The Essential Guide to Automating Malware Investigations

How Can Security Analysts Perform More Effective Malware Investigations at Scale?

Enhancing your security automation and response capabilities across multiple platforms while tending to large amounts of threat investigations is anything but easy. However, not doing so requires a dependency on manual processes, increasing incident investigation time and the overall risk of malware infections. To prepare for the next inevitable attack, SOC teams must continuously look for ways to improve their postincident activity processes.

The impetus for automating malware investigations came out of conversations with our customers on the challenges they faced on a day-to-day basis when responding to malware alerts.

Malware Incident Response Challenges

Rudimentary Automation for Malware Investigation

Many SecOps teams had limited automation deployed regarding malware. They might use basic rule-based automated actions provided by their EDR tools. These quick actions can be a time saver for a finite set of actions but are not scalable across multiple systems, nor do they truly tap into the full potential of automation. They might use a threat intel management (TIM) tool for indicator extraction and enrichment. But beyond that, there was no automation, and analysts were on their own investigating alerts or manually executing their security operating procedures.

Investigations Were Still Largely Manual

Some customers had started to integrate some tools into their investigation process. For example, they had Active Directory integrated to provide context on assets, and analysts could trigger response through the layout. Analysts had access to malware analysis tools, but fetching the file and detonating it was still done manually.

From talking to customers, we identified many repetitive activities that could save their organization days per month in human effort.

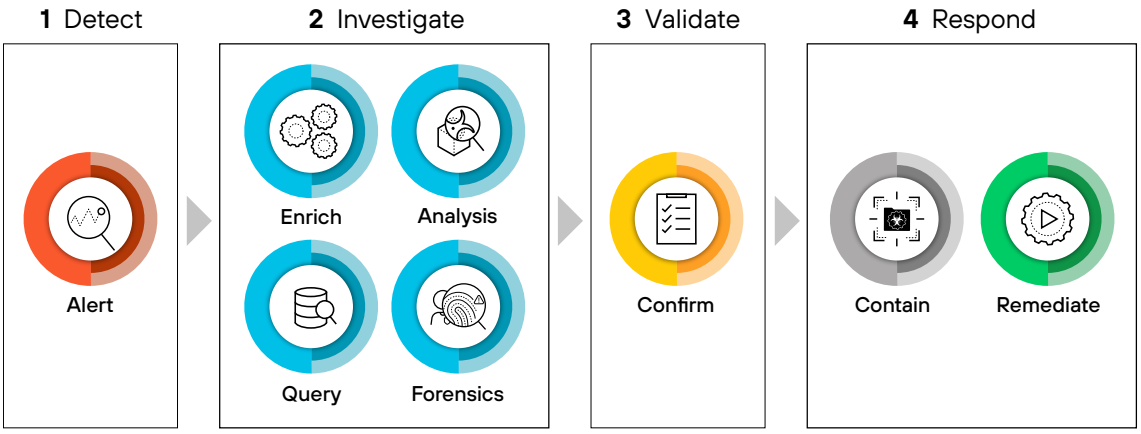

Figure 1: The malware investigation and response process

Malware Analysis and Forensics: Detect, Investigate, and Validate

The investigation process is the most time-intensive step when responding to malware alerts. Of course, an analyst must investigate whether a file or process is bad, but what are the detailed questions they should ask and what supporting evidence should they collect?

Can the evidence that needs to be collected answer questions such as:

- Is there evidence of persistence (scheduled job, registry entry, startup folder, new service, etc.)?
- Is there evidence of evasion or tampering (service stop, process kills, etc.)?
- Is there evidence of lateral movement (network connections, file share enumeration, etc.)?
- Is there evidence of PowerShell or command-line abuse?
- Are the associated files digitally signed?

As part of malware analysis, if an analyst is using a sandbox to detonate any malware, they will need to review the malware report. They also need to know which users and/or departments are impacted.

During an investigation, it is critical to understand what is happening on the endpoint at the time the alert is detected rather than at a later point during the investigation. Sometimes, it can be minutes or even hours before an analyst looks at a detected alert, at which point the state of the endpoint is likely different. This can make the investigation challenging.

Containment and Remediation

Once the investigation is complete, the analyst will need to take action based on the results of the investigation. If the alert is a true positive, the analyst will want to take containment precautions to prevent the malware from spreading. These actions include pivoting to various systems and performing the actions manually. Best case, the analyst might have created a limited set of rule-based automated actions that fire when a specific condition is met.

Introducing the Malware Investigation and Response Content Pack

We wanted to help SecOps teams speed up investigations and deal with malware quickly by building automation into their incident response process. The Malware Investigation and Response Content Pack accelerates the investigation process for endpoint malware incidents and alerts by collecting evidence of malicious behaviors, searching telemetry data available through EDRs, and processing malware analysis reports through sandboxes. Incident layouts also include buttons to quickly trigger containment activities. Where automation ends, analysts have at their disposal all information—incident windows with rich data from EDR/XDR, sandboxes, threat intel feeds, user data, etc.—needed to facilitate investigation drill-down and integrated case management to manage their incidents.

Automated Data Collection and Enrichment

Evidence from endpoint security alerts are collected automatically, enriched by querying various threat intel platforms, to automatically populate the endpoint account. During this enrichment process, the playbook also checks for any MITRE techniques and maps them to the MITRE ATT&CK® framework. All this information can be viewed from the Investigation tab of the incident.

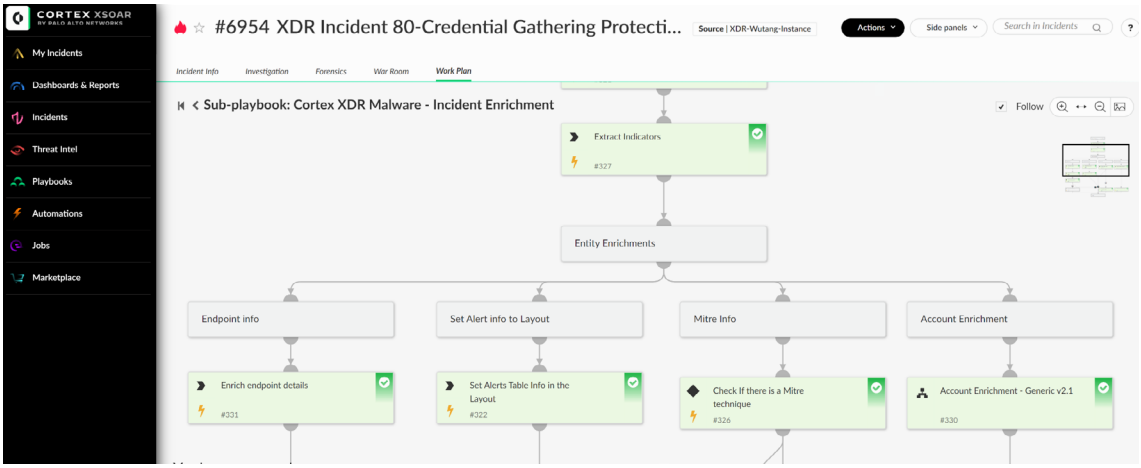

Figure 2: Sample of malware investigation playbook

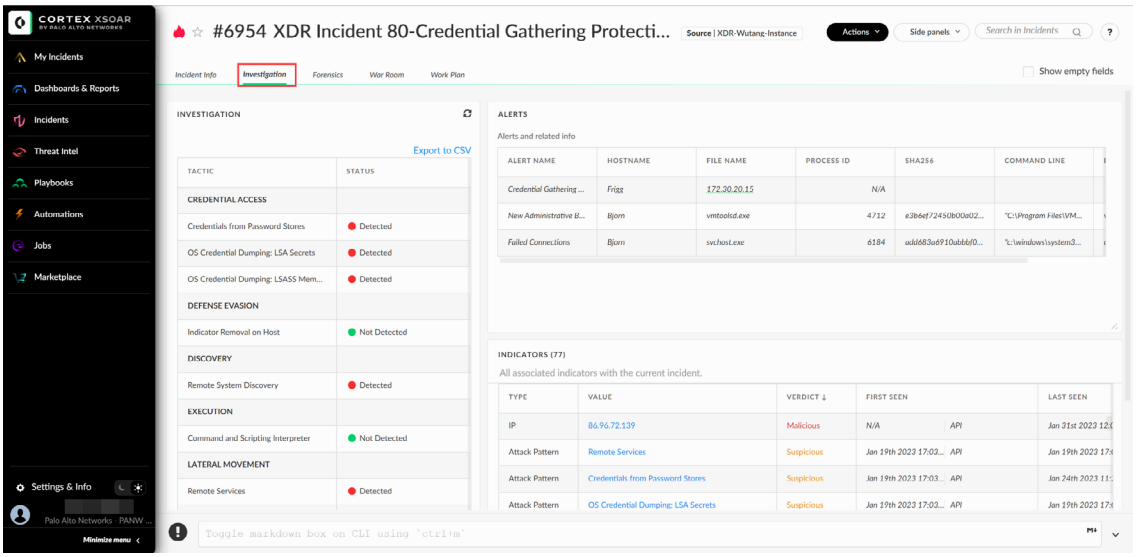

Figure 3: Investigation window with incident details

Endpoint and Account Enrichment

With this content pack, you can automatically retrieve information about active users on the impacted endpoints. For example, providing insight into the active user's department—whether they are in finance or engineering—enables the analyst to disable the user's account in the corresponding IdP as needed.

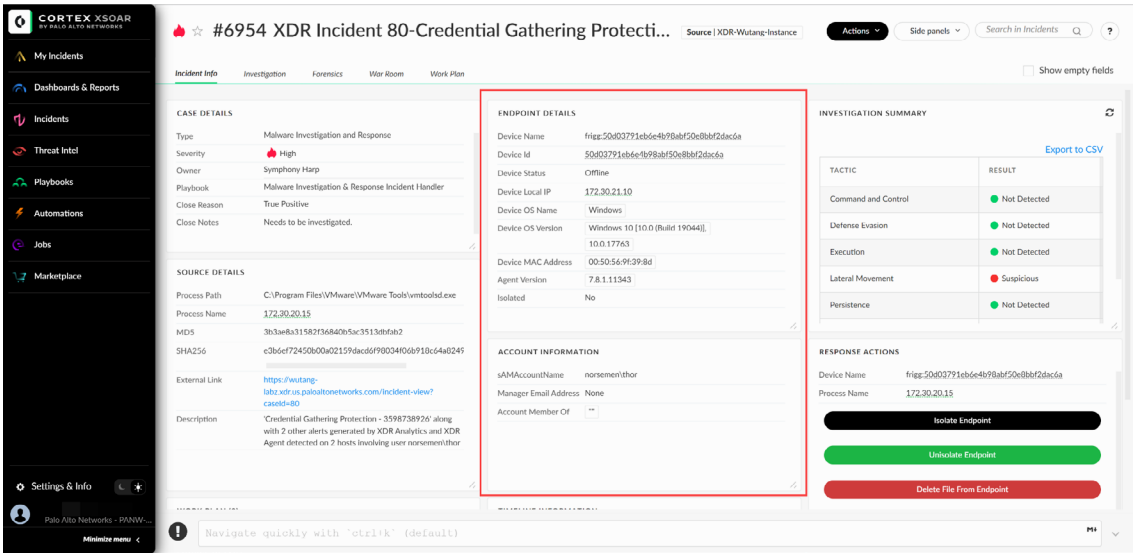

Figure 4: Account information details in incident view

Firewall Enrichment and Validation

Integrations with SIEMs and network security tools give more context to the threats in your organization. This provides valuable context regarding the severity of the threat and how widespread it is within your organization. For the list of SIEMs and network security tools we integrate with, please check out the Cortex Marketplace.

Malware Analysis

If you have a sandbox integrated with Cortex XSOAR® for malware analysis, the playbooks included in this pack will automatically retrieve the malware report if available. If a report is unavailable, the suspicious file will be retrieved using EDR and passed to the sandbox for detonation. The pack supports most sandboxes in the market. The report, when available, will be parsed, mapped to MITRE, and displayed in the incident layout.

For example, our integration with Palo Alto Networks WildFire®* allows analysts to retrieve submitted file information or automatically detonate files that are detected by the deployed EDR. The retrieved information allows the analyst to gain more insights on the alert by using the full sandbox analysis report or a quick view of the extracted IoCs, such as MITRE ATT&CK information, from the layout itself.

* Note: We also provide prebuilt integrations with other sandboxes such as Joe Security, CrowdStrike Falcon, Cuckoo, FortiSandbox, Triage, Malwation, Any.Run, etc. You will find the complete list in our Cortex Marketplace.

So, from one location, the analyst can drill down to get detailed information to aid in their investigation.

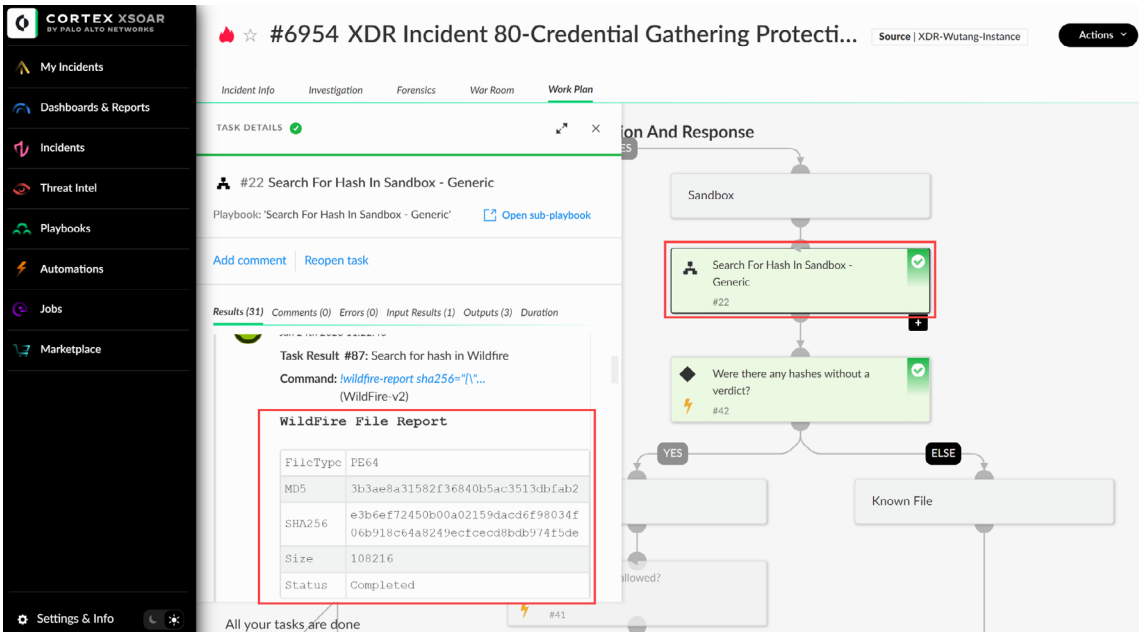

Figure 5: Drilled down details on WildFire indicator data

1 File Information

File Type	PE64
File Signer	
SHA-256	912d217d9f34121bc6150a2d7f22b49d2c876942653348c671f358ff58af0eba
SHA-1	74f28dd9b0da310d85f1931db2749a26a9a8ab02
MD5	ad99b6147cbff1c8ecce8ce44e742681
File Size	822272bytes
First Seen Timestamp	2020-02-26 03:06:28 UTC
Verdict	Benign
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains non-standard section names

Standard section names are defined by the compiler. Non-standard section names may indicate a packed or obfuscated PE file.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Contains a TLS section

Thread-local storage (TLS) is normally used to manage data in multithreaded applications. However, it can also allow execution of code outside of the expected entry point of a PE file.

Figure 6: WildFire file report—File Information and Static Analysis

3 Dynamic Analysis

3.1. VM1 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010)

3.1.1. Behavioral Summary

This sample was found to be **benign** on this virtual machine.

Behavior	Severity
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Sample is invalid or corrupted The sample is either corrupted or an invalid file type. It cannot be analyzed.	

Figure 7: WildFire file report—Dynamic Analysis

3.2. VM2 (Windows 10 x64, Flash 22, Adobe Reader 11, Office 2010)

3.2.1. Behavioral Summary

This sample was found to be **benign** on this virtual machine.

Behavior	Severity
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Started a process from a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Malware often runs executable content out of these folders to avoid detection, while legitimate applications are usually run out of the Windows, Windows system, or Program Files folders.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	
Opened a Command Prompt window Command Prompt is the built-in Windows command-line interface. While it is common for users to open Command Prompt windows, legitimate applications rarely do so.	
Crashed when loaded Compatibility issues and missing resources might cause legitimate applications to crash. However, malware also often crashes applications as a side-effect of attempting to exploit them, and may still be successful in spite of the crash.	

Figure 8: WildFire report—Behavioral Summary

3.2.3. Host Activity

Process Activity

Process Name - sample.exe

(command: C:\Users\Administrator\sample.exe)

Process Activity

Child Process	Action
C:\Windows\system32\cmd.exe	Create

Created Mutexes

Mutex Name
Local\SM0:3304:120:WilError_02
Local\SessionImmersiveColorMutex

Process Name - cmd.exe

(command: C:\Windows\system32\cmd.exe)

No activity recorded for this process.

Event Timeline

1 Created Process C:\Users\Administrator\sample.exe

2 Created Process C:\Windows\system32\cmd.exe

3 Created mutex Local\SM0:3304:120:WilError_02

4 Created mutex Local\SessionImmersiveColorMutex

Figure 9: WildFire report—Host Activity

Response: Containment and Remediation

Once the investigation is complete and it is determined that the alert is a true positive, the analyst will need to quickly take steps to prevent the malware from spreading. The layout for the malware incident type includes buttons to easily trigger endpoint isolation, file deletion, and kill process commands.

The analyst can also apply a tag on the primary indicator. It allows your XSOAR indicator management workflow to add the indicator to a deny list or allow list. For example, an EDR deny list or a firewall external dynamic list (EDL) tag can be added to block access across the environment. If the file is benign or a false positive, the analyst can apply the allow list tag to avoid repeated alerting.

For remediation, the playbook has a parameter to open a JIRA ServiceDesk or ServiceNow ticket so that the IT team knows to reimage the compromised endpoint or use the appropriate IT workflow your company has in place.

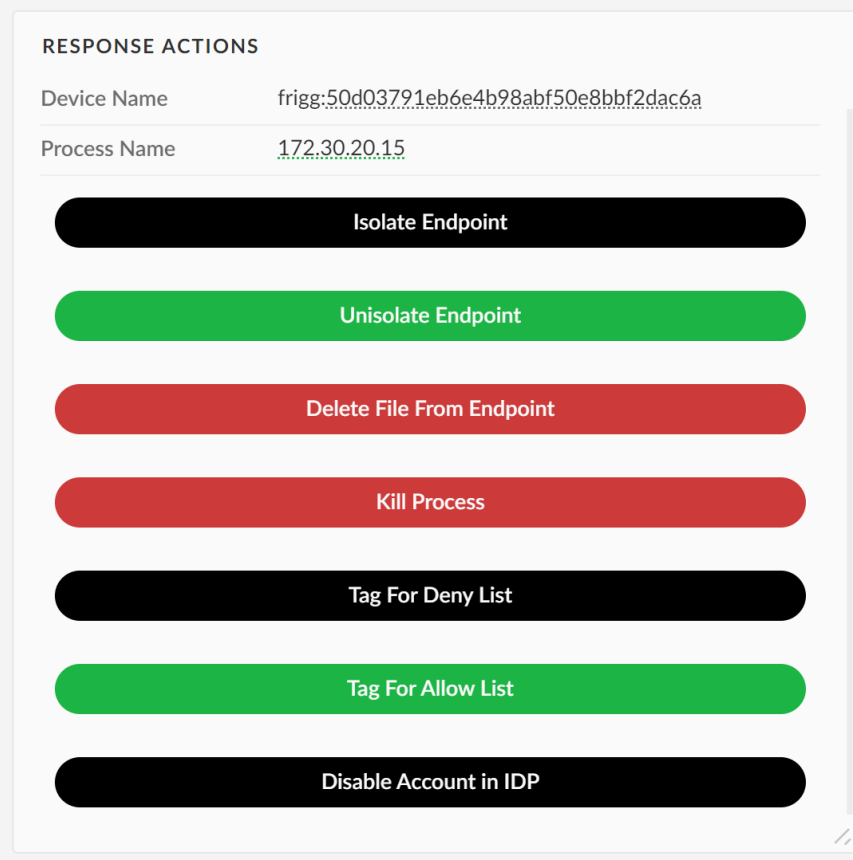

Figure 10: Remediation Action

Managing Service-Level Agreements (SLAs)

Security investigations are time sensitive. The longer the threat is uncontained, the greater the risk of exposure to the organization. With this pack, you can easily track and monitor triage, remediation, and containment SLAs.

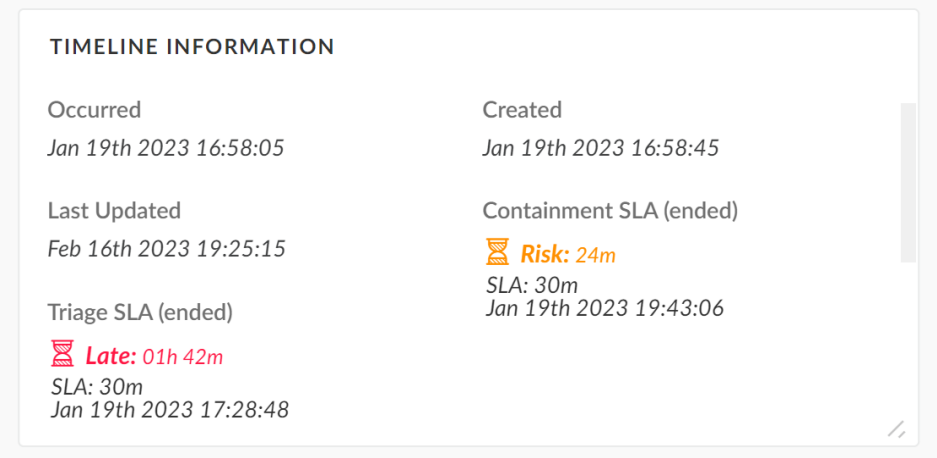

Figure 11: SLA section within the incident

An SLA dashboard also allows you to quickly filter your incident types based on severity so you can properly diagnose your SLAs.

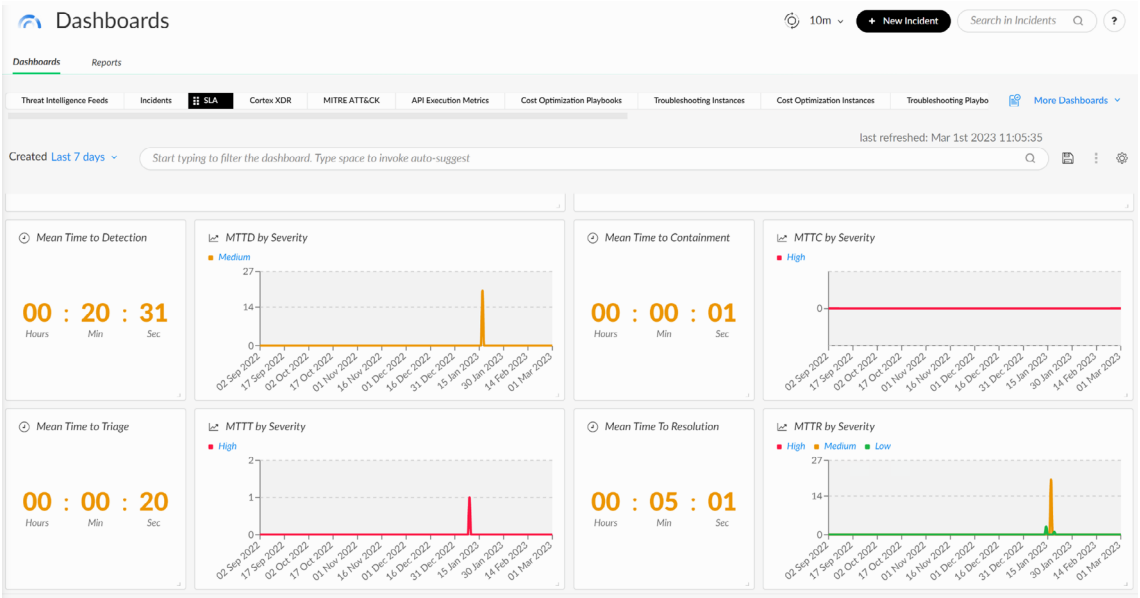

Figure 12: SLA dashboard

Assigning an Analyst to the Incident

To better manage workloads across your team, you can also assign an analyst to an incident based on their availability. Moreover, you may define if you would like to assign an on-call analyst using the playbook inputs.

Where to Start?

The Malware Investigation and Response Content Pack can be found in the Cortex Marketplace. We provide hundreds of out-of-the-box integrations and packs for various use cases.

We also offer a deployment wizard that walks you through the installation of the pack.

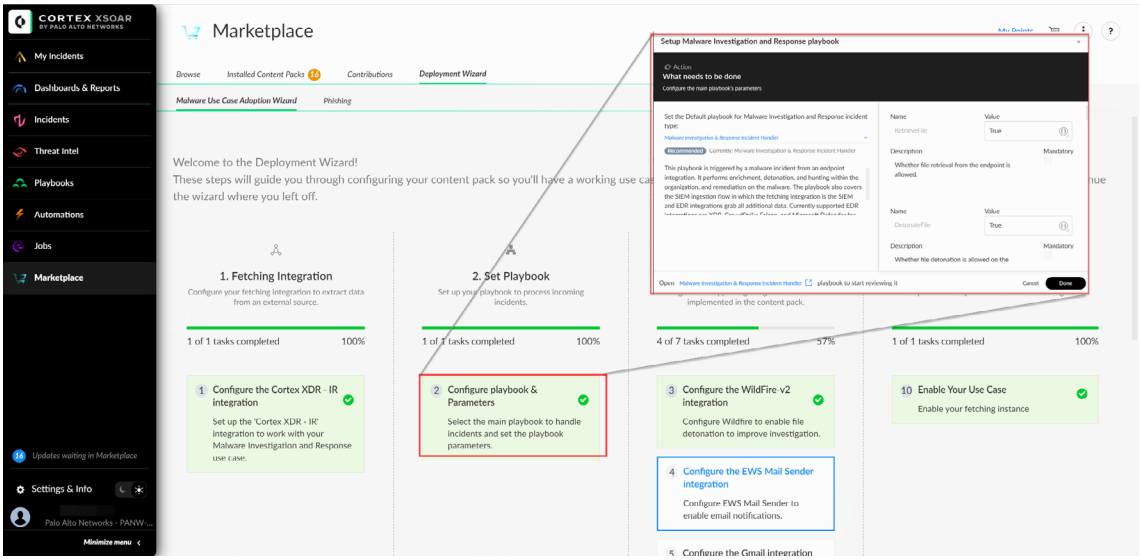

Figure 13: Deployment wizard

Learn More

Here are some other resources:

- Access this webinar on demand and learn best practices, preventative measures, and strategies for automating and speeding up malware investigations.
- Less busywork. More security. Catch our on-demand webinar to discover the top ways to automate security operations.
- Dive into our XSOAR Playbook of the Week blog series.

Engage with us on LinkedIn.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex_ds_essential-guide-to-automating-malware-investigations_122123