



MDR vs. The Inevitable

Managed Detection and
Response by Rapid7



Data breaches are so frequent, they've been normalized.

They show up on the nightly news. They're called "inevitable." So the real question is: how well do you respond?

In this eBook you'll find some real life examples of common threats handled by the Rapid7 Managed Detection and Response (MDR) team on behalf of our customers. We invite you to check out the speed and accuracy with which we identify, contain, and respond to malicious actors. According to IBM, it takes an average of 287 days to identify a breach and about 80 to contain it. You don't have that kind of time with the types of attackers you'll read about here.

It takes an average of 204 days to identify a breach and about 73 days to contain it.

IBM, "Cost of a Data Breach" report, 2023

You'll see other differences too. Rapid7 takes detection and response end-to-end. Most do not. You'll also learn about the comprehensive, security-posture boosting Incident Reports we deliver to customers.



If a breach is inevitable, you're smart to imagine it will be a formidable one."

Everybody needs **24x7x365** **detection and response**

Attacks are sophisticated and relentless, and state-backed groups have especially been having a field day. Hackers don't work 9 to 5 and in your time zone, so neither can your security team: everybody needs a 24x7x365 SOC. Standing one up requires highly skilled, specialized security experts. A big ask in a cybersecurity job market with 0% unemployment. Let's be honest, few could do it even with a blank check.

By 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today.

Gartner, 2023 Market Guide for Managed Detection and Response Services

By 2025, more than half of all businesses are expected to turn to a MDR service: an end-to-end, turnkey solution, providing threat detection, incident validation, and response.

What's behind that major shift? It's the understanding that going it alone can be a cost prohibitive exercise and that your team will be subject to knowledge gaps, talent shortages, and potential burnout. Instead, extending your own SOC with the expertise and tools of a cybersecurity partner means your team is free to look at the bigger picture, without the day to day struggles of managing a 24-hour global SOC.

This extended SOC idea isn't a product. It's a philosophical shift in the way in-house cybersecurity teams work alongside their security partners to a brand new approach. It leans proactive, controlling your exposure with joint, extended operations. Coupling this forward thinking approach with round the clock needs of a modern SOC, it's a solution to both the cybersecurity talent shortage and staying ahead of attackers and secure from a breach.

Timelines take you inside our always-on MDR SOC

Later on in this eBook, you'll find timelines labeled by industry, threat actor, criticality, and other considerations you may want to know. But don't be fooled, these attacks can happen to any organization, in any vertical, at any time.

You'll see how quickly Rapid7 MDR gets to the who-what-when-where-why with a 3x faster MTTD and MTTR than most teams do on their own. You'll see the work of our Customer Advisors, practitioners with strong technical expertise tasked with knowing your environment and security goals as well as you do. They guide security maturation, and can help with board, executive, and CISO security advisorship.

You'll also see how thoroughly we report out incidents with in-depth remediations and mitigation recommendations. Customers need more than quick notification emails when something happens – they need analysis and answers, not just the highlights and metrics.

But first, a little bit about how Rapid7's MDR extends your SOC capabilities from day one.



What you can't see is just as important

At Rapid7 our Digital Forensics and Incident Response (DFIR) team and our MDR SOC work hand in hand to create an integrated team of Detection and Response experts. If an incident investigation appears major, analysts simply (and literally) swivel their chairs and tap Senior Incident Response consultants and DFIR practitioners on the shoulder. They learn from each other daily.

For every single incident, Rapid7's TIDE Team (Threat Intelligence and Detections Engineering) is right there too. They keep a close eye on new and emerging threats, and develop new detections in real time. This allows us to stay on top of the latest tactics, techniques, and procedures threat actors are taking, and find them in all customers' environments as they emerge. The TIDE team allows us to add granularity, reduce noise, and avoid recurrency over time.

Rapid7's sprawling detections library includes threat intelligence from our open-source communities, advanced attack surface mapping, proprietary machine learning, research projects, real-world follow-the-sun SOC experience, and 4.8+ trillion weekly security events observed across our detection and response platform.

If you get overwhelmed at the thought of hiring to meet all of that, then you understand the need for extending your SOC capabilities.

**4.8+ trillion weekly security
events observed across our
detection and response platform**



You can go through the MDR motions,

or choose 549% ROI

Rapid7 commissioned Forrester Consulting to study the Total Economic Impact™ (TEI) of our MDR. The assessment? A 549% ROI over three years, with a three-month payback, a 70% reduction to your cyber risk profile, and a 90% reduction in the likelihood of a major breach.

The fact is, you can have high expectations when you partner with us:

- You hear about true threats only, so you can pinpoint and act with confidence
- We take initial countermeasures to paralyze the attacker for you
- You get 24x7x365 SOC coverage and analysts that own your outcomes



**A breach may be inevitable, but your
success with just any MDR isn't."**

**The following timelines are real and fairly
common threats handled by Rapid7 MDR
on behalf of our customers.**

**Attacker's linger, and
dwell times keep going
up. You can't allow
that with the kind of
intrusions you see here.**

Compromise, Investigation, and Response Timeline

Healthcare Attack Breakdown

Threat

Solarmarker
Jupyter infoStealer
Yellow Cockatoo

Type

Persistence -
Run Key Added by Reg.exe

Severity

High

Alert Priority:

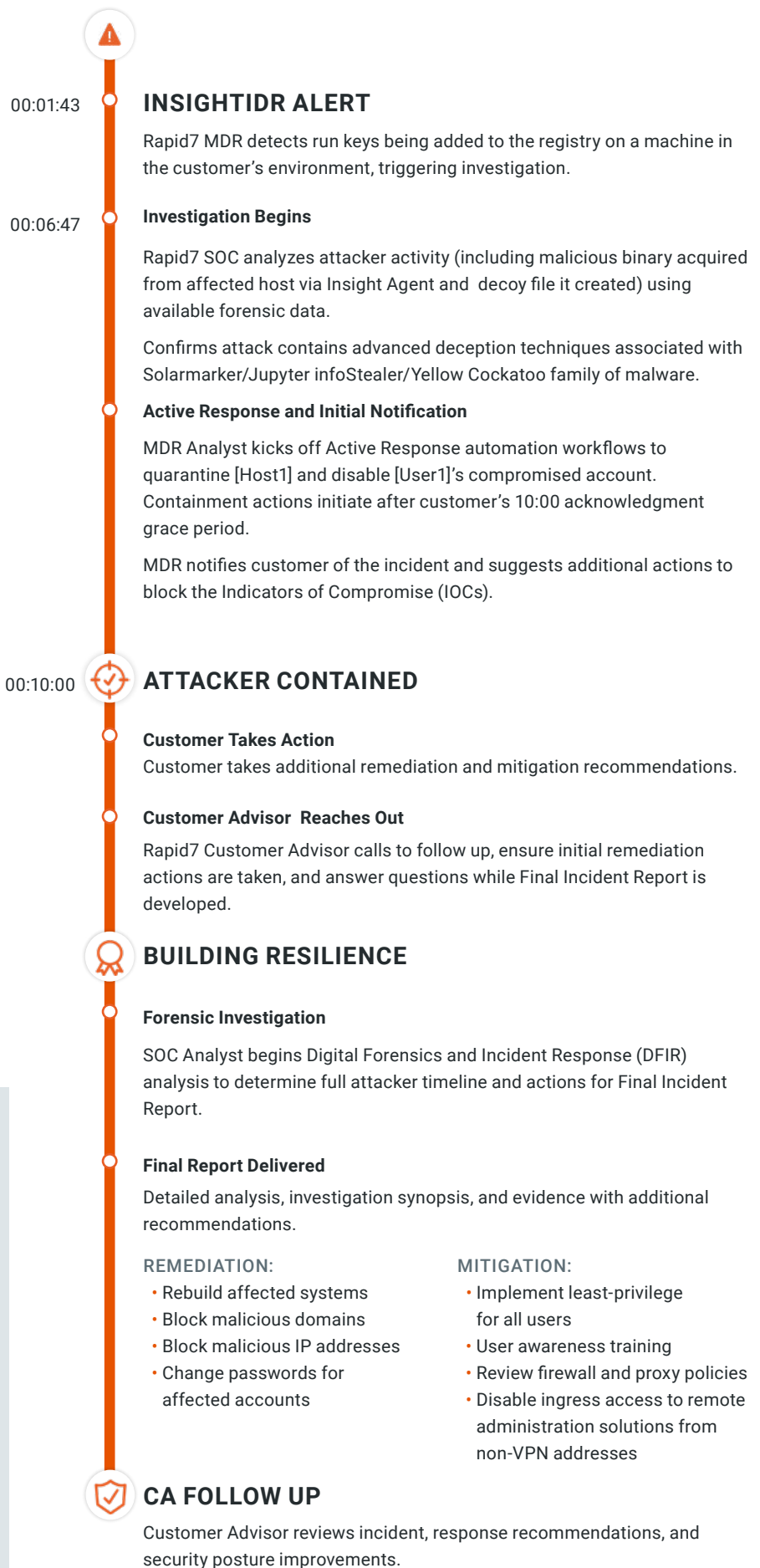
Medium

Event Source

Process Start Activity (Insight Agent)

Attacker Activity

- [User1] searches "employee handbook of pharmaceutical employees" on Edge browser, unknowingly downloads malicious binary masquerading as a document file.
- User executes binary on [Host1], which renamed itself and created a decoy file in an attempt to hide in the filesystem, in addition to creating a Windows registry run key to establish persistence on the host.
- Executable file attempts to communicate with unknown Command and Control (C2) to post information about the asset and exfiltrate more data.



Compromise, Investigation, and Response Timeline

Energy and Utilities Attack Breakdown

Threat

Remnant of malware persistence mechanism / Cryptominer

Type

Suspicious Service - Powershell

Severity

Low

Alert Priority

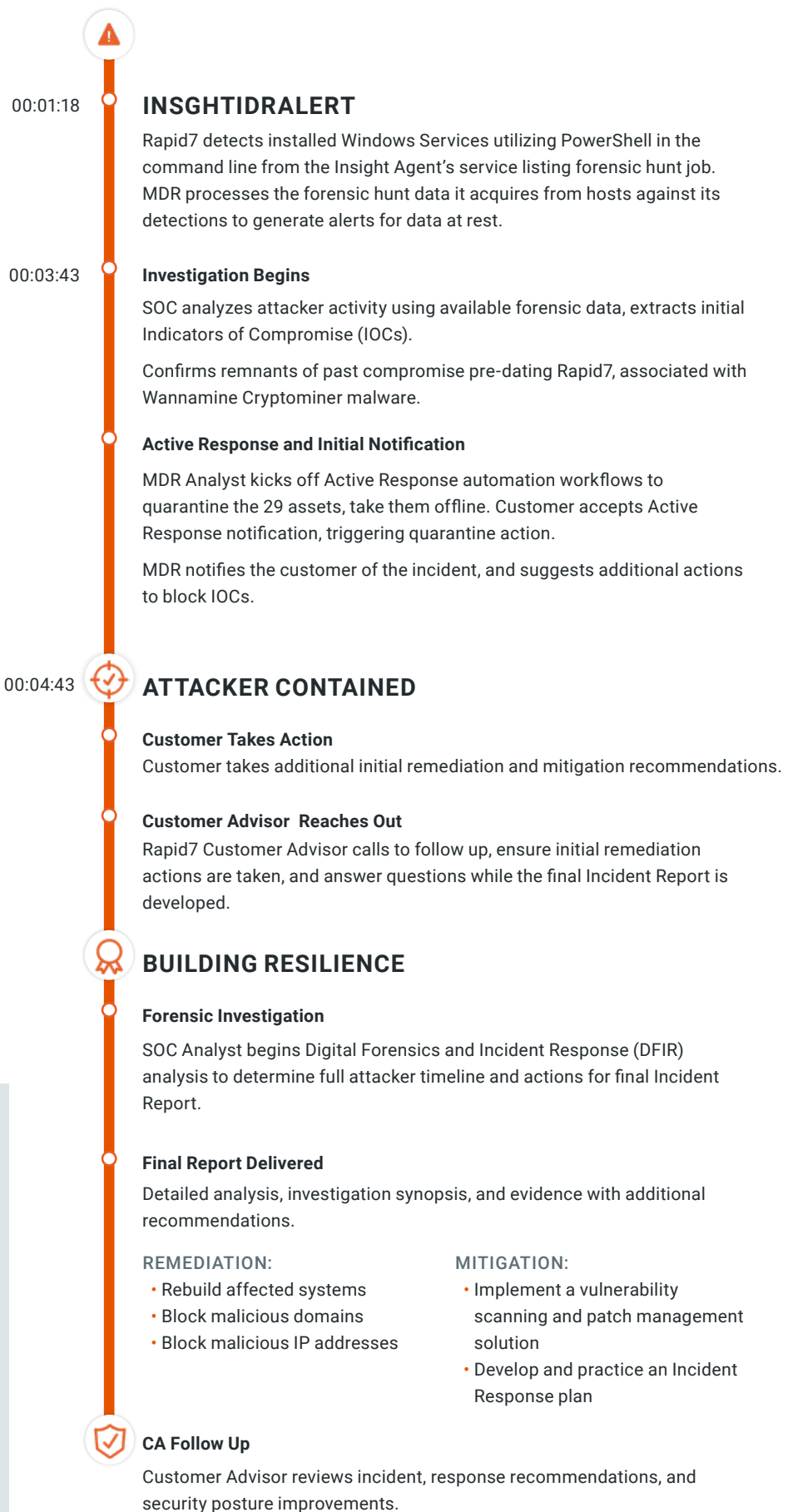
High

Event Source

Forensic Hunt Data

Attacker Activity

- Newly-installed Insight Agent detects 29 assets affected by remnants of past compromise.
- Randomly named scheduled services attempted to reach a remote command and control server to download, execute files no longer being served there.
- Wannamine used Eternal Blue exploit targeting vulnerability in SMBv1, WMI for remote code execution, and ADMIN\$ to move laterally in the customers environment.



Compromise, Investigation, and Response Timeline

Legal Attack Breakdown

Threat

SocGholish Malware Family

Type

Suspicious Process - WScript
Starts File from within Archive

Severity

Medium

Alert Priority

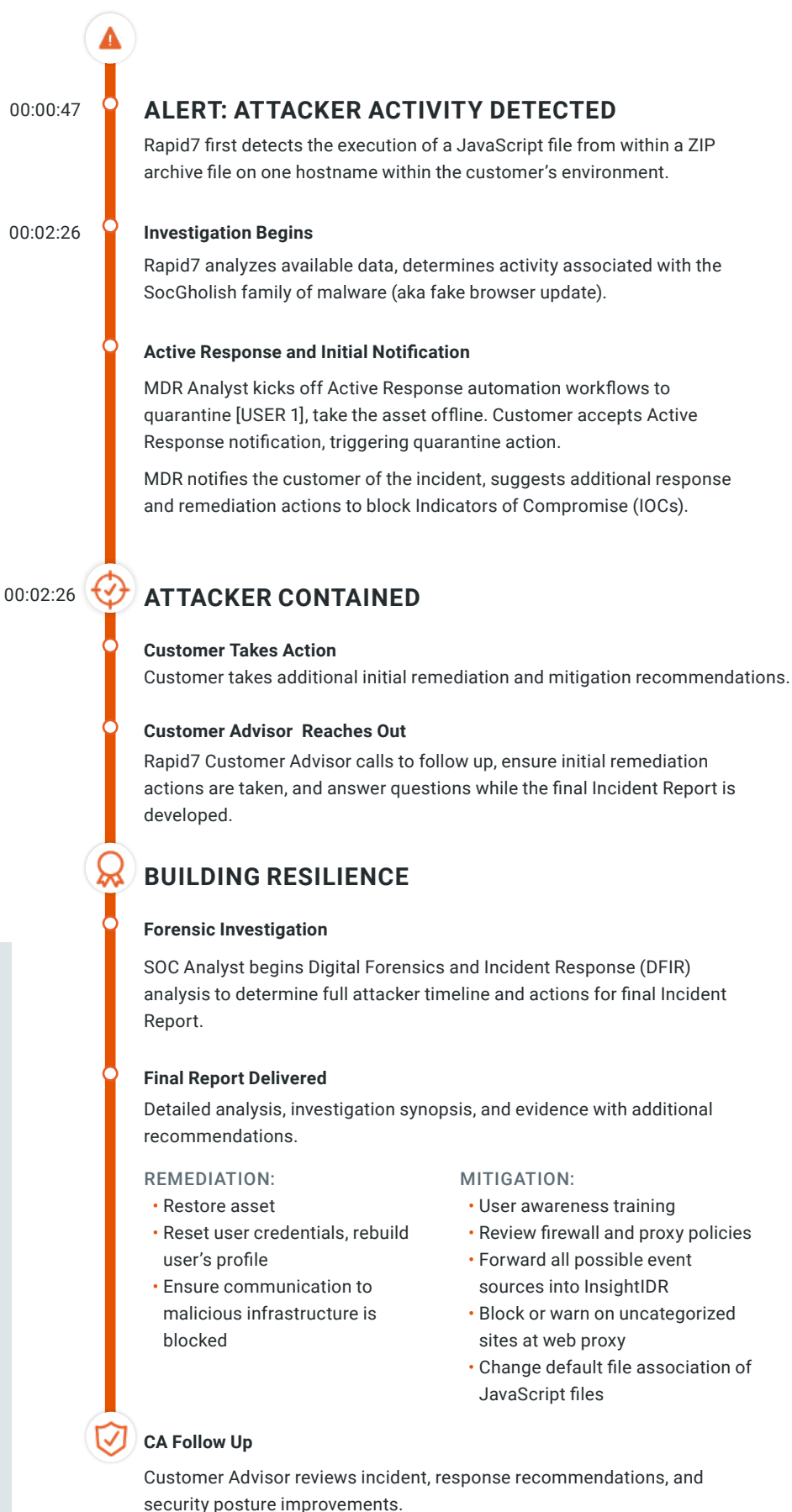
High

Event Source

Process Start Activity

Attacker Activity

- [USER 1] working on legal cases used Chrome browser to visit a legitimate website compromised by malicious embedded JavaScript functions.
- Embedded JavaScript file loaded pop-up, invited user to update browser by downloading ZIP archive containing JavaScript file.
- Once executed, Javascript file communicated with Command and Control (C2) to download and execute a malicious payload, to fingerprint the asset, user, cached password, domains controllers, and trusted domains and output the results to a file at the root of [USER 1]'s %temp% directory to stage the host for subsequent exploitation.



Compromise, Investigation, and Response Timeline

Human Resources/ Finance Attack Breakdown

Threat

More_Eggs Malware Family

Type

Suspicious Process - Potential
MSXSL Proxy Execution

Severity

High

Alert Priority:

High

Event Source

Process Start Activity

Attacker Activity

- [USER 1], senior corporate recruiter, went to a website that was legitimate, but infected, and unwittingly downloaded a fake resume. The resume opened and looked legitimate while spawning two-stage malicious activity in the background.
- The More_eggs family of malware ultimately bypassed application white-listing controls and established a backdoor to run a javascript loader that attempts to download the final stage payload of the malware and inject it into memory. The goal? Deploy ransomware.
- Rapid7 disrupted before it could successfully run.

00:00:52



ALERT: ATTACKER ACTIVITY DETECTED

Rapid7 detects a Potential MSXSL Proxy Execution running on a host in the customer's environment.

00:22:35

Investigation Begins

Rapid7 analyzes available forensic data, extracts initial Indicators of Compromise (IOCs) for the customer to block, and determines activity is associated with More_eggs family of malware.

Active Response and Initial Notification

MDR Analyst kicks off Active Response automation workflows to quarantine asset, take it offline. Customer accepts Active Response notification, triggering quarantine action.

MDR notifies the customer of the incident, suggests additional response and remediation actions to block the Indicators of Compromise (IOCs).

00:26:45



ATTACKER CONTAINED

Customer Takes Action

Customer takes additional remediation and mitigation recommendations.

Customer Advisor Reaches Out

Rapid7 Customer Advisor calls to follow up, ensure initial remediation actions are taken, and answer questions while the final Incident Report is developed.



BUILDING RESILIENCE

Forensic Investigation

SOC Analyst begins Digital Forensics and Incident Response (DFIR) analysis to determine full attacker timeline and actions for final Incident Report.

Final Report Delivered

Detailed analysis, investigation synopsis, and evidence with additional recommendations.

REMEDIATION:

- Rebuild affected systems
- Block malicious domains
- Change passwords for affected accounts

MITIGATION:

- User awareness training
- Block outgoing connections for regsvr32
- Review firewall and proxy policies
- Forward all possible event sources to InsightIDR

CA Follow Up

Customer Advisor reviews incident, response recommendations, and security posture improvements.



Compromise, Investigation, and Response Timeline

Transportation Attack Breakdown

Threat

RedLine InfoStealer Malware Family

Type

Suspicious Process - WScript Starts
File From Within Archive

Severity

Medium

Alert Priority

High

Event Source

Process Start Activity

Attacker Activity

- [User1], a customer Service Specialist, received a phishing email with an attached .zip archive containing a malicious JavaScript file masquerading as a billing invoice.
- When the user opened the "invoice" from the archive, Windows Script Host (wscript.exe), executed the JavaScript file. The JavaScript code reached out to a RedLine InfoStealer Command and Control (C2) to download and execute a second stage payload to fingerprint the host, attempt to harvest credentials from local FTP software clients, and collect information about installed applications. Following the enumeration, the payload attempted to upload it to the C2 for subsequent exploitation.

00:00:09



ALERT: ATTACKER ACTIVITY DETECTED

Rapid7 first detects the execution of a JavaScript file from within a ZIP archive file on one hostname within the customer's environment.

00:08:52

Investigation Begins

Rapid7 SOC analyzes attacker activity using available forensic data. Analyst confirms this attack resulted from a phishing email received by the user, and was associated with the Redline InfoStealer family of malware.

Analyst also identified communication attempts to Command and Control (C2) server within current session data acquired via IDR agent forensic job.

Active Response and Initial Notification

MDR Analyst kicks off Active Response automation workflows to quarantine the asset. Customer accepts Active Response notification, triggering quarantine action.

MDR notifies the customer of the incident, suggests additional response and remediation actions to block Indicators of Compromise (IOCs).

00:29:55



ATTACKER CONTAINED

Customer Takes Action

Customer takes additional remediation and mitigation recommendations.

Customer Advisor Reaches Out

Rapid7 Customer Advisor calls to follow up, ensure initial remediation actions are taken, and answer questions while the final Incident Report is developed.



BUILDING RESILIENCE

Forensic Investigation

SOC Analyst begins Digital Forensics and Incident Response (DFIR) analysis to determine full attacker timeline and actions for final Incident Report.

Final Report Delivered

Detailed analysis, investigation synopsis, and evidence with additional recommendations.

REMEDIATION:

- Rebuild affected systems
- Block Malicious domains
- Block malicious ip addresses
- Terminate malicious processes
- Quarantine network traffic from affected endpoints
- Block the affected accounts
- Change passwords for affected accounts
- Identify and remove malicious email from all inboxes
- Block sender's email address

MITIGATION:

- Update frequently targeted applications
- Use an application sandbox to run frequently targeted applications
- User awareness training
- Implement an anti-phishing solution
- Review firewall and proxy policies
- Block executable files at web proxy
- Block or warn on uncategorized sites at the web proxy

CA Follow Up

Customer Advisor reviews incident, response recommendations, and security posture improvements.



Compromise, Investigation, and Response Timeline

Healthcare Attack Breakdown

Threat

Citrix / BazarLoader / CobaltStrike
Malware Family

Type

Suspicious Process - Malicious
Hash on Asset

Severity

Medium

Alert Priority

High

Event Source

Process Start Activity

Attacker Activity

- While the customer was in onboarding, the attacker initiated a RDP session connecting to the target hostname. Two days later the attacker used a Citrix remote-access tool to remotely connect to a vulnerable host and execute malicious files directly on the asset.

00:00:11



ALERT: ATTACKER ACTIVITY DETECTED

Rapid7 MDR first detects suspicious wuaucrt.exe process launching without standard argument. Malicious actors have been observed with this activity associated with Process Injection.

00:31:43

Investigation Begins

Rapid7 SOC analyzes attacker activity using available forensic data, extracting initial IOCs. Analyst confirms the activity was associated with the BazarLoader family of malware. BazarLoader is a malware stager used to download additional payloads for post-exploitation.

Rapid7 acquired the malicious files using the Insight Agent forensic acquisition capability and determined that the malware reached out to the Command and Control (C2) to post information about the asset and exfiltrate more data and were associated with the BazarLoader_ Printnightmare family of malware.

Rapid7 MDR ultimately determined that the threat actor's goal was to load a Cobalt Strike beacon into memory for post-exploitation and likely stage deployment of ransomware.

Active Response and Initial Notification

MDR Analyst kicks off Active Response automation workflows to quarantine the asset. Customer accepts the Active Response notification, triggering quarantine action.

MDR notifies customers of the incident, suggests additional response and remediation actions to block Indicators of Compromise (IOCs).

00:48:32



ATTACKER CONTAINED

Customer Takes Action

Customer takes additional remediation and mitigation recommendations.

Customer Advisor Reaches Out

Rapid7 Customer Advisor calls to follow up, ensure initial remediation actions are taken, and answer questions while the final Incident Report is developed.



BUILDING RESILIENCE

Forensic Investigation

SOC Analyst begins Digital Forensics and Incident Response (DFIR) analysis to determine full attacker timeline and actions for Final Incident Report.

Final Report Delivered

Detailed analysis, investigation synopsis, and evidence with additional recommendations.

REMEDIATION:

- Rebuild affected systems
- Block malicious domains
- Block malicious IP addresses
- Terminate malicious processes
- Change passwords for affected accounts
- Identify and remove malicious email from all inboxes
- Block sender's email address

MITIGATION:

- User awareness training
- Implement an anti-phishing solution
- Block outgoing connections for regsvr32
- Review firewall and proxy policies
- Block executable files at web proxy
- Block or warn on uncategorized sites at the web proxy



CA Follow Up

Customer Advisor reviews incident, response recommendations, and security posture improvements.

Compromise, Investigation, and Response Timeline

Healthcare Attack Breakdown

Threat

Intrusion Attempts

Type

Attacker Technique - CertUtil With
URLCache Flag

Severity

High

Alert Priority:

High

Event Source

Process Start Activity

Attacker Activity

- Executed a ping command on an internal IP address
- Downloaded a payload from an external URL
- Executed Base64 PowerShell commands to download additional payload to collect information about the asset and send it to a Command and Control (C2) server
- Executed a suspicious UPX packed binary with a Base64 encoded argument to download additional files
- Attempted and failed lateral movement with authentication attempts to 27 assets as local account `administrator`
- Download and execute a Windows privilege escalation tool.
- Maintained consistent firewall traffic from the asset to the C2.
- Created suspicious files associated with Maze ransomware that dated back to before the Rapid7 Insight Agent was deployed on the asset, suggesting that the asset was previously compromised and not patched accordingly.

00:02:34



ALERT: ATTACKER ACTIVITY DETECTED

Rapid7 MDR first identified the execution of suspicious PowerShell commands on [ASSET 1]. This specific technique is used by malicious actors to retrieve files hosted on a remote web server and write them to disk.

00:06:22

Investigation Begins

Rapid7 SOC reviewed all available forensic evidence from [ASSET 1] and determined that a malicious actor likely exploited a four year old remote code execution vulnerability (CVE-2017-9841) within the PHPUnit framework, commonly used by content management system (CMS) software.

Active Response and Initial Notification

MDR Analyst kicks off Active Response automation workflows to quarantine the asset. Customer accepts Active Response notification, triggering quarantine action.

MDR notifies the customer of the incident and suggests additional response and remediation actions to block the Indicators of Compromise (IOCs).

00:11:22



ATTACKER CONTAINED

Customer Takes Action

Customer takes additional remediation and mitigation recommendations.

Customer Advisor Reaches Out

Rapid7 Customer Advisor calls to follow up, ensure initial remediation actions are taken, and answer questions while Final Incident Report is developed.



BUILDING RESILIENCE

Forensic Investigation

SOC Analyst begins Digital Forensics and Incident Response (DFIR) analysis to determine full attacker timeline and actions for Final Incident Report.

Final Report Delivered

Detailed analysis, investigation synopsis, and evidence with additional recommendations.

REMEDIATION:

- Rebuild affected systems
- Block malicious domains
- Block malicious IP addresses

MITIGATION:

- Update frequently targeted applications
- Implement vulnerability scanning and patch management solution
- Implement application allowlisting for critical systems
- Disable credential caching on servers, workstations
- Restrict server internet access
- Segment the network based on data sensitivity, type
- Review firewall, proxy policies
- Patch vulnerable web servers
- Implement web application firewall
- Enable powershell script block logging on all systems
- Block executable files at web proxy
- Block or warn on uncategorized sites at web proxy
- Enable account audit logging on all systems



CA Follow Up

Customer Advisor reviews incident, response recommendations, and security posture improvements.

Compromise, Investigation, and Response Timeline

Engineering Attack Breakdown

Threat

Intrusion Attempts

Type

Account Compromise/Phishing/
Malicious Inbox Rules (Attacker
Technique - Suspicious Inbox
MoveToFolder Rule Created)

Severity

High

Alert Priority:

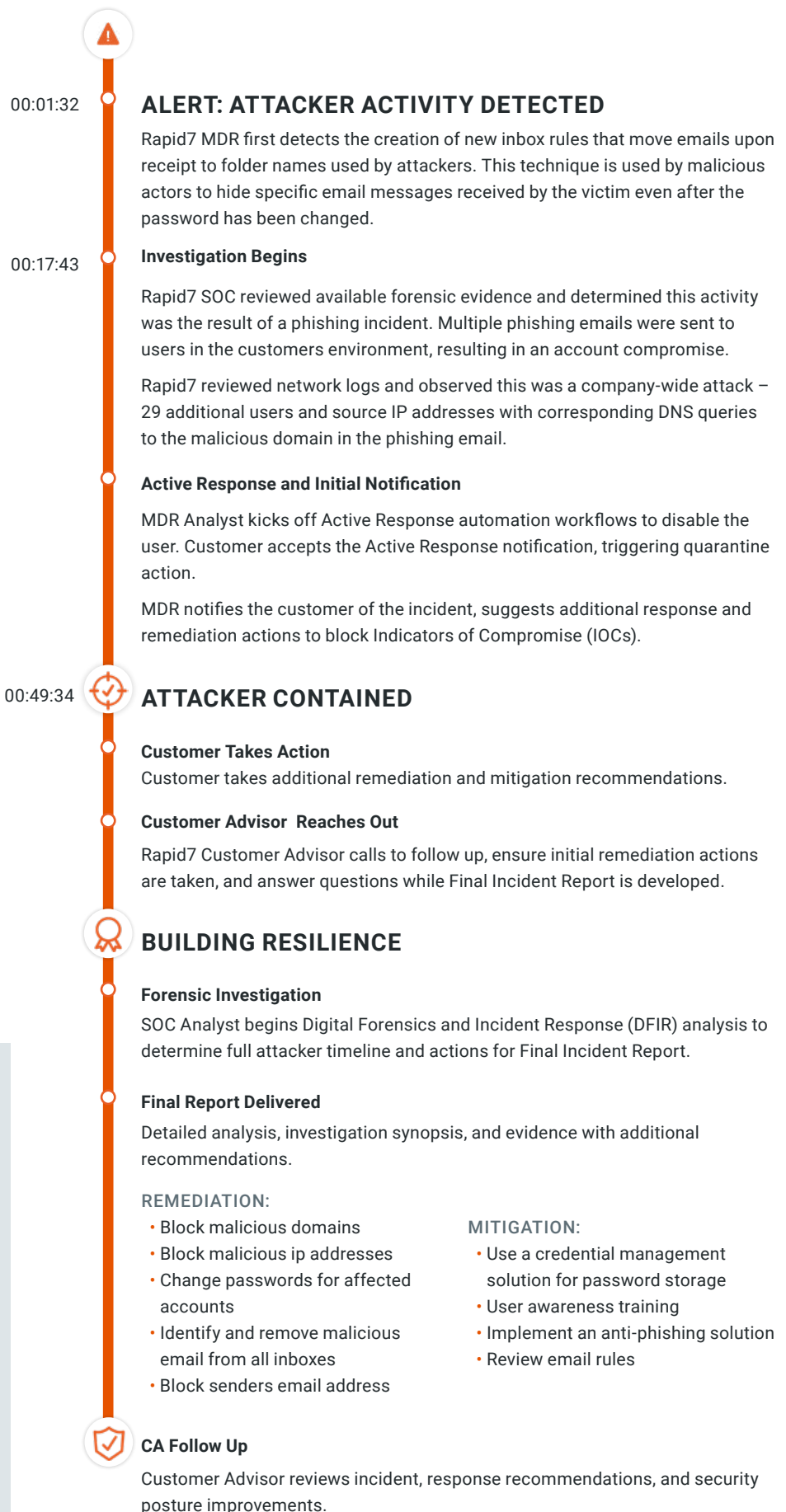
High

Event Source

Microsoft Office 365 (Cloud
Service Activity)

Attacker Activity

- [USER 1] received two phishing emails two days earlier - the first email contained a link to a credential harvesting page, second email contained a malicious PDF attachment.
- Once the attacker attained credentials to [User1]'s compromised user's email account, they created three inbox rules in an attempt to maintain access to other accounts associated with the victim email address. The rule moved all emails containing "payroll" or "paycheck" or "direct deposit" to the "RSS Subscriptions" folder and marked the emails in question as read.



Compromise, Investigation, and Response Timeline

Non-profit Attack Breakdown

Threat
Cloud/AWS Compromise

Type
Account Compromise

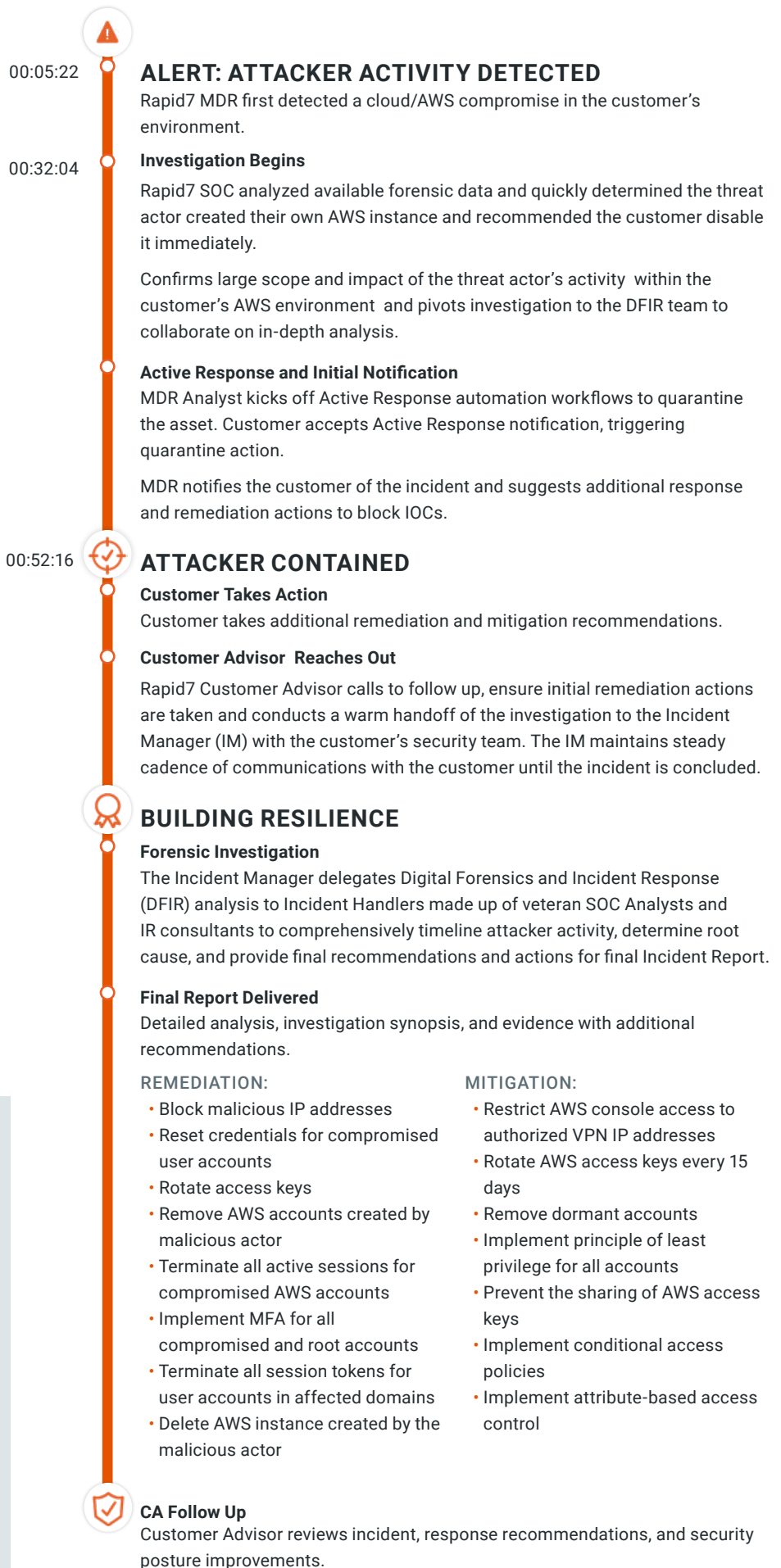
Severity
High

Alert Priority
High

Event Source
AWS Cloudtrail

Attacker Activity

A malicious actor compromised a customer's AWS environment when an AWS [Account 1] was enumerated and then compromised. The compromise of the original account led to a total four additional accounts compromised and the creation of eight new attacker accounts. Using the compromised and created accounts, the malicious actor was able to perform enumeration, create a new AWS instance, and harvest session tokens for nine domains.



Compromise, Investigation, and Response Timeline

Food and Hospitality Attack Breakdown

Threat

Malicious document - Emotet malware family

Type

Malicious Code (Malicious Document - Regsvr32 Spawned By Word, MSPub or Excel)

Severity

High

Alert Priority:

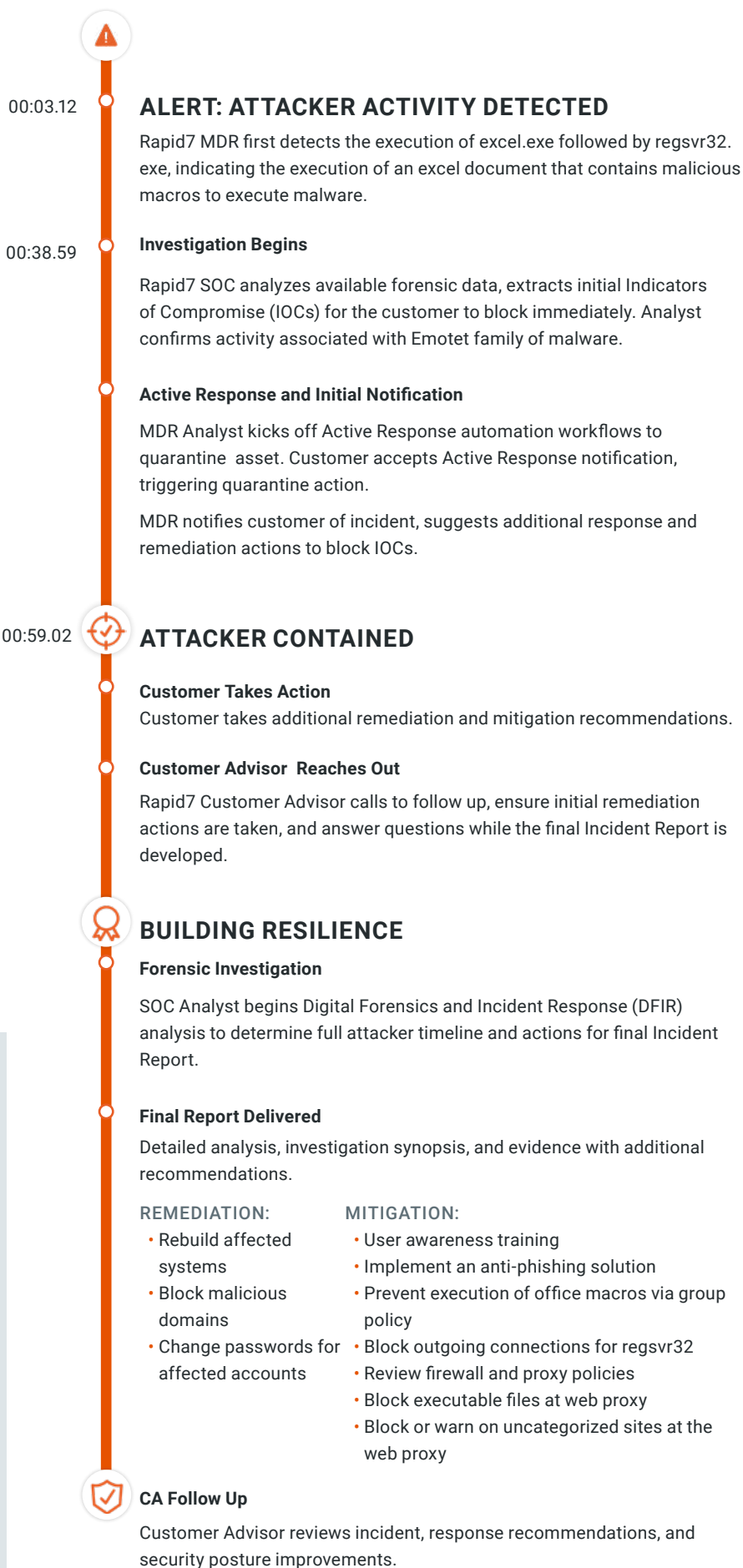
High

Event Source

Process Start Activity

Attacker Activity

- [User 1] received a phishing email containing a zip archive which contained a malicious Excel document.
- [User1] then interacted with the excel document which resulted in the execution of a malicious vb script. Web traffic evidence indicated attempted communication with four Command and Control (C2) servers to download multiple second stage DLL payloads and save them with an '.ocx' file extension. The script downloaded one .dll file successfully and attempted to execute it with regsvr32.exe. Forensic analysis of the .dll file and host based evidence indicated the attack chain was unsuccessful past this point.



Why it's not outsourcing: the right MDR service is a partner

Technology and transparency

Typical MDR services stay behind the curtain like the "Wizard of Oz." They won't give you access to their technology or provide you transparency into the SOC's operations. You see high-level metrics only, and few details into investigations, alerts, etc. unless you pay for basic level "data exploration" or "log search" capabilities. (We don't believe in wizards at all and think customers should be able to see everything.)

Rapid7 MDR: full access to InsightIDR, our unified SIEM and XDR. You see what we see. You can run your own investigations, create dashboards, run reports, and more. There's no additional cost.

Digital forensics and incident response

Typical MDR has a warranty for specific major breach events, such as Ransomware or Business Email Compromise. If you're compromised and you need to access Incident Response experts ASAP, you'll need to jump through hoops to make a claim, ensure you qualify for money, and then invoke your IR Retainer or contact an outside Breach Response firm, and you might still have to pay out of pocket anyways.

Rapid7 MDR: customers get unlimited DFIR for all incidents, regardless of time or complexity, until the work is done. We have expert DFIR teams all over the world: Australia, Ireland, and the United States. You'll get the same treatment as if you had an IR Retainer without paying a cent more.

MDRP and greater control of the external attack surface

It can be unbelievably challenging to navigate the entirety of the clear, deep, and dark web for potential threats to your networks. Without the specialized skills to triage external threat alerts you could be chasing your tail for days on false positives while legit threats slip through. Even if your SOC could identify and triage threats, it can be challenging to effectively act on insights with point solutions that don't weed out the noise.

Rapid7 MDR: customers gain broad and deep external attack surface monitoring from professionals, marrying our advanced threat intelligence technology with deep expertise in identifying threats early and breaking the kill chain before a breach occurs.

**Rapid7 MDR is an
employer-of-choice
with a 95% retention
rate over 3 years**



Pod model and outcome responsibility

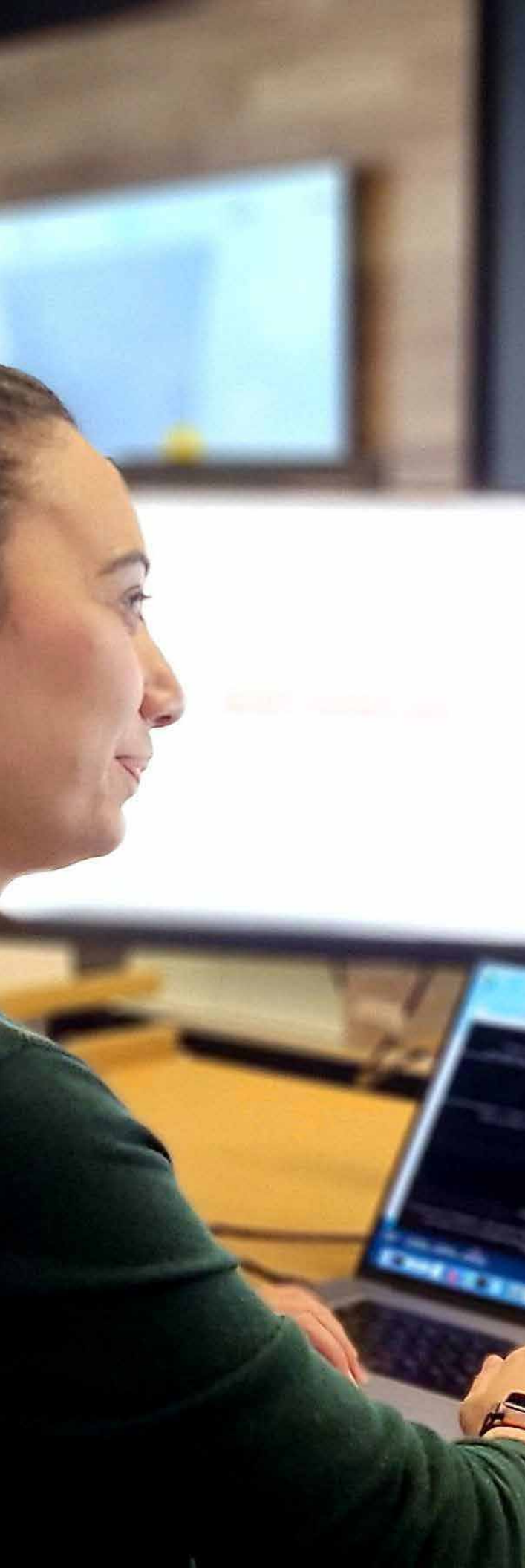
Typical MDR has one giant, shift-scheduling SOC, working all hours of the night, including holidays. The pool of analysts is arranged in tiers. They review pools of alerts. The system misses familiarity with your particular environment, ownership of outcomes, and oversight and advocacy from a lead.

Rapid7 MDR: our analysts take it personally when one of their customers is attacked. Our “follow the sun” pod model allows for all analysts to have a 9-5 shift with seamless handoffs, with each pod owning the responsibility for customer outcomes. While the skills gap is very real, Rapid7 MDR is an employer-of-choice with a 95%+ retention rate over 3 years. Seasoned practitioners lead alert triage, investigate on your behalf, help you remediate and mitigate future attacks, and best of all, remove false positives so you’re only notified when there’s an actual incident.

A real extension of your team

Typical MDR will offer you a contact person who will relay SOC info to you, send additional log info in an excel doc, check health scores, and answer high level questions.

Rapid7 MDR: we expect your named Customer Advisor to act as an extension of your security team. In addition to walking you through the context and details of any attack, you’ll get CISO-level leadership and strategic insights tailored to your security program. They’re more than a point of contact for your service – their strategic guidance will help you build cyber resilience and strengthen your program.



Reporting

With typical MDR, an analyst fills out a reporting template with little context or details, and sends it to you with minimal instructions to “respond” to the threat. That’s it. That’s the report.

Rapid7 MDR: what typical MDR providers send is what we call an “incident notification”, and we don’t believe that’s adequate to do anything other than notify your team of an incident. When there’s an incident, Rapid7 customers receive an exhaustive report on the investigation with root cause analysis, raw details, and an array of resilience recommendations. You’ll also get monthly service and threat reports, and proprietary Threat Intelligence reports so you’re the first to know about emerging threats as they’re discovered.

Data and retention

If you don’t want your data purged after 30-90 days, a typical MDR will charge you.

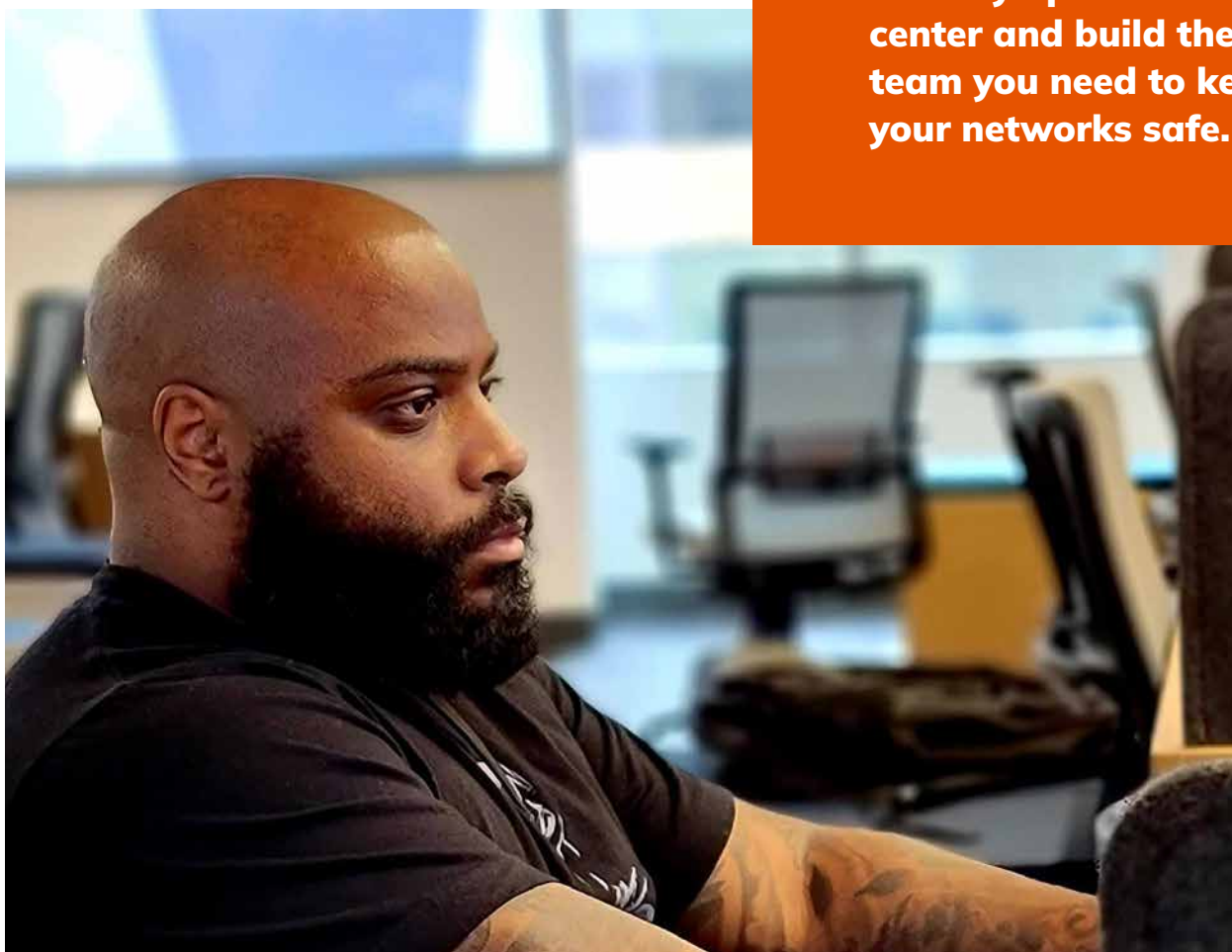
Rapid7 MDR: we offer unlimited data ingestion and 13 months storage by default. MDR analysts need this for hypothesis-driven and retro-threat hunting in your environment. And you might need it for compliance.

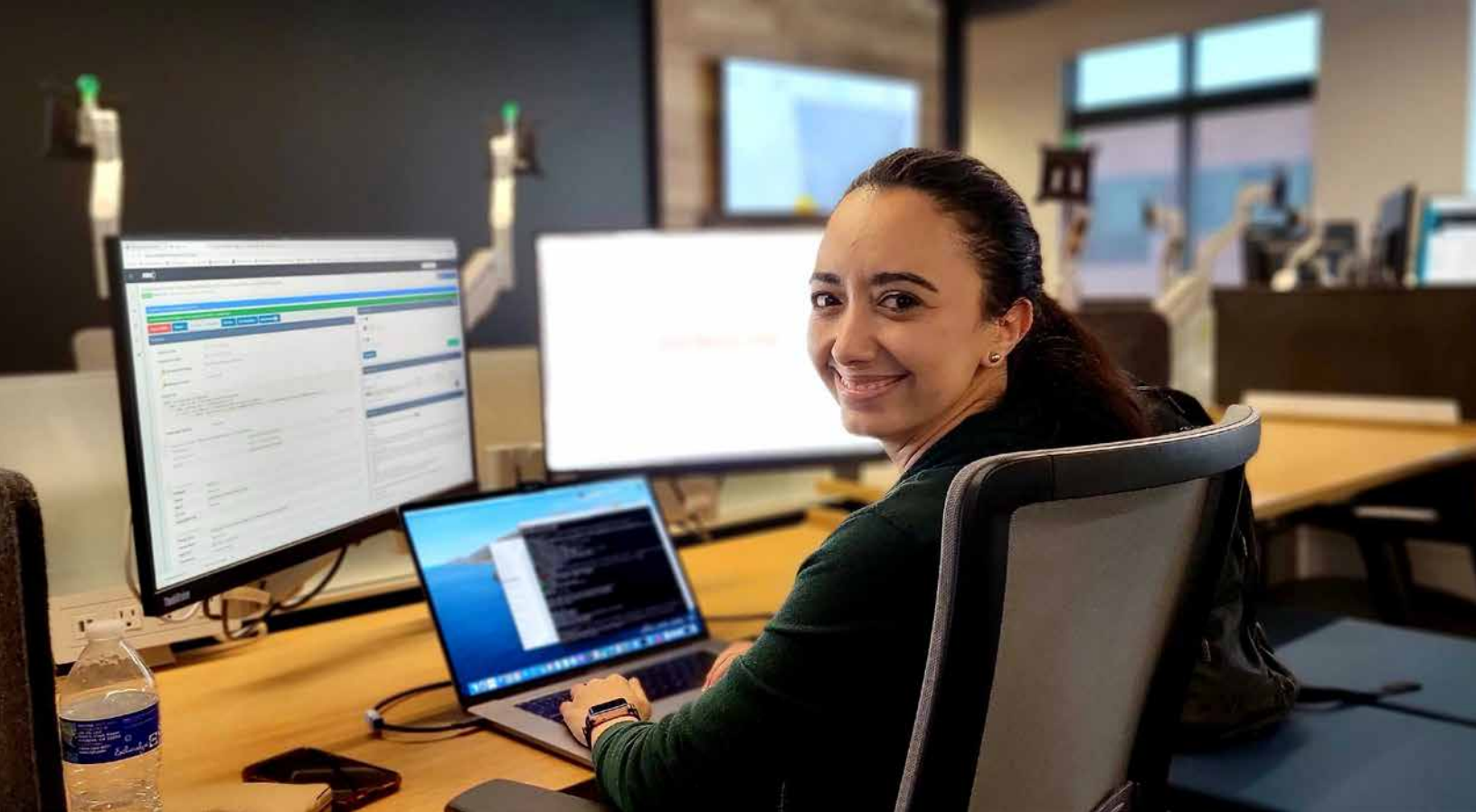
Command Your Attack Surface with Managed Threat Complete

Threats are inevitable, breaches are not. At Rapid7, we have built an industry-leading vulnerability management and detection & response platform which our managed services teams deploy to great effectiveness. With Managed Threat Complete, you will receive **unlimited vulnerability scanning, unlimited incident response, digital risk protection, unlimited data ingestion, and many more features**, all through a transparent operation and at a clear price. There is no stronger way to extend your security operations center and build the team you need to keep your networks safe.

If you're ready to take command of your attack surface, we're ready for you.

There is no stronger way to extend your security operations center and build the team you need to keep your networks safe.





About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research—using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more Rapid7 MDR, speak to an expert: www.rapid7.com