



THE ESSENTIAL GUIDE TO **AUTOMATING MALWARE INVESTIGATIONS**

MARCH 2023

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 overall risk of malware infections. To prepare for the next inevitable attack, SOC teams must continuously look for ways to improve their post-incident 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

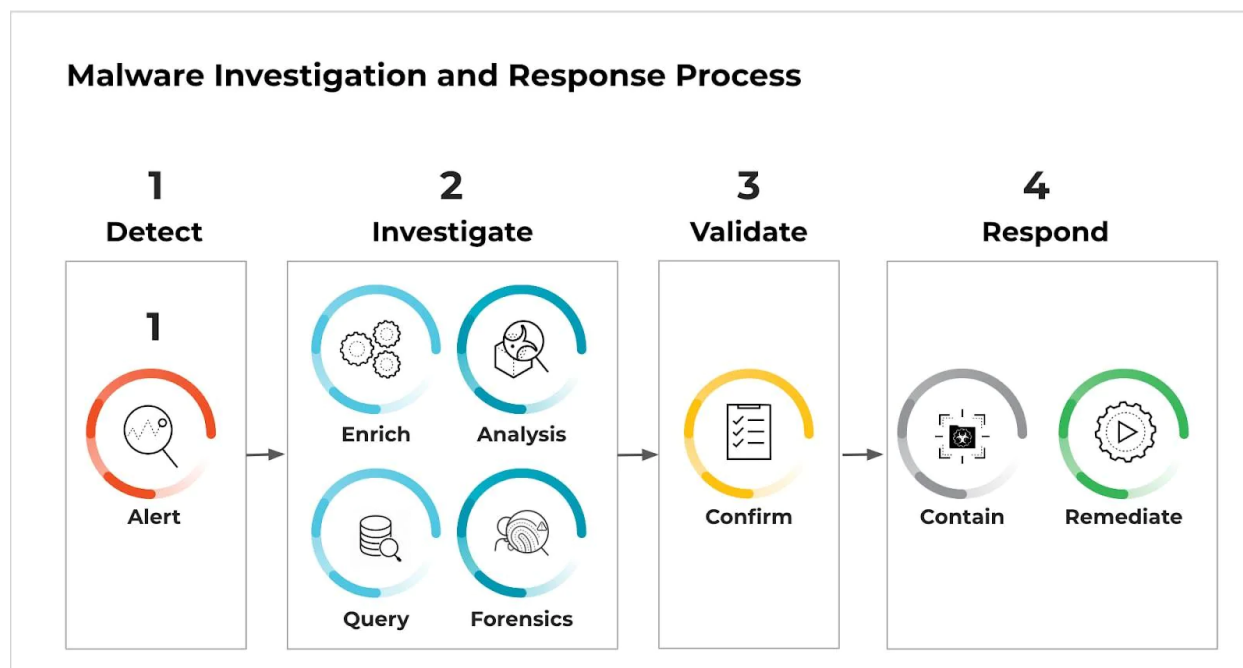
Many SecOps teams had limited automation deployed regarding malware. They might use basic rule-based automated actions provided by their EDR tools. These quick actions can be a time saver for a finite set of actions but are not scalable across multiple systems, nor do they truly tap into the full potential of automation. They might use a TIP (threat intel management) 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.

The Malware Investigation and Response Process



Malware analysis and forensics: Detect, investigate & 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

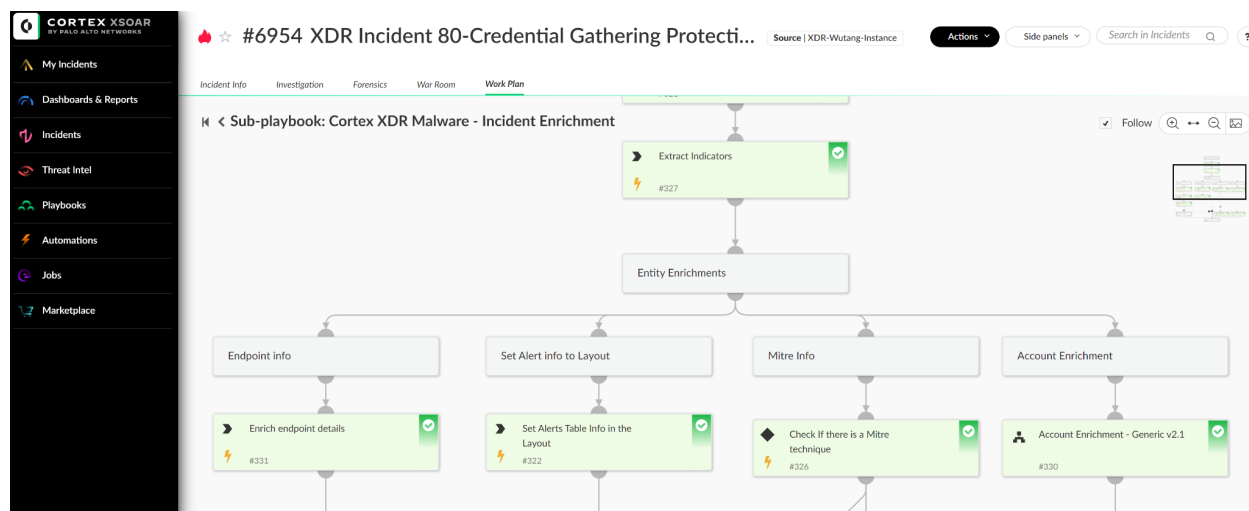
Once the investigation is complete, the analyst will need to take action based on the results of the investigation. If the alert is a true positive, the analyst will want to take containment precautions to prevent the malware from spreading. These actions include pivoting to various systems and performing 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 & Response Content Pack

We wanted to help SecOps teams to speed up investigations and deal with malware quickly by building automation into their incident response process. The Malware Investigation and Response 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.



Sample of malware investigation playbook

The screenshot displays the Cortex XSOAR interface with the 'Investigation' tab selected. The incident title is '#6954 XDR Incident 80-Credential Gathering Protection'. The left sidebar shows navigation options like 'My Incidents', 'Dashboards & Reports', 'Incidents', 'Threat Intel', 'Playbooks', 'Automations', 'Jobs', and 'Marketplace'. The main content area is divided into several sections:

- INVESTIGATION**: A table showing various tactics and their status.

TACTIC	STATUS
CREDENTIAL ACCESS	
Credentials from Password Stores	Detected
OS Credential Dumping: LSA Secrets	Detected
OS Credential Dumping: LSASS Mem...	Detected
DEFENSE EVASION	
Indicator Removal on Host	Not Detected
DISCOVERY	
Remote System Discovery	Detected
EXECUTION	
Command and Scripting Interpreter	Not Detected
LATERAL MOVEMENT	
Remote Services	Detected
- ALERTS**: A table showing alerts related to the incident.

ALERT NAME	HOSTNAME	FILE NAME	PROCESS ID	SHA256	COMMAND LINE
Credential Gathering ...	frigg	172.30.20.15	N/A		
New Administrative B...	bjorn	vmtoolsd.exe	4712	e3b6ef72450b00a02...	"C:\Program Files\VM...
Failed Connections	bjorn	svchost.exe	6184	adfd683a6910abbbf0...	"c:\windows\system3...
- INDICATORS (77)**: A table showing all associated indicators with the current incident.

TYPE	VALUE	VERDICT	FIRST SEEN	LAST SEEN
IP	86.96.72.139	Malicious	N/A	API
Attack Pattern	Remote Services	Suspicious	Jan 19th 2023 17:03...	API
Attack Pattern	Credentials from Password Stores	Suspicious	Jan 19th 2023 17:03...	API
Attack Pattern	OS Credential Dumping: LSA Secrets	Suspicious	Jan 19th 2023 17:03...	API

At the bottom, there is a toggle for 'Toggle markdown box on CLI using `ctrl+m`'.

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.

The screenshot displays the Cortex XSOAR interface with the 'Incident Info' tab selected. The incident title is '#6954 XDR Incident 80-Credential Gathering Protection'. The left sidebar is the same as in the previous screenshot. The main content area is divided into several sections:

- CASE DETAILS**: A table showing case information.

Type	Value
Malware Investigation and Response	
Severity	High
Owner	Symphony Harp
Playbook	Malware Investigation & Response Incident Handler
Close Reason	True Positive
Close Notes	Needs to be investigated.
- SOURCE DETAILS**: A table showing source information.

Field	Value
Process Path	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
Process Name	172.30.20.15
MD5	3b3ae8a31582136840b5ac3513dfrab2
SHA256	e3b6ef72450b00a02159dac6f98034f0d6918c64a8245
External Link	https://wutang-labz.xdr.us.paloaltonetworks.com/incident-view?caseid=80
Description	'Credential Gathering Protection - 3598738926' along with 2 other alerts generated by XDR Analytics and XDR Agent detected on 2 hosts involving user norsemen@thor
- ENDPOINT DETAILS**: A table showing endpoint information.

Field	Value
Device Name	frigg:50d03791eb6e4b78abf50e8bf2dac6a
Device ID	50d03791eb6e4b78abf50e8bf2dac6a
Device Status	Offline
Device Local IP	172.30.21.10
Device OS Name	Windows
Device OS Version	Windows 10 [10.0 (Build 19044)]
Device MAC Address	00:50:56:9f:39:8d
Agent Version	7.8.1.11343
Isolated	No
- ACCOUNT INFORMATION**: A table showing account information.

Field	Value
sAMAccountName	norsemen@thor
Manager Email Address	None
Account Member Of	
- INVESTIGATION SUMMARY**: A table showing investigation results.

TACTIC	RESULT
Command and Control	Not Detected
Defense Evasion	Not Detected
Execution	Not Detected
Lateral Movement	Suspicious
Persistence	Not Detected
- RESPONSE ACTIONS**: A table showing response actions.

Field	Value
Device Name	frigg:50d03791eb6e4b78abf50e8bf2dac6a
Process Name	172.30.20.15

At the bottom, there is a toggle for 'Navigate quickly with `ctrl+k` (default)'.

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 pre-built integrations with other sandboxes such as Joe Security, CrowdStrike Falcon, Cuckoo, Forti sandbox, Triage, Malwation, AnyRun, etc. You will find the complete list at our [Cortex Marketplace](#).

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

WildFire File Report

FileType	PE64
MD5	3b3ae8a31582f36840b5ac3513dbfab2
SHA256	e3b6ef72450b00a02159dadc6f98034f06b918c64a8249ecfced8bdb974f5de
Size	108216
Status	Completed

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.

Wildfire file report - static analysis summary

3 Dynamic Analysis

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

3.1.1. Behavioral Summary

1/4

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.	

Wildfire file report - dynamic analysis summary

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.	

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

Wildfire report-Host Activity

Response: Containment & 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.

RESPONSE ACTIONS

Device Name frigg:50d03791eb6e4b98abf50e8bbf2dac6a

Process Name 172.30.20.15

Isolate Endpoint

Unisolate Endpoint

Delete File From Endpoint

Kill Process

Tag For Deny List

Tag For Allow List

Disable Account in IDP

Remediation Actions

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.

TIMELINE INFORMATION

Occurred

Jan 19th 2023 16:58:05

Last Updated

Feb 16th 2023 19:25:15

Triage SLA (ended)



Late: 01h 42m

SLA: 30m

Jan 19th 2023 17:28:48

Created

Jan 19th 2023 16:58:45

Containment SLA (ended)



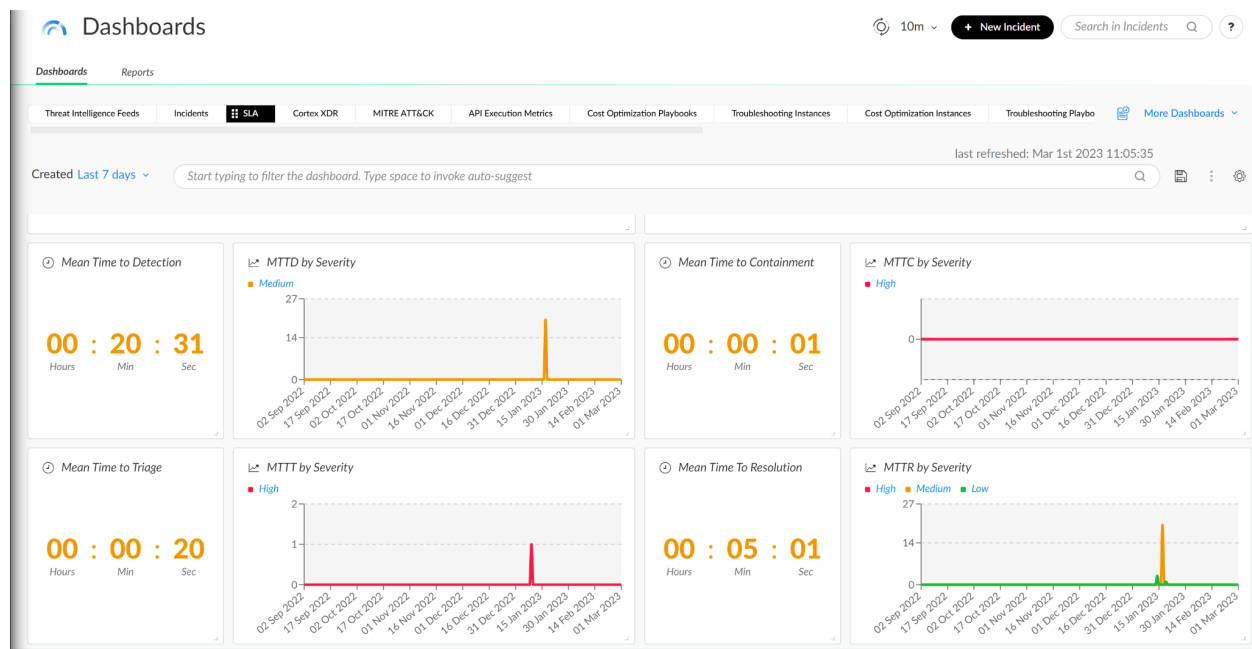
Risk: 24m

SLA: 30m

Jan 19th 2023 19:43:06

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.



SLA Dashboard

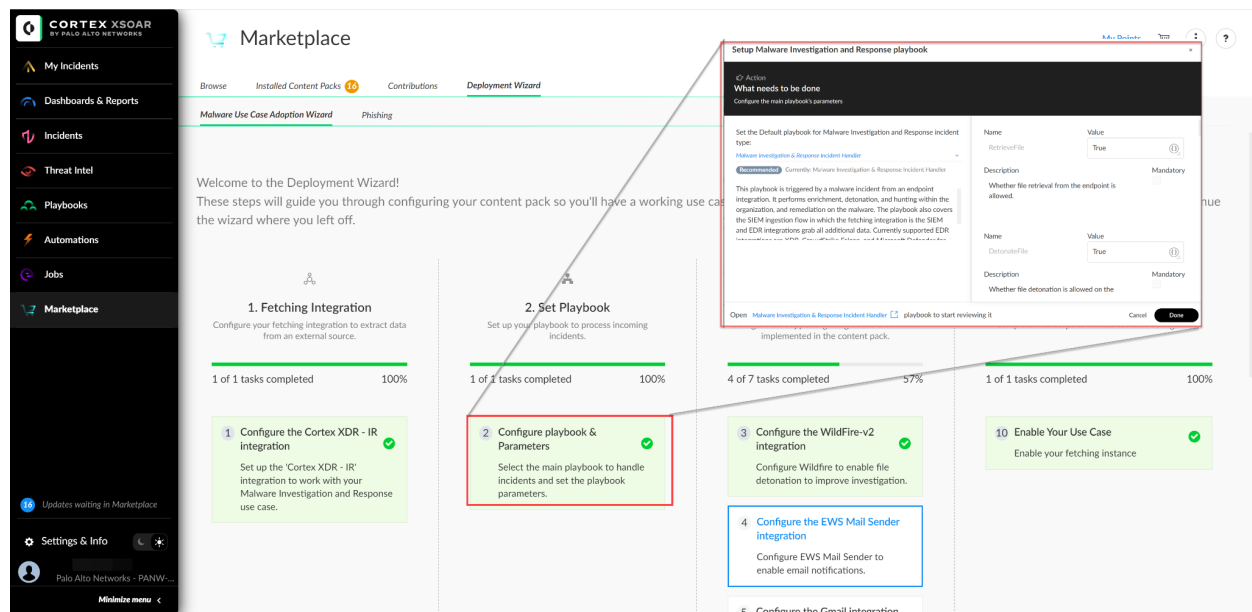
Assigning an analyst to the incident

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.



Deployment wizard

To Learn More...

Here are some other resources

- Sharpen your SOC Automation Skills by joining an upcoming Hands-On Workshop
 - [March 29](#) | [April 19](#) | [May 16](#)
- Learn how you can save your SOC team 100's of hours on daily tasks!
 - [April 4](#)
- Get the XSOAR playbook of the week on our [blog](#).

Engage with us on [LinkedIn](#)