SANS

Analyst Program

Product Review

Streamline Your Enterprise Security with Cortex XDR

Written by **Matt Bromiley**

January 2022

paloalto NETWORKS

CORTEX BY PALO ALTO NETWORKS

Introduction

Cyber intrusions are just not the same anymore. While “low and slow” cyber espionage attacks still occur, “smash and grab” adversaries seem to have taken the spotlight. Launching attacks that go from zero to full compromise in less than 24 hours, adversaries have developed techniques and tools that allow them to move quickly through an environment, wreaking havoc along the way. Many organizations have quickly realized that legacy or atomic, single-source detections no longer work or are too slow. Defenders simply don’t have that much time.

Instead, we are seeing a shift to relying on multiple sources of telemetry and crafting detections that can branch across these sources. Our goal is to detect attacks as quickly as they happen—not minutes, hours, or days afterward. In this product review, we look at a platform that does just that: Palo Alto Networks Cortex XDR. Highly integrated and boasting advanced detection and response capabilities, Cortex XDR is a powerful platform that offers defenders a much-needed advantage.

We had a chance to get hands-on with Cortex XDR and walk through several of its newer features. Some of our key takeaways from the platform include:

- Enterprise monitoring capabilities allow you to keep tabs on the assets within your environment.
- Endpoint protection allows for blocking of exploits, malware, and fileless attacks.
- Integrated telemetry across multiple sources, including network and endpoint, are enriched with powerful threat intelligence and malware analysis.
- Advanced behavioral and non-behavioral detection capabilities coupled with powerful endpoint analytics allow for advanced adversary detection.
- Deep-dive forensic analysis capabilities speed up incident response and host triage.

Additionally, we were able to experience Cortex XDR’s Managed Threat Hunting service, which keeps a close eye on the environment even when your defenders are putting out other fires. Managed Threat Hunting brings the experience of seasoned hunters from Palo Alto Networks to your environment, detecting threats that may otherwise go undetected. A powerful XDR platform coupled with threat hunting is exactly the advantage defenders need.

As you work your way through this review, we encourage you to consider the tooling defenders currently have available within your environment. In particular, ask the following questions:

- Can we gain asset visibility and vulnerability insight from the same place we detect and respond to threats?
- Can we detect threats in near real-time via myriad sources, including network and endpoint?
- Can we automatically correlate artifacts, assets, and intrusion data points to form a cohesive understanding of a threat to our environment?

These questions, and many more, surfaced as we worked through Cortex XDR. From a single vantage point, we were able to assess our assets, manage vulnerabilities, detect threats, perform hunts across our environment, and forensically triage systems. With this much power and capability, adversaries will have a hard time finding success in any environment.

Enterprise Management

Our review of Cortex XDR begins at the same place any good XDR strategy should begin: visibility. Visibility into an *entire* environment is critical for modern enterprise security, and you should ask that your security tooling and controls focus on visibility as a key feature. Luckily, with the out-of-the-box and customizable dashboards available, Cortex XDR wastes no time in getting to data of value. Figure 1 provides a screenshot of the default Incident Management Dashboard.

While this review focuses on Cortex XDR as a product, an XDR strategy is one that an organization may implement to obtain multisource visibility and detection capabilities. Aptly named, Cortex XDR can help get there faster with a single implementation.

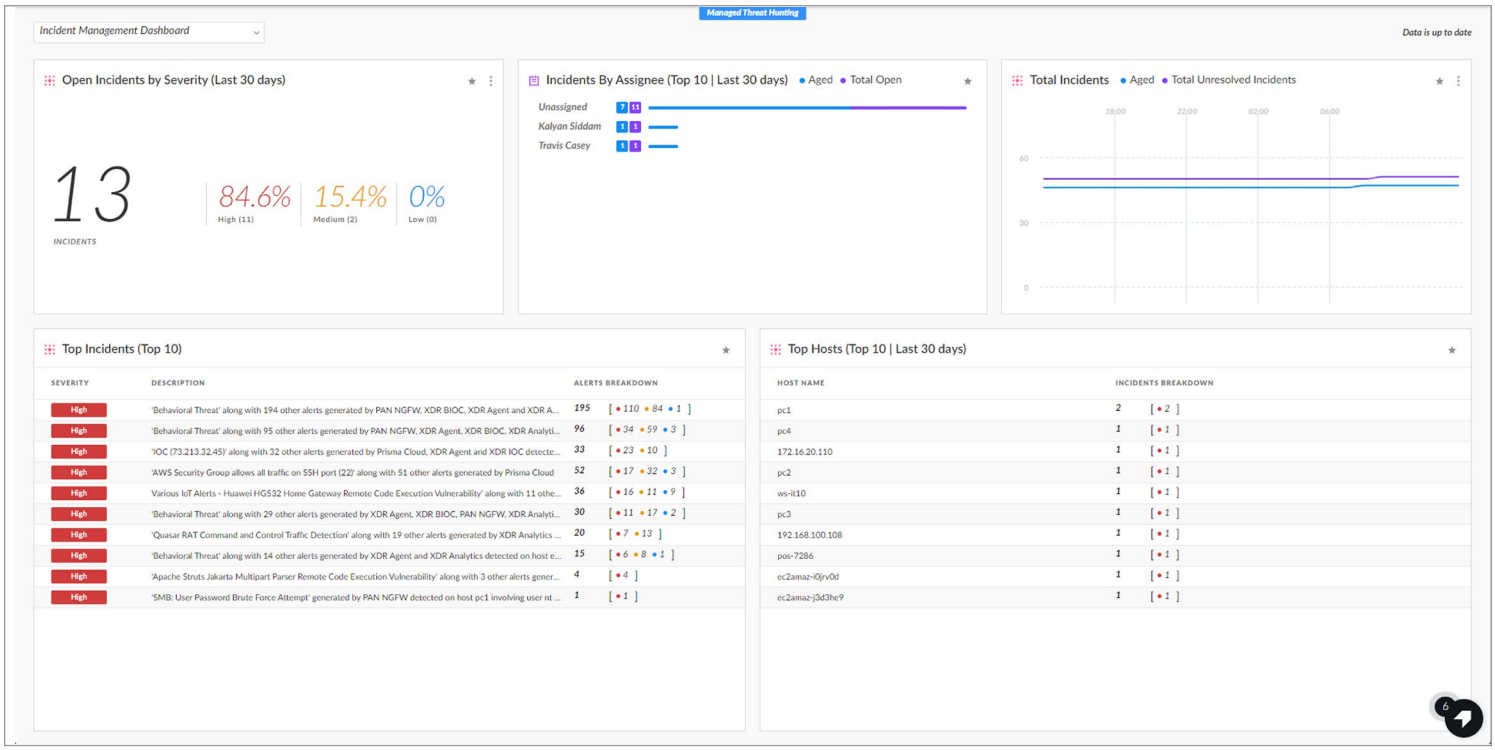


Figure 1. Incident Management Dashboard

The Incident Management Dashboard is a perfect starting point for SOC analysts or incident responders, because it calls attention to top incidents, open incidents, and impacted hosts. Cortex XDR further streamlines incident data with "rolled up" statistics, as shown in the Top Incidents tab. Figure 2 zooms in on this widget to highlight summarized incident details.

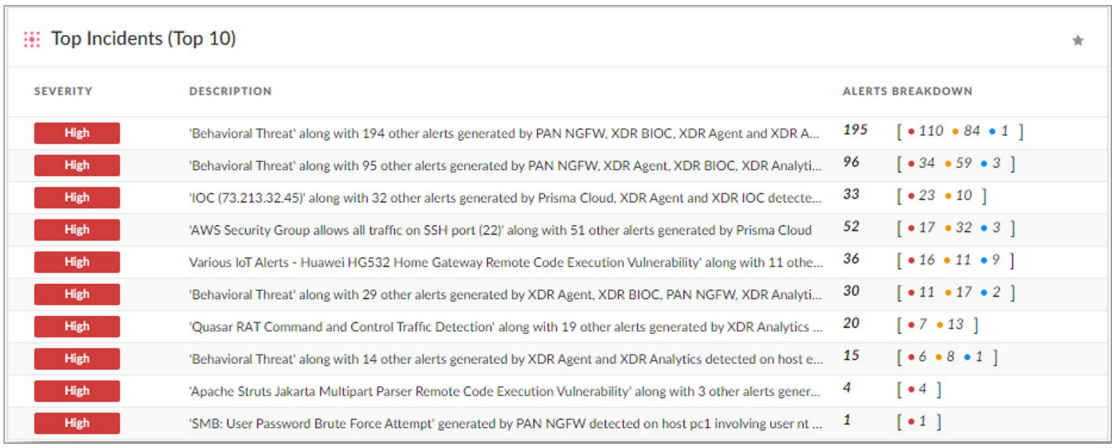


Figure 2. Enlarged View of Top Incidents Widget

Along with incident severity, analysts are provided a summarized description and breakdown of alerts. For example, the first incident is comprised of 195 alerts, which the platform automatically correlates and collates. But these are not single-source alerts. Cortex XDR has combined alerts from network, endpoint, and custom analytics into a single incident. This gives analysts a one-stop shop for incident analysis.

Cortex XDR also provides dashboards that cater to various roles and requirements of the organization. Figure 3 provides a snippet of the Dashboards menu. In addition to the Incident Management Dashboard, the platform provides additional "reactive" dashboards, such as MITRE, Threat Hunting 101, and security role-specific options. However, note that the platform also provides "proactive" dashboards, such as Agent Management, Data Ingestion, and Vulnerability Assessment. We are labeling these dashboards as "proactive" because they can help an organization assess its current strengths and posture, rather than always and only responding to alerts.

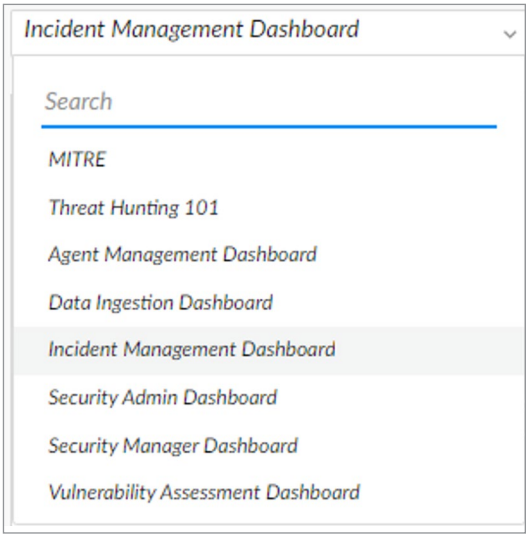


Figure 3. Dashboards Menu from the Initial Cortex XDR Screen

By combining sources of telemetry, Cortex XDR offers more correlated data in one place. This means that analysts can create custom dashboards for both proactive *and* reactive uses, relying on a wide range of data sources for effective security posture management.

This is the first strength of any XDR implementation, especially one with Cortex XDR. With multiple correlated data sources, such as endpoint and network data, organizations can move beyond an always-reactive state. The same data that can identify a network breach can be used to identify a vulnerability—before it is exploited by an opportunistic threat actor. Figure 4 shows the Vulnerability Assessment Dashboard.

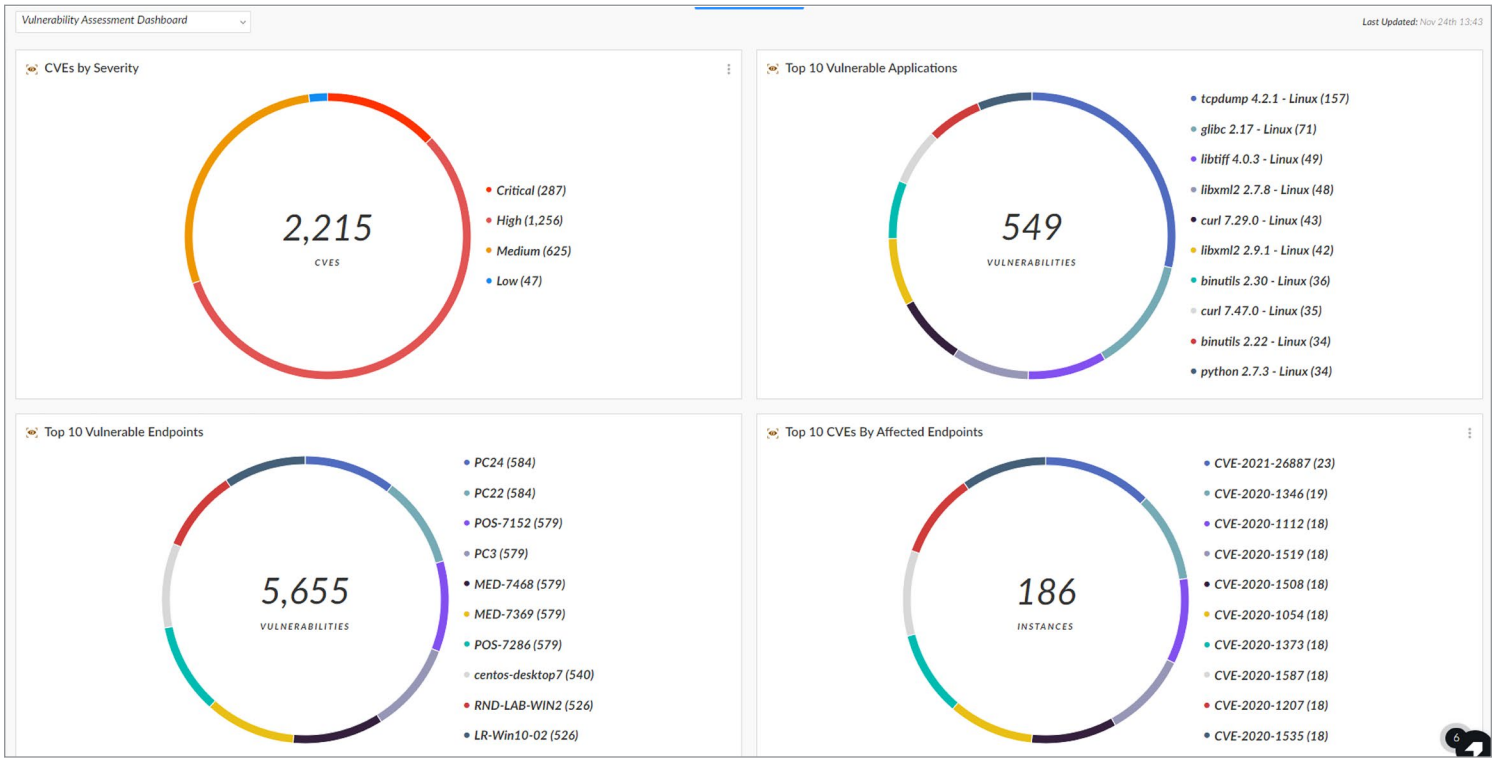


Figure 4. Vulnerability Assessment Dashboard

Simple and straightforward, the Vulnerability Assessment Dashboard is a useful vantage point for defenders and application owners to have into potential weaknesses within the environment. As expected, this dashboard is also interactive, and users can click anywhere for more details. While the dashboard itself does not provide granular details, such as vulnerability descriptions or which systems have which vulnerabilities, a single click takes users to a more granular vulnerability assessment screen. Figure 5 provides a screenshot of more details into the Vulnerability Assessment add-on, which drives the Vulnerability Assessment Dashboard.

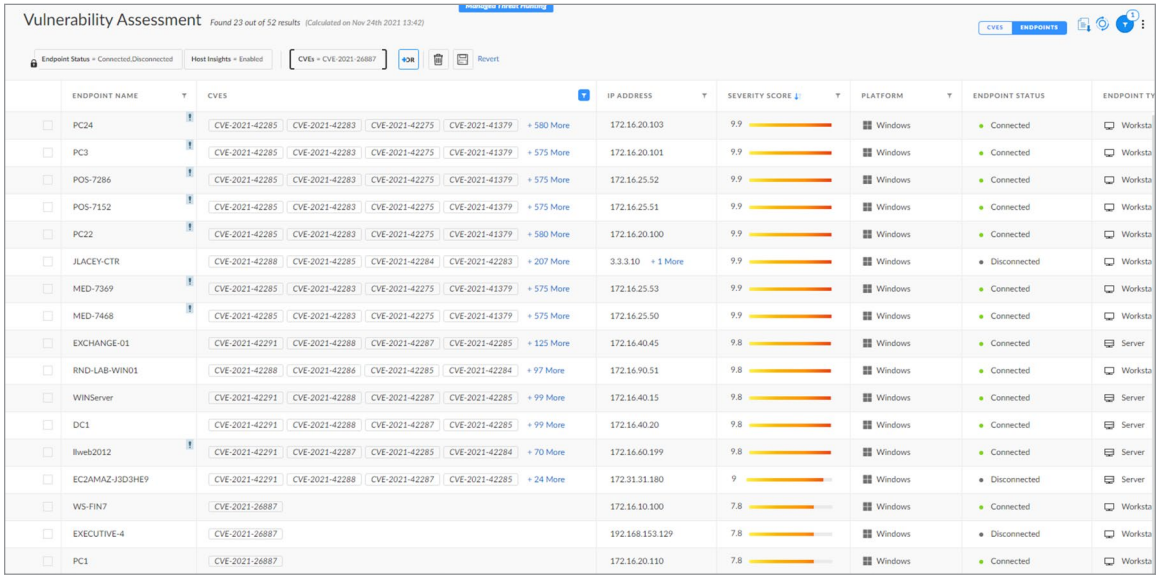


Figure 5. Vulnerability Assessment Add-On Within Host Insights

Herein lies one of the primary strengths of a holistic platform like Cortex XDR. Rather than only thinking about how a platform can help us detect, we should look at how enterprise visibility can be extended to *protect and prevent*. One method by which Cortex XDR extends its capabilities is through add-ons. The Vulnerability Assessment capability stems from Host Insights—a platform add-on that provides deep insight into hosts within an environment. This brings Cortex XDR into a position that allows it to function as a multipurpose tool, providing enterprises a single stop for endpoint management, vulnerability assessments, and incident detection and response.

While it is extremely powerful on its own, Palo Alto Networks can "extend" Cortex XDR through Add-ons—specific modules that allow analysts to take the platform's capabilities, visibility, and technology to the next level by offering advanced forensics, risk management, hunting, and response capabilities.

As seen in Figure 5, the platform provides granular insight into observed vulnerabilities. This includes CVE names, severity levels, affected product(s), and whether the vulnerabilities are application- or OS-specific. This is a wealth of information for defenders looking to patch or mitigate vulnerabilities before they can be exploited by threat actors.

Cortex XDR's capabilities as an enterprise visibility tool do not stop here. One of the platform's primary telemetry sources is Cortex XDR's endpoint agent, which offers robust insight into the organization. As expected, and as shown in Figure 6, the platform offers very detailed endpoint administration capabilities, including endpoint details such as hostname, IP address, operating system, and version number.

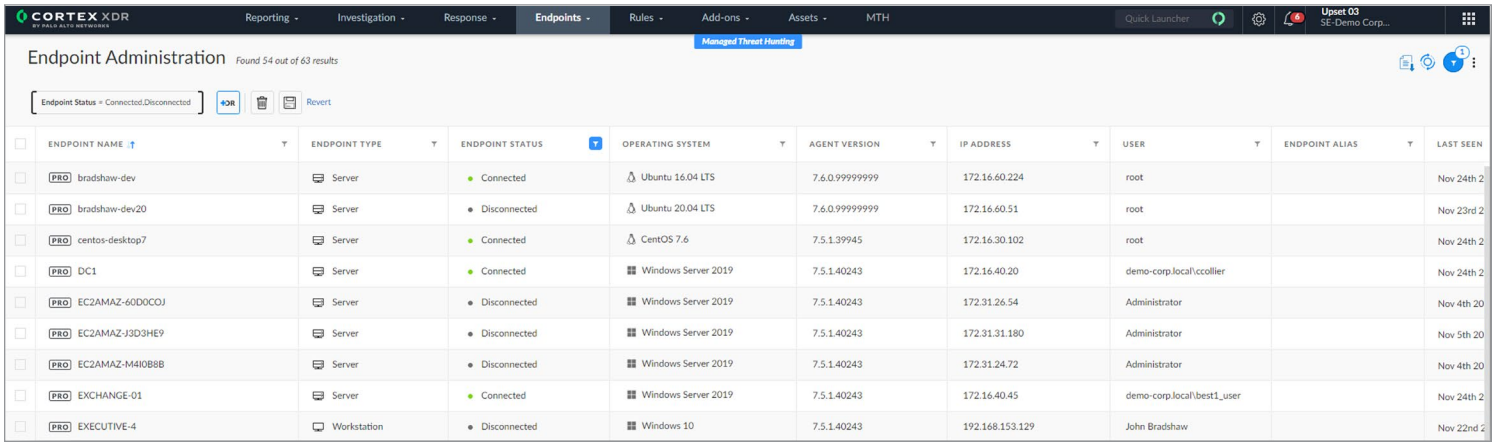


Figure 6. Endpoint Administration

It also appropriately categorizes endpoints as servers vs. workstations—an important distinction. Endpoint visibility and categorization is not a novel concept. Many platforms offer this capability. However, when coupled with Cortex XDR's prevention policies, it gives defenders a powerful automated response capability. See Figure 7.

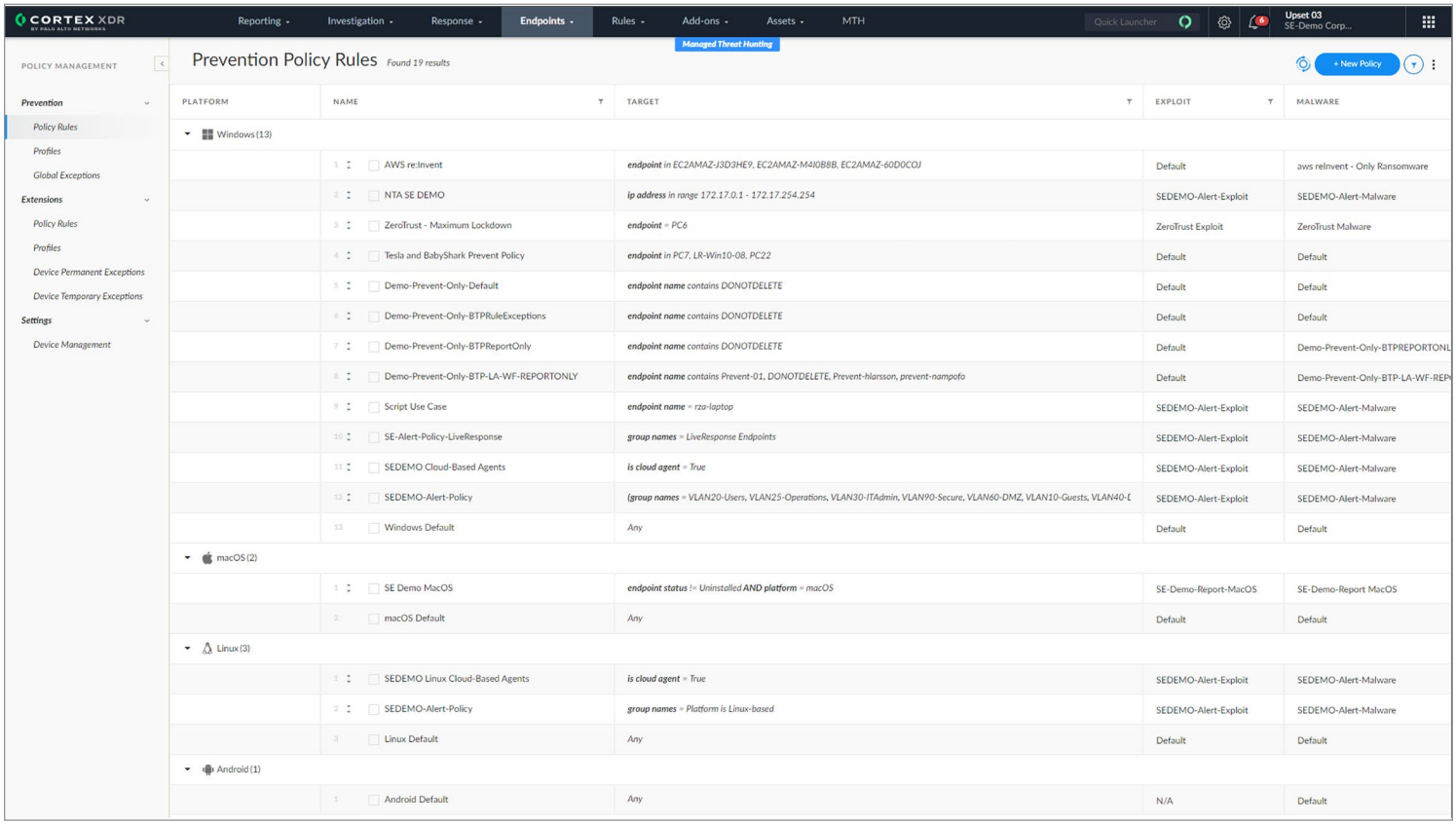


Figure 7. Prevention Policy Rules

Cortex XDR's prevention policies are the first stop where defenders can utilize the platform's holistic visibility and create custom policies to protect assets within the environment. Cortex XDR offers an extremely robust policy capability, allowing users to create policies with granular details such as system type, hostname, operating system, IP address, whether the system is cloud or on-prem, and/or within a customer-defined group.

The true power in prevention policies comes when defenders segment the environment according to system functionality and detection threshold(s). For example, consider two systems: an external-facing web server and an internal domain controller. Any security team would likely want to enable different policies and thresholds for each. We would expect an external system to reach outbound, a domain controller not. One of the fastest ways security teams can gain an advantage over attackers is to realize that with granular security and prevention policies, they can apply various security rules across the environment without hampering business functionality. The outcome? They eliminate a flat network and make it difficult for adversaries to achieve their objectives.

Enterprise Detection

In the previous section, we demonstrated how analysts can use dashboards and correlated, multisource data points to quickly gain insight into suspicious activity within an environment. As a robust XDR platform, Cortex XDR also provides analysts with the capabilities to dig deep into detections and incidents. Figure 8 shows the Incidents screen, with a focus on a spearphishing attack with Quasar and DarkComet malware.

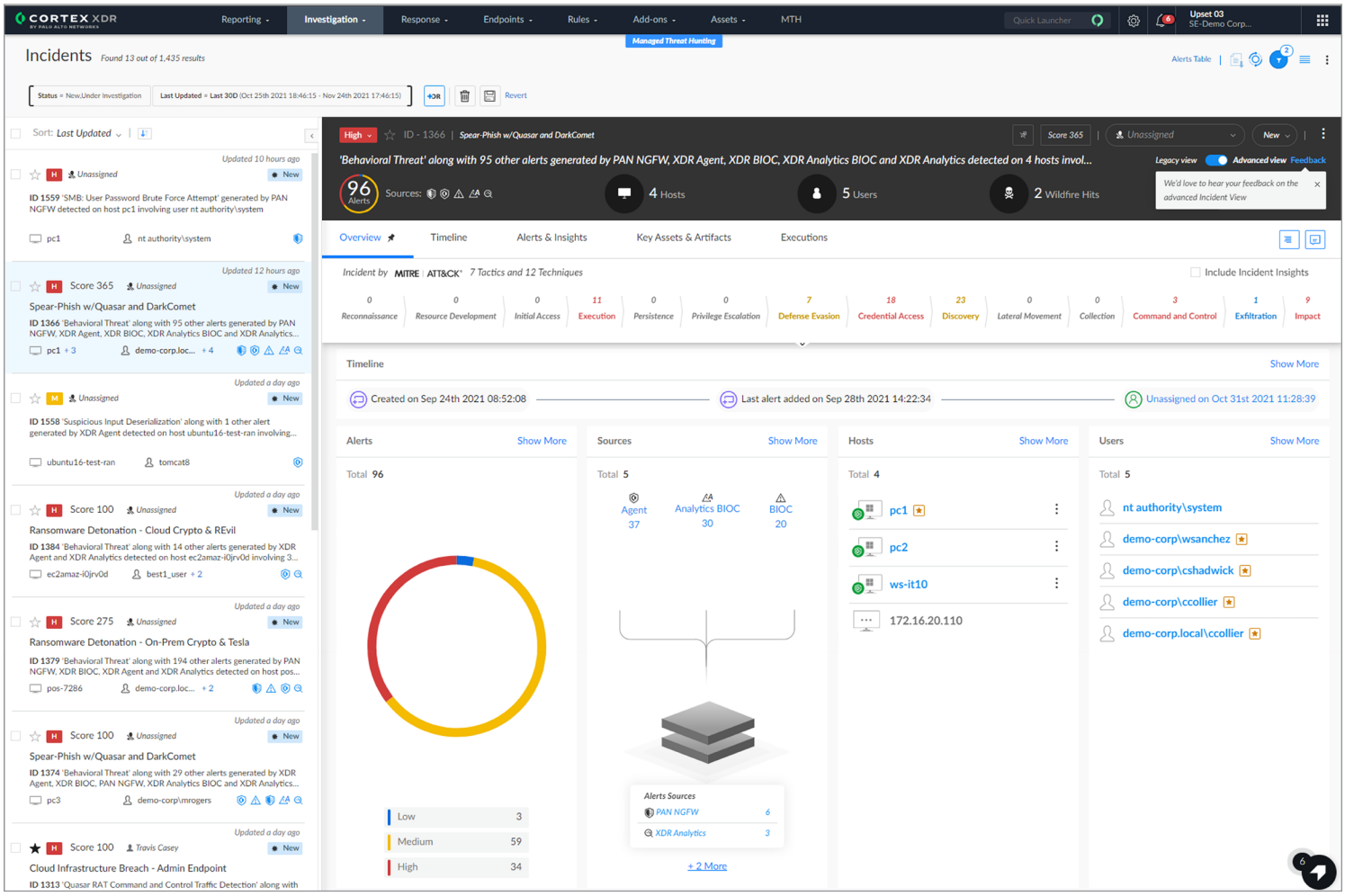


Figure 8. Incidents Tab with Focus on a Detected Spearphish

On the surface, this might seem like a simple incident. A spearphishing email was detected with Quasar and DarkComet malware attached. However, upon closer examination of the events associated with the incident, it's easy to see that this is anything but a simple detection. Within an incident like this, the true power of the Cortex XDR platform is clear to see. This incident includes:

- A combination of 211 alerts, from multiple sources: Behavioral and XDR Analytics, Palo Alto Networks NGFW, Insights, and endpoint agent events
- At least three impacted systems
- At least four impacted user accounts
- Seven tactics and 12 techniques from MITRE ATT&CK®, including Execution, Defense Evasion, Credential Access, and Exfiltration
- And much more

These automated alert analysis and correlation are huge. This is normally the job of security analysts—analyzing hundreds and thousands of alerts, looking for context and key artifacts, triaging, prioritizing, and responding accordingly. Cortex XDR does this *automatically!* Figure 9 provides a snippet of the timeline, which shows exactly how the platform goes about correlating events for analysts.

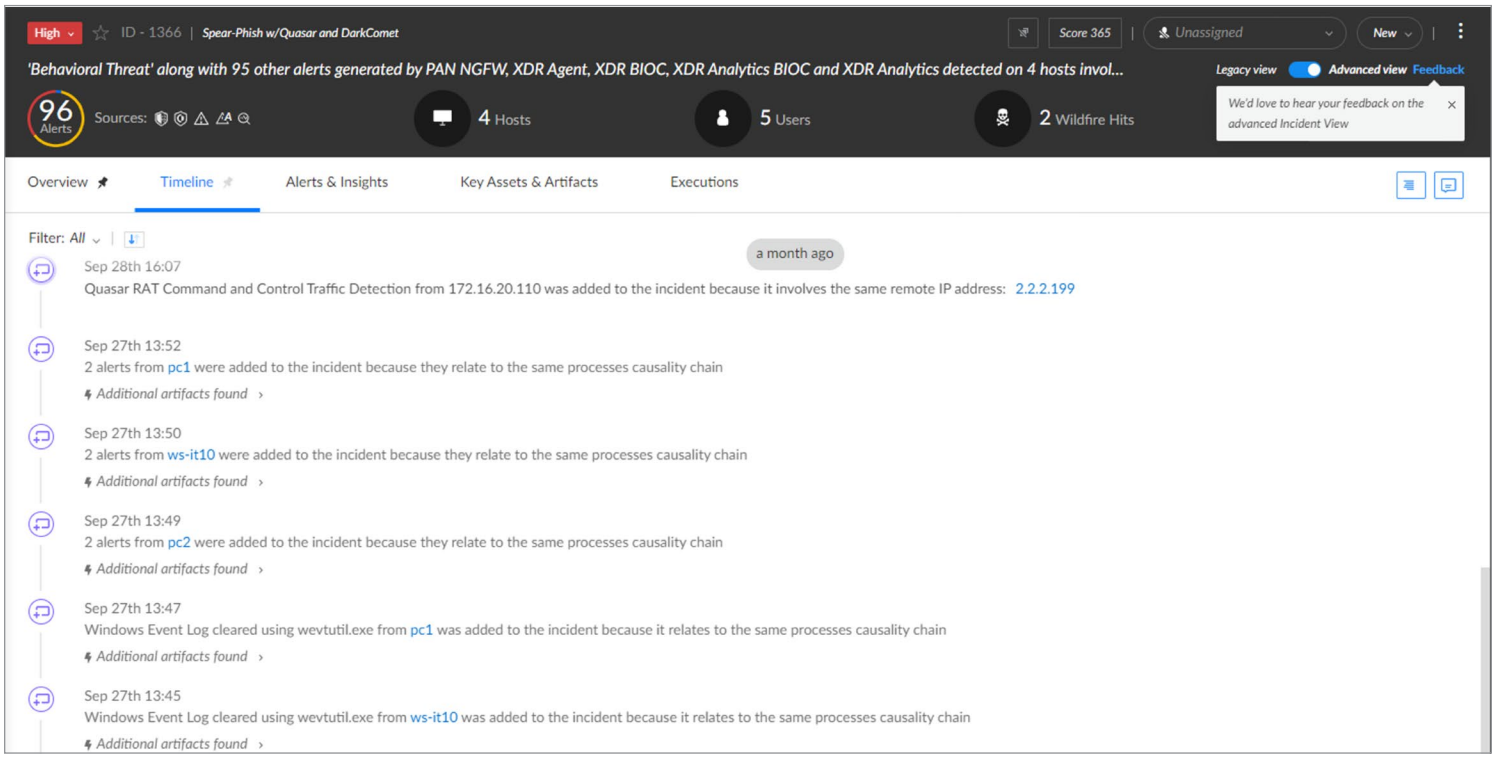


Figure 9. Timeline from the Spearphishing Incident

Cortex XDR automatically recognizes causality chains and associated artifacts from an event. For example, the clearing of Windows Event Logs on the system **`ws-it10`** was associated with an incident, due to "surrounding" events. Two minutes later, the system **`pc1`** suffered the same event. It is not uncommon for adversaries to perform the same actions on multiple systems; it is part of their playbook and attack tactics, techniques, and procedures (TTPs). By correlating similar artifacts and events, Cortex XDR helps analysts correlate what may appear to be two separate events but that are, in fact, related to the same ongoing incident. We also observe that two more alerts were generated on the system **`ws-it10`** and included in the overall investigation. As mentioned earlier, this is usually a process that is left up to security analysts, consuming time that could be spent responding to the activity.

Digging deeper into an incident, we can view granular data points about the various artifacts and assets as observed by Cortex XDR. Figure 10 shows the type of artifact, malware, and forensic details that analysts often need to respond to, triage, and eradicate a threat from the environment. Cortex XDR brings all this information to the surface. Analysts do not have to go "diving" for the key details they need. We love this! Furthermore, we can clearly see what users and systems are associated with an incident. This allows the security team to make faster decisions about cutting off user accounts or isolating systems and stopping adversaries in their tracks.

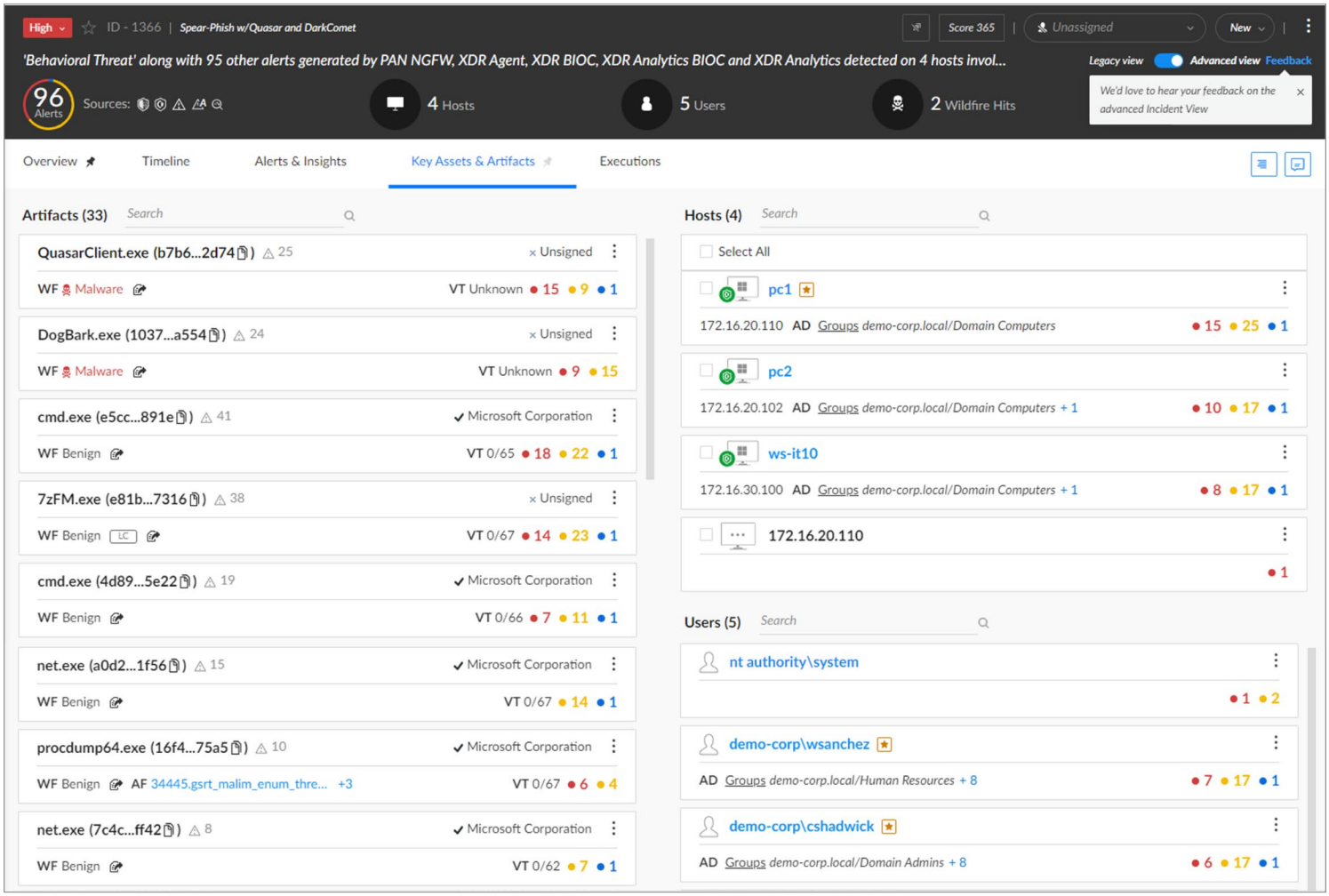


Figure 10. Key Assets and Artifacts Tab from the Spearphishing Incident

As shown in Figure 10, the adversary compromised at least five accounts (five are listed, but only two are shown in our screenshot). It's easy to see that one of the accounts belongs to a member of the Human Resources AD group, while the other is a Domain Administrator. Again, analysts do not have to dig for this. The information is up front, and analysts can make critical decisions about how to limit this account activity and what the adversary might be planning next.

What's in a Detection?

You may have noticed throughout our review terms like "IOC," "BIOC," or "XDR Agent." Unique to Cortex XDR, these terms represent the type of detections within the platform. For example, BIOCs (Behavioral IOCs), look for adversary activity that might warrant further investigation, but fall outside of the normal atomic IOCs that many analysts are used to, such as MD5 hashes and known-bad IP addresses.

Finally, the platform also allows users to view the individual alerts associated with an incident. However, as expected, Cortex XDR does not simply provide raw alerts (see Figure 11). The name "Alerts and Insights" is fitting for Cortex XDR because these are not raw alerts. Data points are enriched, and multiple sources and hosts are correlated on time-based pivots. For example, between `13:44` and `13:37`, we can see the adversary moving between three systems, triggering behavioral IOCs that detect malicious activity. However, the alerts list shows that prior to this activity, `ws-IT10` was the system that the adversary had the largest foothold on.

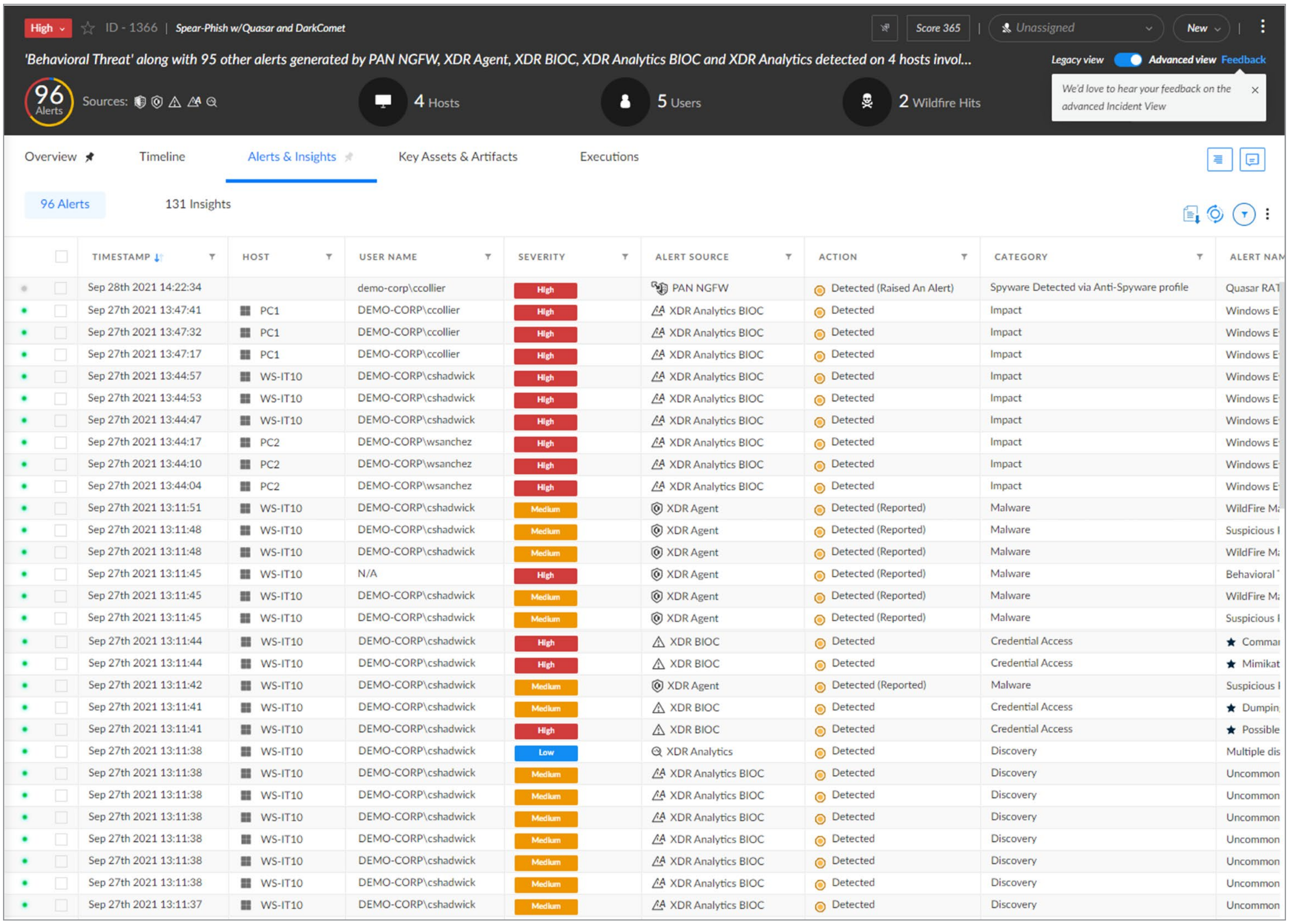


Figure 11. Alerts & Insights Tab from the Spearphishing Incident

The benefit of enriched alert data and asset details should be obvious to security teams. Many defenders will remember that they had to (and some might still be required to) correlate artifacts across multiple systems to understand the scope and impact of an intrusion. Oftentimes, it is a single event or malware alert that initiates an investigation. The Cortex XDR platform automates these analysis and correlation activities, freeing up analysts to *respond to the threat* in a timely manner, rather than losing time collecting more artifacts.

Does this mean that the investigation is complete? Of course, not. Analysts likely need to perform more artifact analysis. However, even with a single incident, such as a spearphishing-borne intrusion, Cortex XDR has automatically correlated dozens of alerts, systems, and users. Analysts can open a single screen, quickly assess the threat, decide what to do next, and get it done.

Speaking of correlation, another impressive feature of triaging and investigating with Cortex XDR is the Causality Chain view, available with investigations. Figure 12 shows this view.

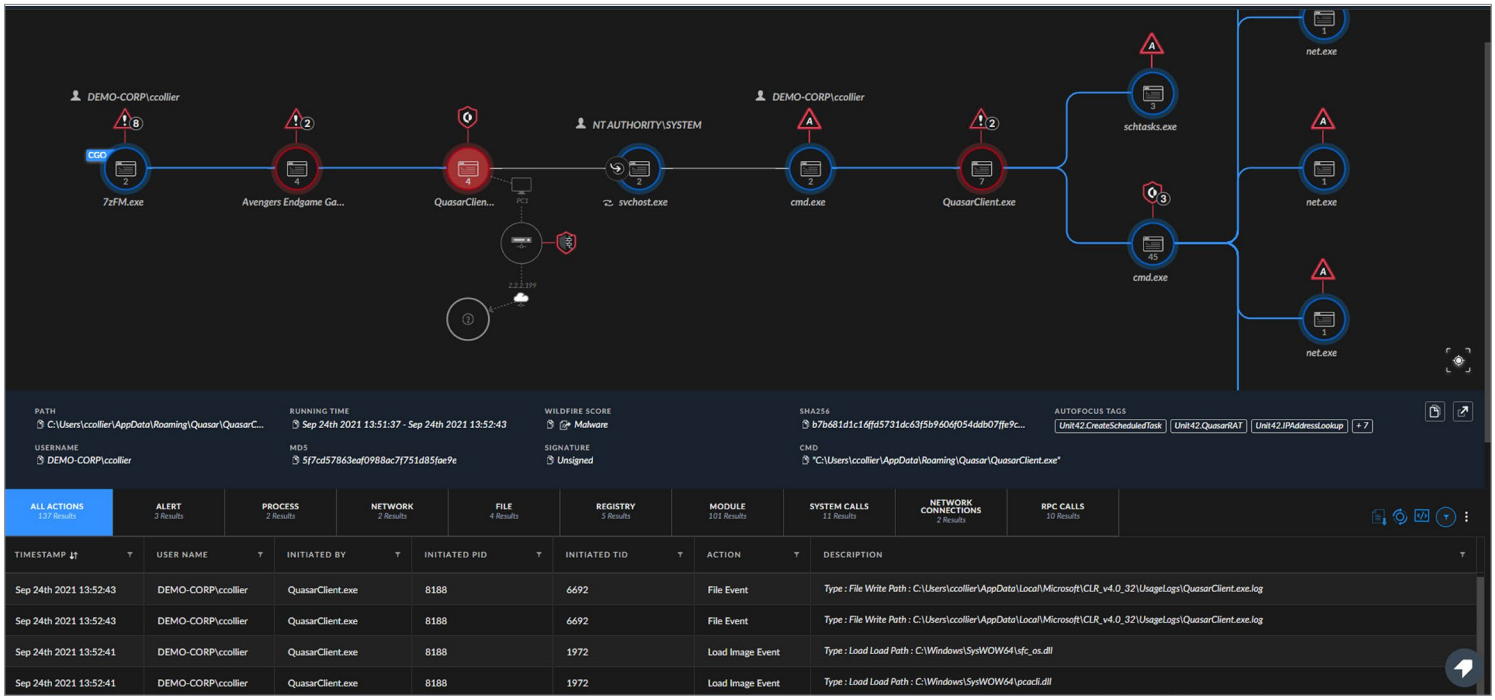


Figure 12. Causality Chain for an Investigation

This view helps analysts see and understand the various steps of an intrusion or suspicious activity. Along with correlated alerts, this view also helps analysts piece together the critical elements of an incident, such as potential entry vector, abused account, and impacted systems. This information is often hard to come by and may slow eradication or remediation efforts. Thinking ahead, Cortex XDR includes these details up front and automatically correlated.

Furthermore, as seen at the bottom of Figure 12, this view also provides a step-by-step replay of the actions observed and associated with various alerts. For example, this figure shows that there has been a multitude of file and registry events, network connections, system and RPC calls, and process launches. Without needing to go deep dive into every system, Cortex XDR automatically is recorded and provides that data in an easy-to-use manner.

Managed Threat Hunting

The analyst advantage does not stop with correlated and enriched incident details. During our review of Cortex XDR, we also noticed that the platform had a Managed Threat Hunting tag on certain screens, as shown in Figure 13.

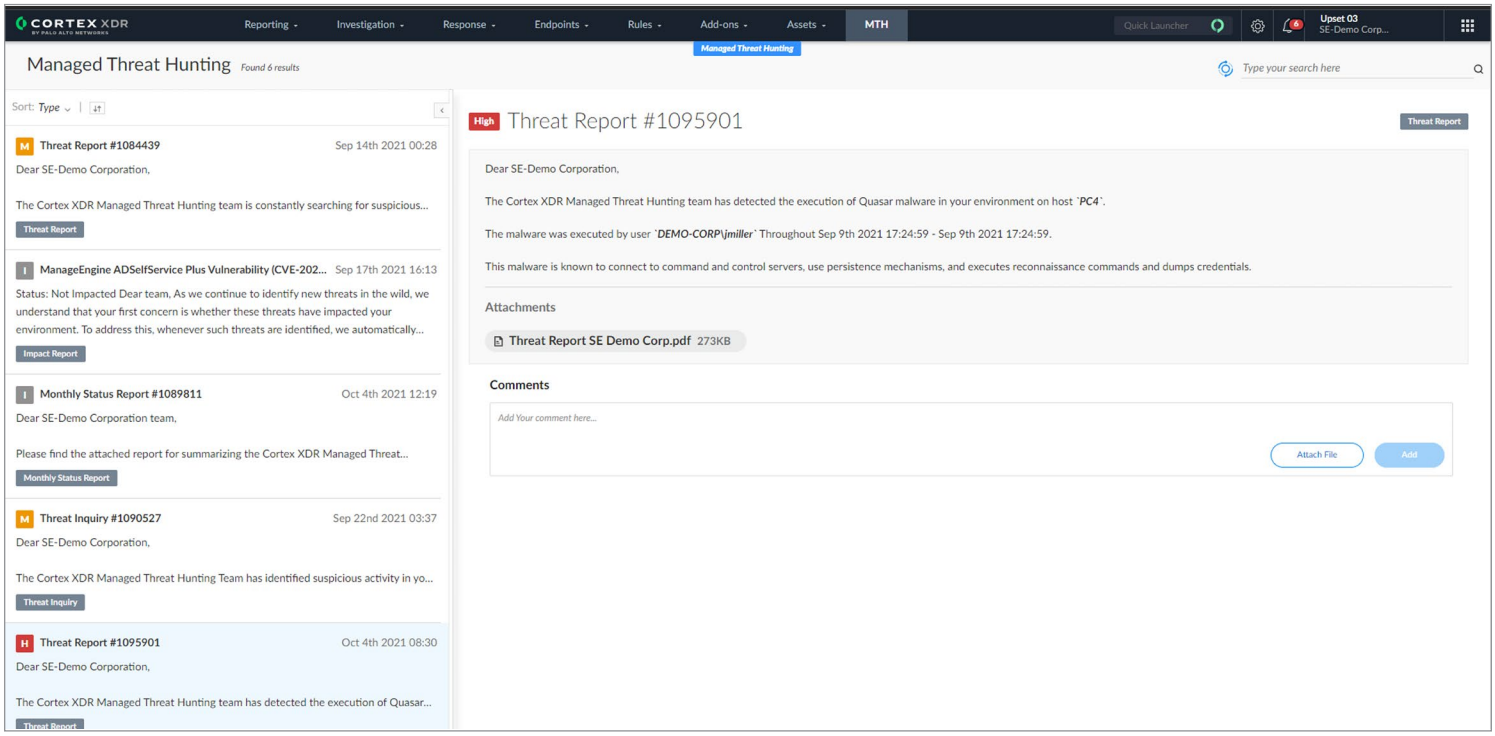


Figure 13. Managed Threat Hunting Capabilities

This version of Cortex XDR features Managed Threat Hunting and allows customers to add to their capabilities. Managed Threat Hunting takes advantage of the wealth of experience and threat intelligence at Palo Alto Networks, as seasoned threat hunters are constantly combing across various artifacts within customer environments. If a threat is detected, customers receive a custom notification with a complete summary PDF and investigation next steps. Figure 13 shows an example of a hunt that found evidence of Quasar malware execution within a test environment.

This capability—which occurs in the background and is completely invisible to the end user—allows customers to focus on other issues within the environment and simultaneously leverage the technical acumen of the Palo Alto Networks Unit 42 team.

Enterprise Response

While enterprise monitoring and incident detection are extremely powerful within the Cortex XDR platform, Palo Alto Networks did not stop there. Cortex XDR also features a robust response capability, ensuring no part of the XDR acronym is underserved. Furthermore, via its various acquisitions and code improvements, Cortex XDR offers a range of manual to automated response capabilities. These feature sets allow security teams of all shapes, sizes, and skills to truly customize the platform to their response needs.

Actions

We begin with an examination of Actions, within the Response capability of the Cortex XDR platform (see Figure 14). For all intents and purposes, Actions are programmable responses analysts can configure the platform to do.

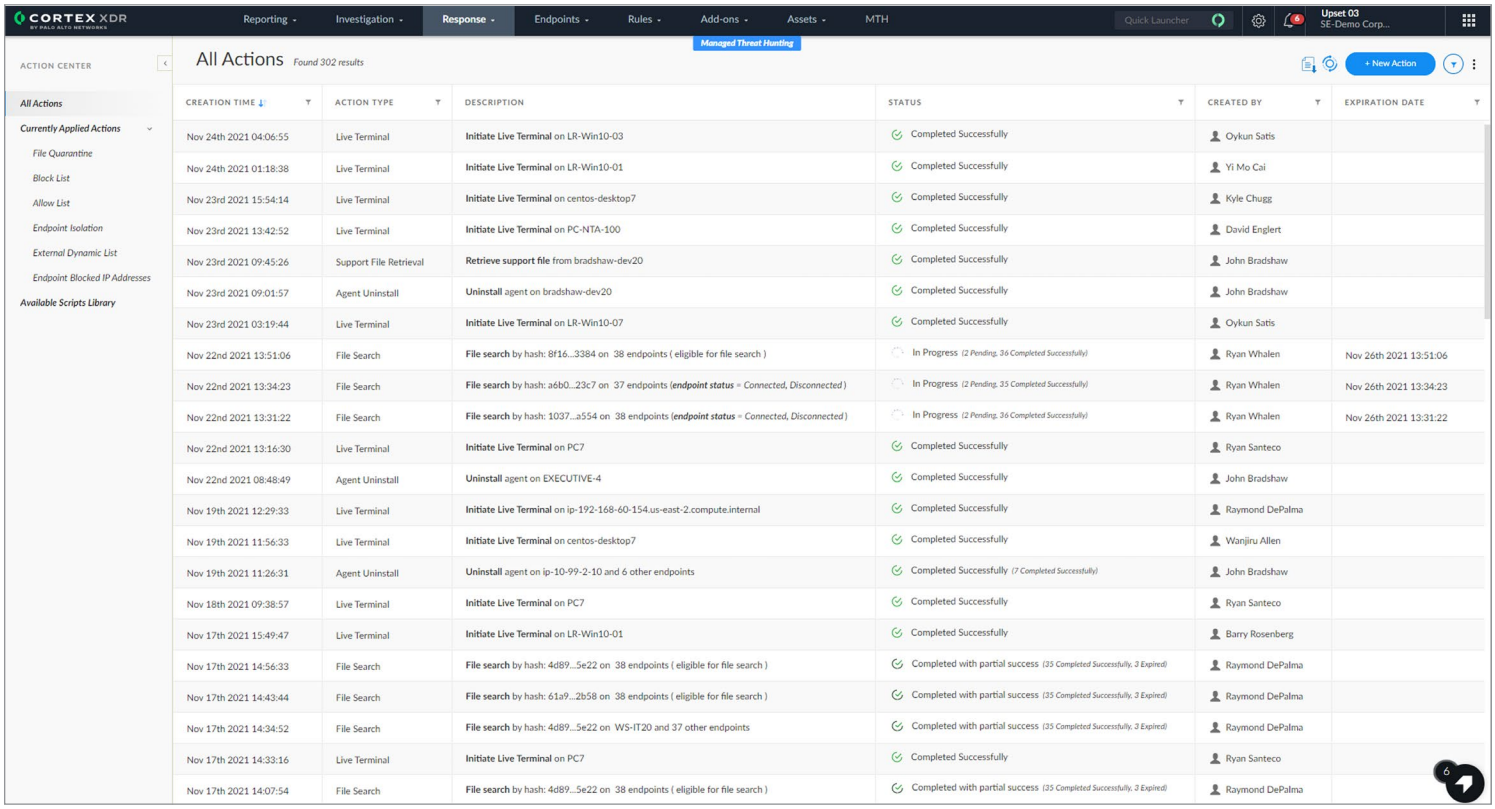


Figure 14. Action Center

As seen in Figure 14, configurable Actions include things such as searching and/or retrieving files (based on MD5 hash), blocking an IP address, allowing or blocking files, or killing processes—to name a few. Actions can be performed across a single or multiple systems, allowing for security teams to quickly scale from one-to-many during an investigation or incident response.

For example, Figure 15 provides a sample file search for **`cmd.exe`**, a well-known executable standard to any Windows installation. Searching for files across all known endpoints is a common incident response activity because it helps responders identify additional malicious files within an environment and identify the scope of an incident. To quickly kick off an Action looking for files, processes, or registry keys and go about other response activities is a welcome gain in efficiency for security analysts and responders.

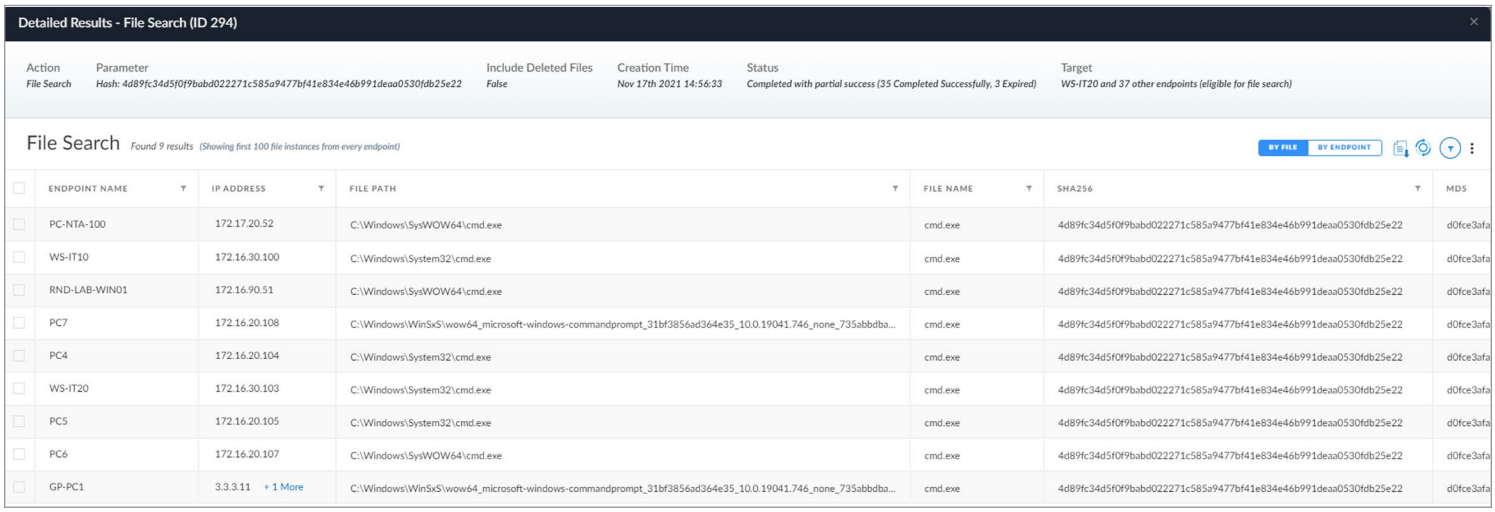


Figure 15. Action Looking for ***`cmd.exe`*** *Within a Population of Windows Systems*

Live Terminal

If a responder needs to get hands-on with an impacted system, Cortex XDR also provides (via its endpoint agent) the capability to establish a Live Terminal on connected systems. Being able to get "on" a system while not physically next to it is one of the most powerful features of this platform. As shown in Figure 16, analysts can open a terminal or browse files and tasks on a connected system, open a Command Line or PowerShell prompt, or even run Python scripts. In the example, we ran simple **`whoami`** and **`dir`** commands on a remote system, showing the current user and listing the current directory.

Cortex XDR's Live Terminal feature enables analysts to interact with a system with escalated privileges, allowing for real-time, advanced defense capabilities against ongoing attacks. Rather than simply waiting for alerts, analysts can issue ad-hoc defenses to protect users and enterprise data. Live Terminal is also an excellent tool for investigation and response of attacks within the environment.

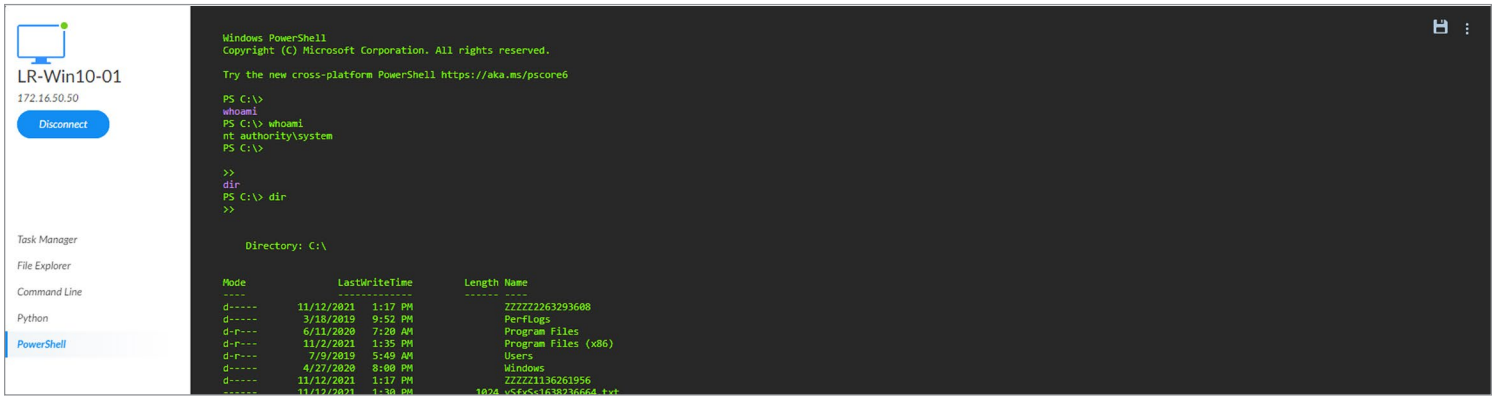


Figure 16. Live Terminal on a Windows 10 System

Figure 17 highlights available actions within the Live Terminal File Explorer. Analysts can upload or download files from a system, push files directly to VirusTotal, or get a verdict from Palo Alto Networks' Wildfire Malware Analysis Engine. Files can be marked as interesting (to further assist in an investigation) or moved/renamed.

It cannot be understated, especially in today's remote, disparate workplace, how critical this Live Response capability is to help combat threats to the environment. Long gone are the days when analysts have time or proximity to physically approach and analyze a system. And adversaries these days move faster than ever and have various tools to evade defenses. Relying *only* on alerts and never digging deep into a system, it's likely that the true extent of compromise on a system would remain unknown. However, by directly accessing and live triaging a victim system, defenders can quickly assess the state of a host and act appropriately.

The need for these capabilities is not new or uncommon to incident responders. For decades, forensic teams have dutifully collected images for subsequent analysis to identify the true scope of an intrusion. However, as time progresses, we have realized that real-time access and triage is necessary for truly effective, point-in-time incident response. Cortex XDR realizes this and gives analysts a powerful capability. But, of course, the platform does not stop there.

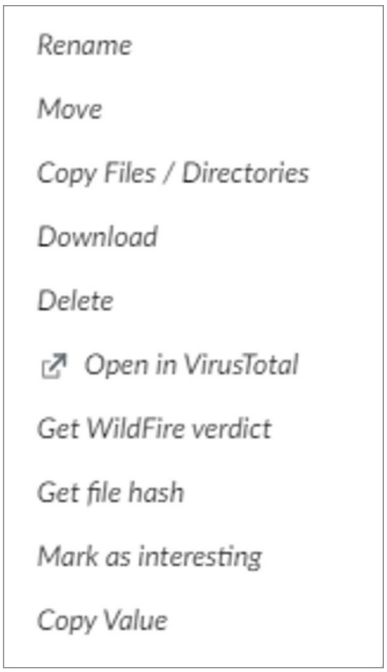


Figure 17. Actions in Live Terminal File Explorer

Forensics

As part of our product review, we also were granted access to the Forensics add-on. Like the Host Insights add-on, this is an additional capability that can be added to the Cortex XDR platform. Figure 18 provides a screenshot of the Forensics add-on.

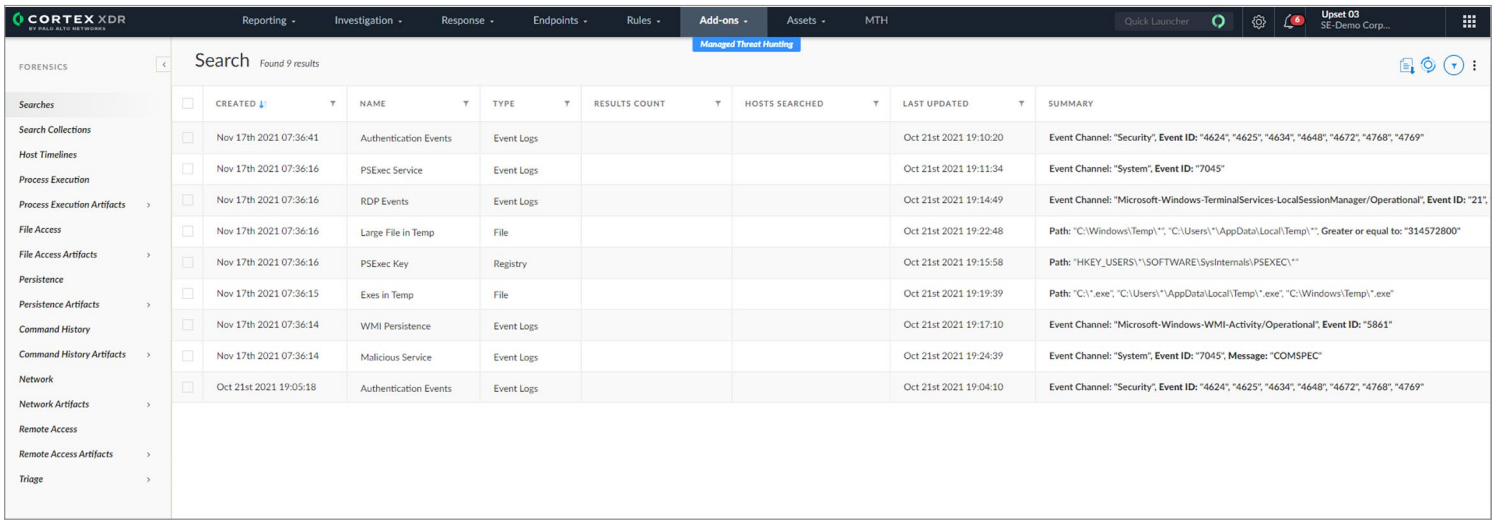


Figure 18. Forensics Add-On Within the Cortex XDR Platform

While the Live Terminal functionality allows analysts to get on a system in real-time for light data collection, the Forensics add-on is a force multiplier for system investigations. As seen in Figure 18, Cortex XDR's forensic capabilities go beyond simple file listings and a live terminal. Users have powerful options such as:

- Collect process execution and process artifacts over time
- Identify file access and artifacts of file access
- Identify persistence mechanisms
- Pull command-line history and remote access records
- Pull live network artifacts, including active interfaces and active connections

Analysts can use the Forensics module to collect system event logs; pull back volatile, memory-based artifacts; or examine a system registry or other configuration details. Furthermore, analysts can even collect a system timeline *directly from the platform* while a host is active. See Figure 19.

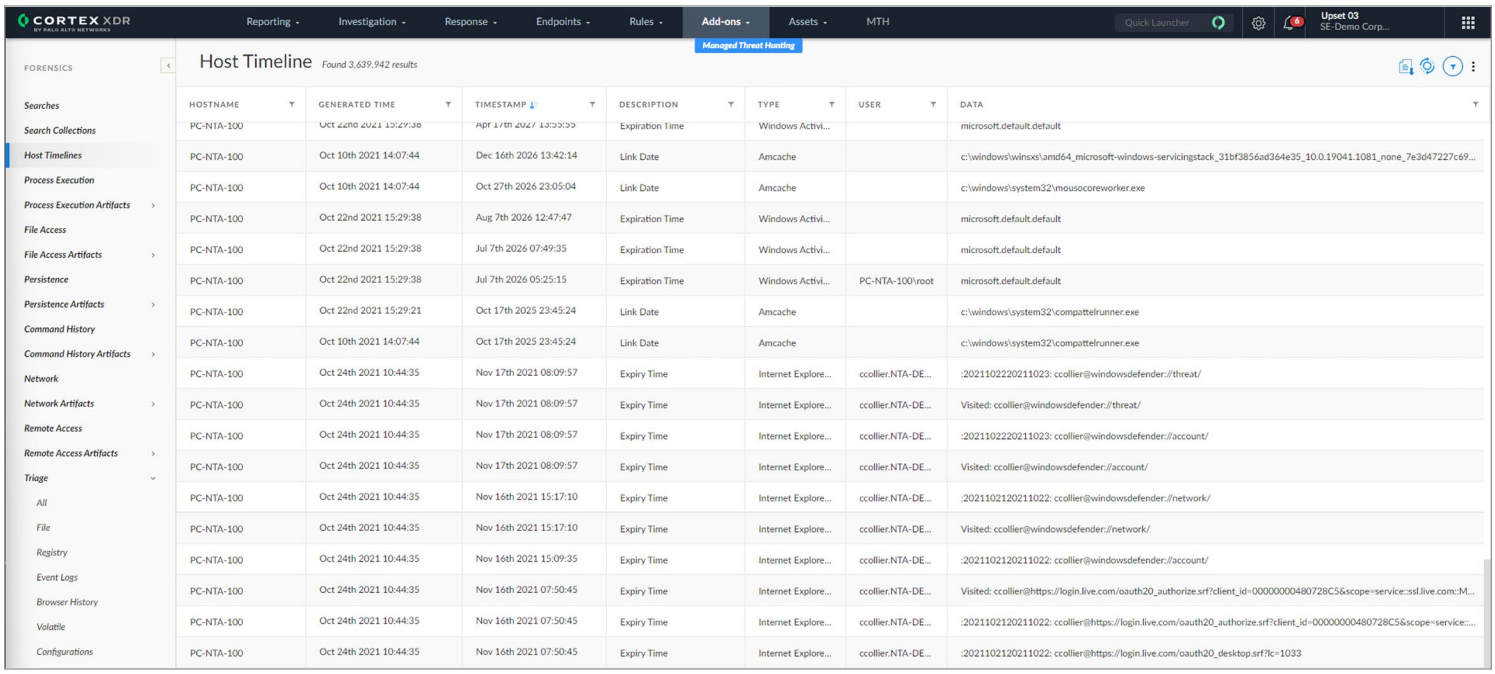
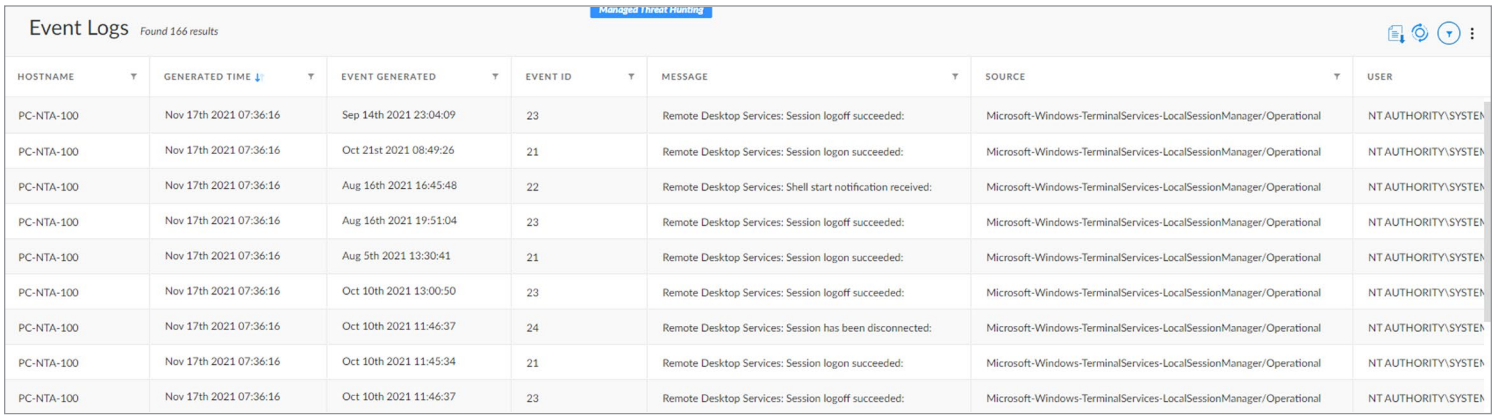


Figure 19. Host Timeline from the Forensics Add-On

This is truly a game-changer for enterprise-wide incident response. Collection and analysis of forensic artifacts is often a time-consuming activity that many security teams are unable to do on-demand. However, with this feature set in Cortex XDR, any security team immediately levels up with the ability to collect and analyze artifacts outside of normal detections.

The Forensics add-on also provides analysts with a unique threat-hunting capability to help detect threats outside of platform detections. For example, consider a security team that wants to look for evidence of RDP usage within the environment. This activity is not inherently malicious; however, the context of the system or a particular user account may warrant further investigation. Via the Forensics add-on, a search could be crafted to look for associated activity among system event logs. Figure 20 provides a screenshot of such a search.



Event Logs Found 166 results

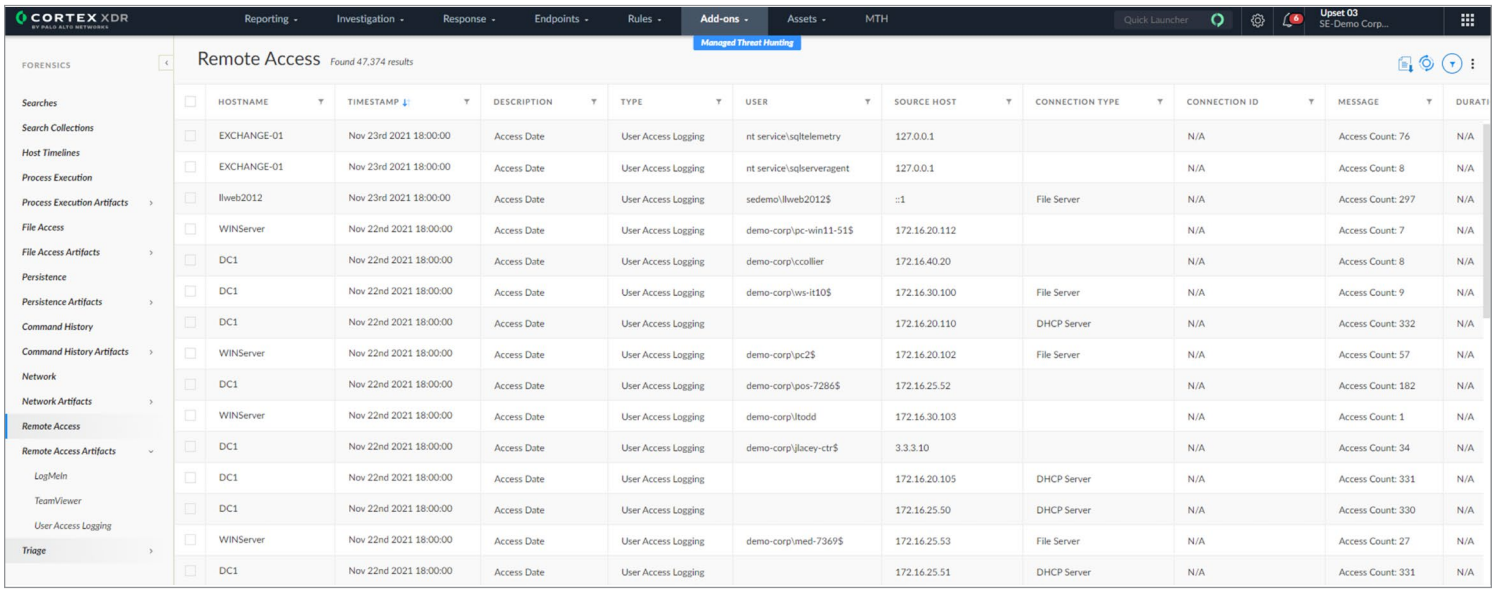
Managed Threat Hunting

HOSTNAME	GENERATED TIME	EVENT GENERATED	EVENT ID	MESSAGE	SOURCE	USER
PC-NTA-100	Nov 17th 2021 07:36:16	Sep 14th 2021 23:04:09	23	Remote Desktop Services: Session logoff succeeded:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Oct 21st 2021 08:49:26	21	Remote Desktop Services: Session logon succeeded:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Aug 16th 2021 16:45:48	22	Remote Desktop Services: Shell start notification received:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Aug 16th 2021 19:51:04	23	Remote Desktop Services: Session logoff succeeded:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Aug 5th 2021 13:30:41	21	Remote Desktop Services: Session logon succeeded:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Oct 10th 2021 13:00:50	23	Remote Desktop Services: Session logoff succeeded:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Oct 10th 2021 11:46:37	24	Remote Desktop Services: Session has been disconnected:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Oct 10th 2021 11:45:34	21	Remote Desktop Services: Session logon succeeded:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Oct 10th 2021 11:46:37	23	Remote Desktop Services: Session logoff succeeded:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	NT AUTHORITY\SYSTEM

Figure 20. Forensic Search of RDP Activity

This figure provides a succinct view of RDP event log entries from a single system. Analysts can easily observe session logon and logoff events, the source artifact, and user account(s) associated with the activity. The team did not need to collect forensic images or deploy complex scripts. Cortex XDR was able to leverage its presence in the environment to collect artifacts of interest. The platform also includes built-in forensic collection and data representation.

Consider the previous example, where an analyst crafted a search for RDP-focused event log entries. While RDP is a common remote access method, it is hardly the only form of remote access found within many enterprise environments. To help combat the need to write complex collection searches, Cortex XDR also includes artifact-based searches out of the box. For example, Figure 21 provides a snippet of the Remote Access search.



CORTEX XDR | Reporting | Investigation | Response | Endpoints | Rules | Add-ons | Assets | MTH | Quick Launcher | Upset 03 SE-Demo Corp...

Managed Threat Hunting

FORENSICS

Searches
Search Collections
Host Timelines
Process Execution
Process Execution Artifacts
File Access
File Access Artifacts
Persistence
Persistence Artifacts
Command History
Command History Artifacts
Network
Network Artifacts
Remote Access
Remote Access Artifacts
LogMeIn
TeamViewer
User Access Logging
Triage

Remote Access Found 47,374 results

HOSTNAME	TIMESTAMP	DESCRIPTION	TYPE	USER	SOURCE HOST	CONNECTION TYPE	CONNECTION ID	MESSAGE	DURATI
EXCHANGE-01	Nov 23rd 2021 18:00:00	Access Date	User Access Logging	nt service\sqltelemetry	127.0.0.1		N/A	Access Count: 76	N/A
EXCHANGE-01	Nov 23rd 2021 18:00:00	Access Date	User Access Logging	nt service\sqlserveragent	127.0.0.1		N/A	Access Count: 8	N/A
llweb2012	Nov 23rd 2021 18:00:00	Access Date	User Access Logging	sedemo\llweb2012$	::1	File Server	N/A	Access Count: 297	N/A
WINServer	Nov 22nd 2021 18:00:00	Access Date	User Access Logging	demo-corp\pc-win11-51$	172.16.20.112		N/A	Access Count: 7	N/A
DC1	Nov 22nd 2021 18:00:00	Access Date	User Access Logging	demo-corp\ccollier	172.16.40.20		N/A	Access Count: 8	N/A
DC1	Nov 22nd 2021 18:00:00	Access Date	User Access Logging	demo-corp\ws-it10$	172.16.30.100	File Server	N/A	Access Count: 9	N/A
DC1	Nov 22nd 2021 18:00:00	Access Date	User Access Logging		172.16.20.110	DHCP Server	N/A	Access Count: 332	N/A
WINServer	Nov 22nd 2021 18:00:00	Access Date	User Access Logging	demo-corp\pc2$	172.16.20.102	File Server	N/A	Access Count: 57	N/A
DC1	Nov 22nd 2021 18:00:00	Access Date	User Access Logging	demo-corp\pos-7286$	172.16.25.52		N/A	Access Count: 182	N/A
WINServer	Nov 22nd 2021 18:00:00	Access Date	User Access Logging	demo-corp\ltodd	172.16.30.103		N/A	Access Count: 1	N/A
DC1	Nov 22nd 2021 18:00:00	Access Date	User Access Logging	demo-corp\jlacey-ctr$	3.3.3.10		N/A	Access Count: 34	N/A
DC1	Nov 22nd 2021 18:00:00	Access Date	User Access Logging		172.16.20.105	DHCP Server	N/A	Access Count: 331	N/A
DC1	Nov 22nd 2021 18:00:00	Access Date	User Access Logging		172.16.25.50	DHCP Server	N/A	Access Count: 330	N/A
WINServer	Nov 22nd 2021 18:00:00	Access Date	User Access Logging	demo-corp\med-7369$	172.16.25.53	File Server	N/A	Access Count: 27	N/A
DC1	Nov 22nd 2021 18:00:00	Access Date	User Access Logging		172.16.25.51	DHCP Server	N/A	Access Count: 331	N/A

Figure 21. Remote Access Collection Within the Forensics Add-On

This provides a much more succinct and analyst-friendly way to view remote access activity within an environment. The results displayed clearly include systems, timestamps, local and remote network addresses, connection type, and associated usernames. Also, note that this search encompassed multiple systems, meaning analysts and responders can quickly scale a finding or a hunt across the entire environment, and allow the platform to display the data in an easy-to-consume manner.

Closing Thoughts

Make no doubt about it, cyberattacks are not what they used to be. Adversaries are much more integrated and capable, coupled with tooling that allows them to burrow deep into a victim network. In the same vein, detecting and responding to attacks also has changed. We no longer can rely on limited or single-source telemetry. It's far too easy to evade detections, and security teams are left cleaning up the mess. If your organization continues to suffer attacks and your security team cannot seem to gain an advantage, it may be time to consider whether you are approaching your enterprise security with the right tooling.

In this product review, we looked at a platform that is changing the game and restoring the advantage to defenders: Palo Alto's Cortex XDR. Built on top of highly integrated endpoint and network defenses, Cortex XDR provides a much-needed holistic view into an organization. Cortex XDR comes equipped with robust detection and threat intelligence capabilities, detecting behavioral and non-behavioral adversary techniques. Finally, the platform also boasts advanced forensic and incident response capabilities, truly cementing Cortex XDR as a platform that can take an investigation from start to finish and disrupt adversaries in your network.

Sponsor

SANS would like to thank this paper's sponsor:

paloalto® NETWORKS

CORTEX BY PALO ALTO NETWORKS