. (10 failed logins to multiple hosts within 20 seconds). This behavior could be an indication of a Brute Force or Password Spraying attack."
- **Suspicious Process - Net Start Outputs Running Services to tmp File (Medium - MDR)**

This detection identifies the windows command line utility Net with an argument Start listing running Windows services and saving the output to a .tmp file in Temp Folder. Malicious Actors may use the output to target which Security Applications to terminate or use for post-exploitation activity.
- **Suspicious Web Request - Possible CrushFTP (CVE-2024-4040) Exploitation (Medium - MDR)**

This detection identifies a Suspicious Web Request to a server hosting CrushFTP. The suspicious request targets a known vulnerability (CVE-2024-4040) that allows for remote file read and authentication bypass on the Server.
- **User Behavior - Multiple User Account Was Disabled (Medium - Customer)**

Multiple User account has been disabled. This event generates when multiple user or computer object is disabled on domain controllers, member servers, and workstations within the specified threshold.
- **WebShell: IIS Launching Discovery Commands (Medium - MDR)**

This detection identifies suspicious host discovery commands launched by webserver processes. This may be indicative of a web shell. Threat actors may try to gather information about registered local system services.



# Hot New Detections Highlights

---

- **AWS CloudTrail: AWS API calls From Low cost VPN providers (Low - Customer)**  
This detection identifies AWS API calls performed from a Low Cost VPN provider.
- **Endpoint Visibility - Linux Auditd Compatibility Mode Requires String Output Format (Low - Customer)**  
This detection identifies when one or more of the Linux hosts in your environment is impacted by an auditd issue that causes events in binary format to be corrupted. This issue was first observed in auditd 3.1.1. Hosts that report this issue will not be able to send process start logs to the Insight Platform, which inhibits InsightIDR's ability to detect malicious activity on the endpoint.
- **Suspicious Process: Outdated CrushFTP.exe process (Low - Customer)**  
This purpose of this detection is to identify the execution of an old CrushFTP process "CrushFTP.exe" with a creation time older than April 2024. CrushFTP is a file transfer tool that allows enterprises to manage file transfer.
- **Suspicious Process: Use of WinSCP to transfer files (Low - Customer)**  
This detection identifies the use of the Windows Secure Copy (WinSCP) tool. WinSCP is a free and open-source file manager that allows for the transfer of files between client computers and remote servers. Threat actors has been observed using this utility for data exfiltration.

# Workshops & Webinars

# Useful Resources

## IVM & IDR Resources

[Rapid7 Status](#)

[Managed Services Resources](#)

[Rapid7 Workshops](#)

[Insight IDR Overview](#)

[Insight IDR Event Sources](#)

[SQL Queries](#)

[Rapid7 IVM API Examples](#)

[False Positive Investigations](#)

[Responding to Emergent Threats](#)

[Using Rapid7 Insight Agent and InsightVM Scan Assistant in Tandem](#)

## News & Helpful Links

[Ongoing Malvertising Campaign leads to Ransomware](#)

[Microsoft Token theft playbook](#)

[Velociraptor 0.7.2 Release](#)

[The Business of Cybersecurity Ownership](#)

[USF College of Engineering Presents Rapid7 With 2024 Corporate Impact Award](#)

[7 Rapid Questions with #77 Ray Bourque!](#)

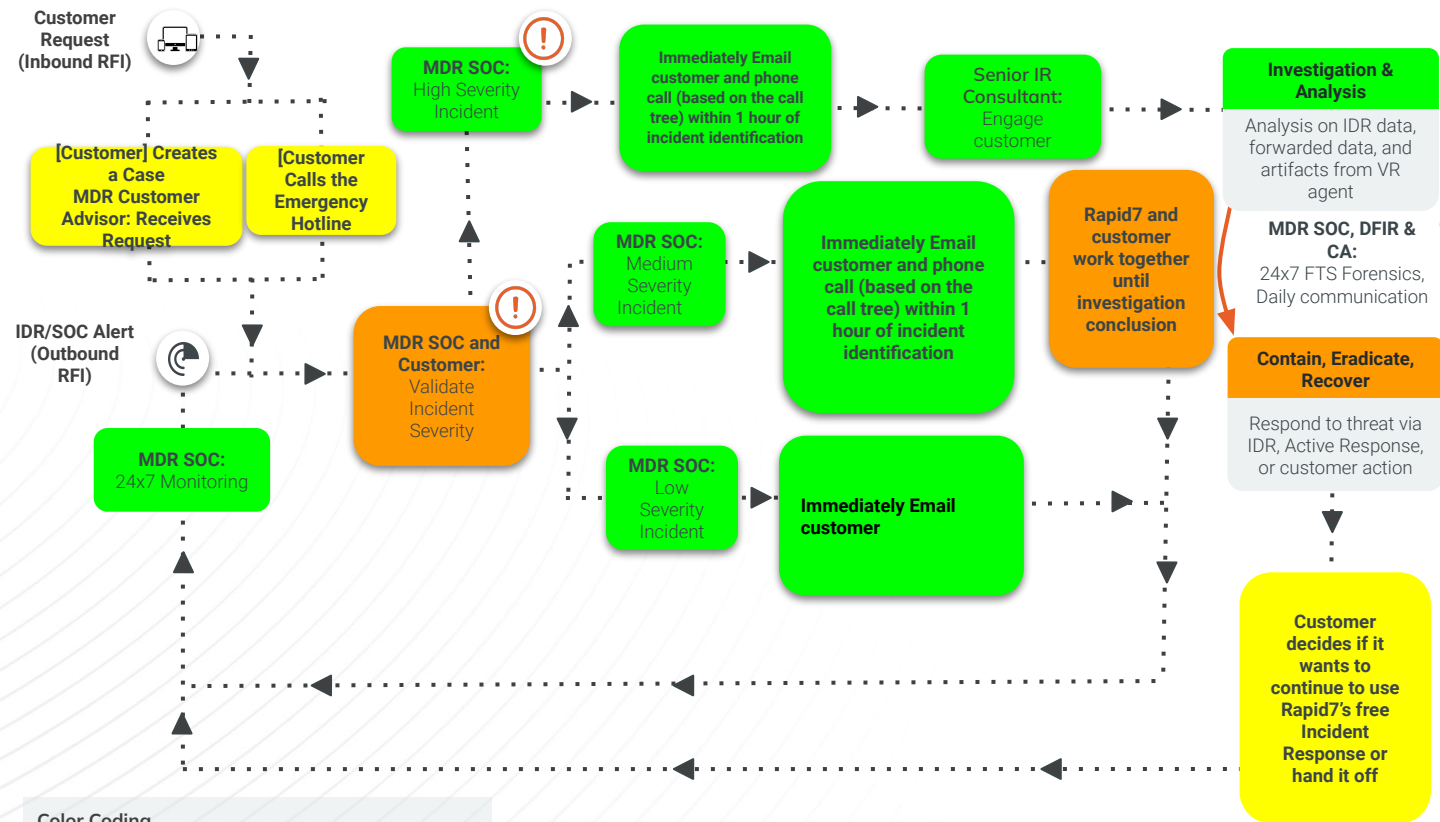
[Why The External Attack Surface Matters](#)

## Events and Recordings

- [Rapid7 Take Command 2024 Cybersecurity Summit](#): May 21st
- [RSA Conference](#): May 6th-9th
- [SANS Ransomware Summit 2023](#): May 31st
- [Gartner Security & Risk Management Summit, National Harbor, MD](#): June 3rd-5th
- [Black Hat, Las Vegas, NV](#): August 3rd-8th
- [Evanta CISO Executive Summit Chicago](#): May 14th

# Appendix - Informational

# MDR Investigation Workflow



**Color Coding**  
 Customer Responsibility  
 Shared Responsibility  
 Rapid7's Responsibility

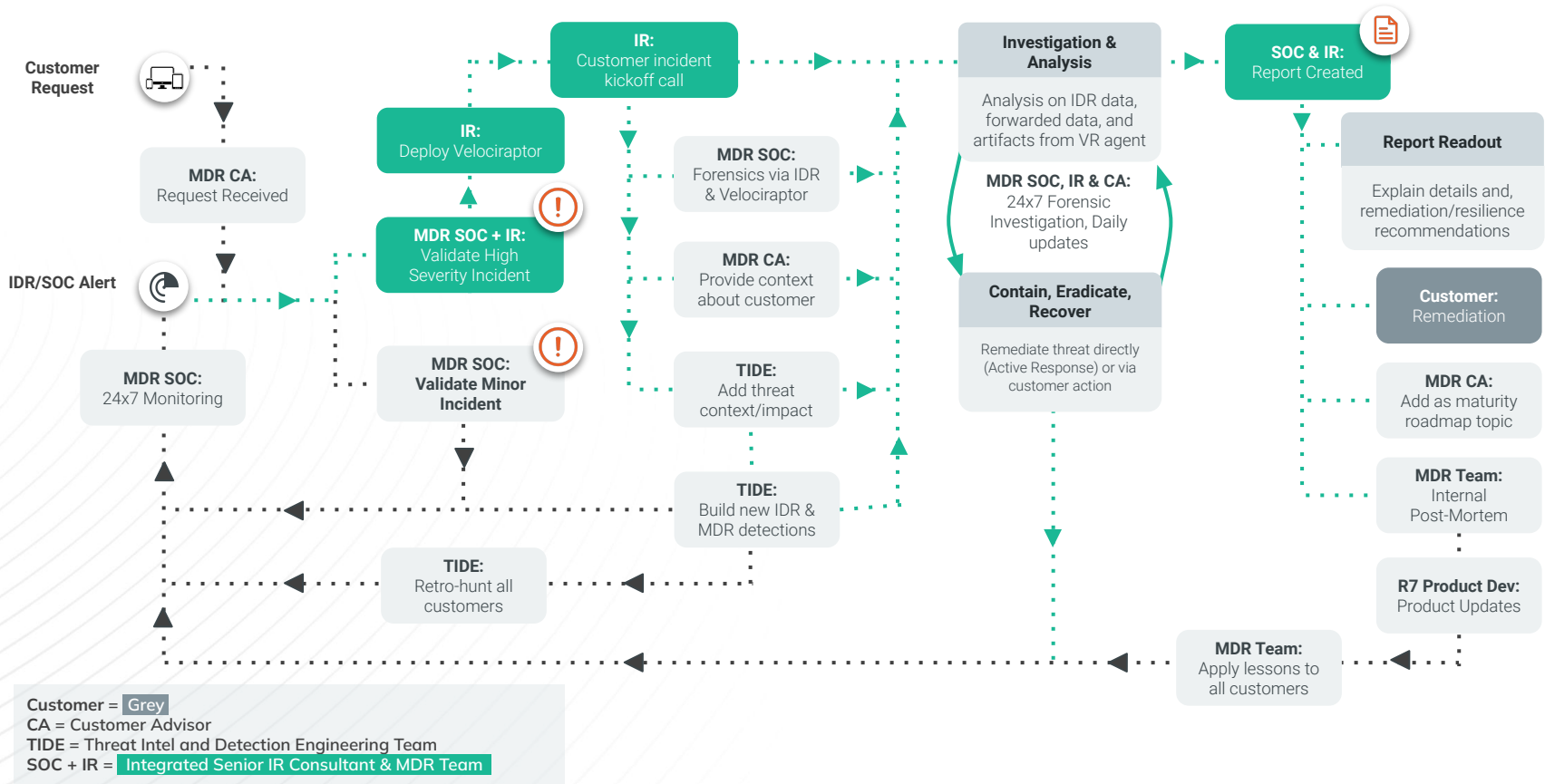
**Legend**

**MDR Hotline**  
 24x7 Emergency Line  
 +1 844-777-7637  
 MDR@rapid7.com

**Call Tree - Customer**

**Rapid7 Non-Emergency Contacts**  
  
 CA:  
  
 CSM:

# High Severity Incident Workflow



# MDR Pre-Penetration Test Recommendations

## Planning for a Successful Offensive Test

We recommend organizations perform a structured offensive test at least once a year. Offensive testing can provide valuable insights for defensive practitioners, identifying potential gaps in detection and coverage. We welcome the opportunity to partner with you to identify blind spots in coverage or capabilities and ultimately improve our detection and response abilities so we can improve your security.

To get the most out of your testing, we recommend you contact your Customer Advisor, who can be a valuable resource to partner with before, during, and after testing. You and your Customer Advisor can proactively prepare without having to share the dates of your test with us. This preparation is essential on an ongoing basis to ensure optimal visibility into your environment. While it may seem like notifying your Customer Advisor is 'giving away the answers to the test,' they will only share your plans with the MDR SOC if you prefer.

Your Customer Advisor will partner with you to review the following and ensure you get the most value from your test:

1. [Insight Agent Health](#)
2. [Configuration and deployment of Event Sources](#)
3. [Alert responsibility](#)
4. The scope and expectations of the MDR Service's response
5. Patch low hanging fruit (ETR, CISA KEV)

You can plan and execute offensive tests in many different ways, depending on your objectives and available testing resources. The MDR SOC's response can vary depending on the type of testing you have performed. In some cases, an offensive tester only intends to validate the preventative controls of an organization and, if this is the case, the tester may limit the scope to initial access and discovery activities. Understanding the intention of the test is important in evaluating the response.

If you also intend to test the detection capabilities of your organization (and, by extension, our MDR service), please consider the following:

- Your test should include as many steps in the Cyber Kill Chain as possible - from initial access to persistence, privilege escalation, and lateral movement. Performing isolated 'suspicious actions' is no substitute for a fully scoped offensive test and may provide you with an inaccurate depiction of the MDR service's response to a real-world threat.

More Information: <https://docs.rapid7.com/services/penetration-tests/>

# MVM Pre-Penetration Test Recommendations

## Planning for a Successful Offensive Test

We recommend organizations perform a structured offensive test at least once a year. Offensive testing can provide valuable insights for defensive practitioners, identifying potential gaps in detection and coverage. We welcome the opportunity to partner with you to identify blind spots in coverage or capabilities and ultimately improve your patch response abilities so we can help improve your security.

To get the most out of your testing, we recommend you contact your Customer Advisor, who can be a valuable resource to partner with before, during, and after testing. You and your Customer Advisor can proactively prepare without having to share the dates of your test. This preparation is essential on an ongoing basis to ensure optimal defensive posturing in your environment.

Your Customer Advisor will partner with you to review the following and ensure you get the most value from your test:

- External Vulnerability Audit
- Rapid7 Emergent Threat Audit
- CISA Known Exploited Vulnerability Audit
- Malware Kits Audit
- Exploitable Vulnerability Audit
- Default Credentials
- After Action Mitigations

If you also intend to test the detection capabilities of your organization, please consider the following:

- Your test should include as many steps in the Cyber Kill Chain as possible - from initial access to persistence, privilege escalation, and lateral movement. Performing isolated 'suspicious actions' is no substitute for a fully scoped offensive test and may provide you with an inaccurate depiction of your response to a real-world threat.

More Information: <https://docs.rapid7.com/services/penetration-tests/>