SANS

Analyst Program

Product Review

Streamline Your Enterprise Security with Cortex XDR

Written by <u>Matt Bromiley</u> January 2022





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.

Incident Management I	Dashboard v	hreat Hunting	Data is up
III Open Incidents	s by Severity (Last 30 days) * : by Severity (Last 30 days) * : Non-signed 2 1 Non-signed 2	10 days) • Aged • Total Open *	Incidents Aged Total Unresolved Incidents * 18,00 22,00 62,00 66,00 0 0 0 0 0
It Top Incidents (* *	III Top Hosts (Top 10 Last 30 days)	
SEVERITY	DESCRIPTION ALERTS BREAKDOWN	HOST NAME	INCIDENTS BREAKDOWN
High	"Behavioral Threat along with 194 other alerts generated by PAN NGFW, XDR BIOC, XDR Agent and XDR A 195 [•110 • 84 • 1]	pc1	2 [•2]
High	'Behavioral Threat' along with 95 other alerts generated by PAN NGFW, XDR Agent, XDR BIOC, XDR Analyti 96 [• 34 • 59 • 3]	pc4	1 [•1]
High	'IOC (73.213.32.45)' along with 32 other alerts generated by Prisma Cloud, XDR Agent and XDR IOC detecte 33 [• 23 • 10]	172.16.20.110	1 [•1]
High	AWS Security Group allows all traffic on SSH port (22)' along with 51 other alerts generated by Prisma Cloud 52 [•17 • 32 • 3]	pc2	1 [•1]
High	Various IoT Alerts - Huawei HG532 Home Gateway Remote Code Execution Vulnerability' along with 11 othe 36 [• 16 • 11 • 9]	ws-it10	1 [•1]
High	'Behavioral Threat' along with 29 other alerts generated by XDR Agent, XDR BIOC, PAN NGFW, XDR Analyti 30 [•11 •17 •2]	pc3	1 [•1]
High	'Quasar RAT Command and Control Traffic Detection' along with 19 other alerts generated by XDR Analytics 20 [•7 •13]	192.168.100.108	1 [•1]
High	'Behavioral Threat' along with 14 other alerts generated by XDR Agent and XDR Analytics detected on host e 15 [• 6 • 8 • 1]	pos-7286	1 [•1]
High	'Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability' along with 3 other alerts gener 4 [•4]	ec2amaz-i0jrv0d	1 [•1]
High	'SMB: User Password Brute Force Attempt' generated by PAN NGFW detected on host pc1 involving user nt 1 [•1]	ec2amaz-j3d3he9	1 [•1]

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

Incidents (Top 10)								
SEVERITY	DESCRIPTION	ALERT	S BREAKDOWN					
High	'Behavioral Threat' along with 194 other alerts generated by PAN NGFW, XDR BIOC, XDR Agent and XDR A	195	[•110 •84 •1]					
High	'Behavioral Threat' along with 95 other alerts generated by PAN NGFW, XDR Agent, XDR BIOC, XDR Analyti	96	[•34 •59 •3]					
High	'IOC (73.213.32.45)' along with 32 other alerts generated by Prisma Cloud, XDR Agent and XDR IOC detecte	33	[•23 •10]					
High	'AWS Security Group allows all traffic on SSH port (22)' along with 51 other alerts generated by Prisma Cloud	52	[•17 •32 •3]					
High	Various IoT Alerts - Huawei HG532 Home Gateway Remote Code Execution Vulnerability' along with 11 othe	36	[•16•11•9]					
High	'Behavioral Threat' along with 29 other alerts generated by XDR Agent, XDR BIOC, PAN NGFW, XDR Analyti	30	[•11 •17 •2]					
High	'Quasar RAT Command and Control Traffic Detection' along with 19 other alerts generated by XDR Analytics	20	[•7•13]					
High	'Behavioral Threat' along with 14 other alerts generated by XDR Agent and XDR Analytics detected on host e	15	[•6•8•1]					
High	'Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability' along with 3 other alerts gener	4	[•4]					
High	'SMB: User Password Brute Force Attempt' generated by PAN NGFW detected on host pc1 involving user nt	1	[•1]					

2 zooms in on this widget to highlight summarized incident details.

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.

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.

Figure 2. Enlarged View of Top Incidents Widget

Incident Management Dashboard	~
Search	
MITRE	
Threat Hunting 101	
Agent Management Dashboard	
Data Ingestion Dashboard	
Incident Management Dashboard	
Security Admin Dashboard	
Security Manager Dashboard	
Vulnerability Assessment Dashboard	

Figure 3. Dashboards Menu from the Initial Cortex XDR Screen

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.



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

Figure 4. Vulnerability Assessment Dashboard

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.

vulnerability descriptions

Vulne	rability Assessme	1t Found 23 out of 52 results (Calculated o	n Nov 24th 2021 13:42)	nunung				CVES ENDPOINTS	€ © €
Endpol	int Status = Connected,Disconnected	Host Insights + Enabled CVEs = CVE-20	21-26887						
	ENDPOINT NAME	CVES			IP ADDRESS T	SEVERITY SCORE	PLATFORM T	ENDPOINT STATUS	ENDPOINT TY
	PC24	CVE-2021-42285 CVE-2021-422	83 CVE-2021-42275 CVE-2021-41379	+ 580 More	172.16.20.103	9.9	Windows	Connected	U Worksta
	PC3	CVE-2021-42285 CVE-2021-422	83 CVE-2021-42275 CVE-2021-41379	+ 575 More	172.16.20.101	9.9	Windows	Connected	💭 Worksta
	POS-7286	CVE-2021-42285 CVE-2021-422	83 CVE-2021-42275 CVE-2021-41379	+ 575 More	172.16.25.52	9.9	Windows	Connected	💭 Worksta
	POS-7152	CVE-2021-42285 CVE-2021-422	83 CVE-2021-42275 CVE-2021-41379	+ 575 More	172.16.25.51	9.9	Windows	Connected	💭 Worksta
	PC22	CVE-2021-42285 CVE-2021-422	83 CVE-2021-42275 CVE-2021-41379	+ 580 More	172.16.20.100	9.9	Windows	Connected	💭 Worksta
	JLACEY-CTR	CVE-2021-42288 CVE-2021-422	85 CVE-2021-42284 CVE-2021-42283	+ 207 More	3.3.3.10 + 1 More	9.9	Windows	Disconnected	💭 Worksta
	MED-7369	CVE-2021-42285 CVE-2021-422	83 CVE-2021-42275 CVE-2021-41379	+ 575 More	172.16.25.53	9.9	Windows	Connected	💭 Worksta
	MED-7468	CVE-2021-42285 CVE-2021-422	83 CVE-2021-42275 CVE-2021-41379	+ 575 More	172.16.25.50	9.9	Windows	Connected	💭 Worksta
	EXCHANGE-01	CVE-2021-42291 CVE-2021-422	88 CVE-2021-42287 CVE-2021-42285	+ 125 More	172.16.40.45	9.8	Windows	Connected	🖶 Server
	RND-LAB-WIN01	CVE-2021-42288 CVE-2021-422	86 CVE-2021-42285 CVE-2021-42284	+ 97 More	172.16.90.51	9.8	Windows	Connected	💭 Worksta
	WINServer	CVE-2021-42291 CVE-2021-422	88 CVE-2021-42287 CVE-2021-42285	+ 99 More	172.16.40.15	9.8	Windows	Connected	🖯 Server
	DC1	CVE-2021-42291 CVE-2021-422	88 CVE-2021-42287 CVE-2021-42285	+ 99 More	172.16.40.20	9.8	Windows	Connected	🖯 Server
	llweb2012	CVE-2021-42291 CVE-2021-422	87 CVE-2021-42285 CVE-2021-42284	+ 70 More	172.16.60.199	9.8	Windows	Connected	🖶 Server
	EC2AMAZ-J3D3HE9	CVE-2021-42291 CVE-2021-422	88 CVE-2021-42287 CVE-2021-42285	+ 24 More	172.31.31.180	9	Windows	Disconnected	🖯 Server
	WS-FIN7	CVE-2021-26887			172.16.10.100	7.8	Windows	Connected	💭 Worksta
	EXECUTIVE-4	CVE-2021-26887			192.168.153.129	7.8	Windows	Disconnected	U Worksta
	PC1	CVE-2021-26887			172.16.20.110	7.8	Windows	Connected	U Worksta

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.

0	CORTEX XDR Reporting -	Investigation - F	esponse - Endpoints -	Rules - Add-ons - A	ssets - MTH		Quick Launcher	• Loset 03 SE-Demo Corp				
E	Endpoint Administration Found 54 out of 63 results											
(Endpoint Status - Connected Disconnected Revert											
	ENDPOINT NAME 👔 T	ENDPOINT TYPE T	ENDPOINT STATUS	OPERATING SYSTEM T	AGENT VERSION T	IP ADDRESS T	USER T	ENDPOINT ALIAS T	LAST SEEN			
	(PRO) bradshaw-dev	Server	Connected	👌 Ubuntu 16.04 LTS	7.6.0.99999999	172.16.60.224	root		Nov 24th 2			
	(PRO) bradshaw-dev20	Server	Disconnected	& Ubuntu 20.04 LTS	7.6.0.99999999	172.16.60.51	root		Nov 23rd 2			
	(PRO) centos-desktop7	Server	Connected	👌 CentOS 7.6	7.5.1.39945	172.16.30.102	root		Nov 24th 2			
	PRO DC1	Server	Connected	Windows Server 2019	7.5.1.40243	172.16.40.20	demo-corp.local\ccollier		Nov 24th 2			
	PRO EC2AMAZ-60D0COJ	Server	Disconnected	Windows Server 2019	7.5.1.40243	172.31.26.54	Administrator		Nov 4th 20			
	PRO EC2AMAZ-J3D3HE9	Server	Disconnected	Windows Server 2019	7.5.1.40243	172.31.31.180	Administrator		Nov 5th 20			
	PRO EC2AMAZ-M4I0B8B	Server	Disconnected	Windows Server 2019	7.5.1.40243	172.31.24.72	Administrator		Nov 4th 20			
	PRO EXCHANGE-01	Server	Connected	Windows Server 2019	7.5.1.40243	172.16.40.45	demo-corp.local\best1_user		Nov 24th 2			
	PRO EXECUTIVE-4	U Workstation	Disconnected	Windows 10	7.5.1.40243	192.168.153.129	John Bradshaw		Nov 22nd 2			

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.

CORTEX XDR	Reporting -	Investigation - Response - Er	ndpoints -	Rules - Add-ons - Assets - M	MTH Quick Law	incher 🔿 🔯 🕼	Upset 03 SE-Demo Corp
POLICY MANAGEMENT	Prevention Poli	CY Rules Found 19 results		Managed Threat Hunting			+ New Policy
Prevention	PLATFORM	NAME	т	TARGET	Ť	EXPLOIT T	MALWARE
Policy Rules	 Windows (13) 						
Profiles Glabal Exceptions		1 0 AWS re:Invent		endpoint in EC2AMAZ-J3D3HE9, EC2AMAZ-M4I0B8B, E	С2АМАZ-60D0COJ	Default	aws reinvent - Only Ransomware
Extensions ~		2 C NTA SE DEMO		ip address in range 172.17.0.1 - 172.17.254.254		SEDEMO-Alert-Exploit	SEDEMO-Alert-Malware
Policy Rules		3 💲 🗌 ZeroTrust - Maximum Lockdown		endpoint = PC6		ZeroTrust Exploit	ZeroTrust Malware
Profiles		4 C Tesla and BabyShark Prevent Policy		endpoint in PC7, LR-Win10-08, PC22		Default	Default
Device Permanent Exceptions Device Temporary Exceptions	8:1 Demo-Prevent-Only-Default en 6:1 Demo-Prevent-Only-BTPRuleExceptions en 7:1 Demo-Prevent-Only-BTPReportOnly en 8:1 Demo-Prevent-Only-BTPReportOnly en 9:1 Demo-Prevent-Only-BTPRLA-WF-REPORTONLY en		endpoint name contains DONOTDELETE		Default	Default	
Settings ~			endpoint name contains DONOTDELETE		Default	Default	
Device Management			endpoint name contains DONOTDELETE	endpoint name contains DONOTDELETE		Demo-Prevent-Only-BTPREPORTONL	
			endpoint name contains Prevent-01, DONOTDELETE, Pre-	vent-hlarsson, prevent-nampofo	Default	Demo-Prevent-Only-BTP-LA-WF-REP	
		9 1 Script Use Case		endpoint name = rza-laptop		SEDEMO-Alert-Exploit	SEDEMO-Alert-Malware
		10 C SE-Alert-Policy-LiveResponse		group names = LiveResponse Endpoints		SEDEMO-Alert-Exploit	SEDEMO-Alert-Malware
		11 2 SEDEMO Cloud-Based Agents		is cloud agent = True		SEDEMO-Alert-Exploit	SEDEMO-Alert-Malware
		12 : SEDEMO-Alert-Policy		(group names = VLAN20-Users, VLAN25-Operations, VLA	N30-ITAdmin, VLAN90-Secure, VLAN60-DMZ, VLAN10-Guests, VLAN40-E	SEDEMO-Alert-Exploit	SEDEMO-Alert-Malware
		13 Windows Default		Any		Default	Default
	• 🏟 macOS (2)						
		1 \$ SE Demo MacOS		endpoint status != Uninstalled AND platform = macOS		SE-Demo-Report-MacOS	SE-Demo-Report MacOS
		2 macOS Default		Any		Default	Default
	 ▲ Linux (3) 						
		1 C SEDEMO Linux Cloud-Based Agents		is cloud agent = True		SEDEMO-Alert-Exploit	SEDEMO-Alert-Malware
		2 C SEDEMO-Alert-Policy		group names = Platform is Linux-based		SEDEMO-Alert-Exploit	SEDEMO-Alert-Malware
		3 Linux Default		Any		Default	Default
	 Android (1) 						
		1 Android Default		Any		N/A	Default

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.

Figure 7. Prevention Policy Rules

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.

CORTEX XDR Reporting - Inves	estigation - Response - Endpoints - Rul	es • Add-ons • Assets • MTH	Quick Launcher	Image: Wight of the second s
Incidents Found 13 out of 1.435 results		Managed Threat Hunting		Alerts Table 📑 🔕 😴 🗮 🚦
Status = New,Under Investigation Last Updated = Last 30D (Oct 25th 2021 18:46:15 - 1	Nov 24th 2021 17:46:15)			
Sort: Last Updated ~ 4	High 🗸 ☆ ID - 1366 Spear-Phish w/Quasar and DarkCo	met	x Score 365	& Unassigned v New v :
Updated 10 hours ago U st. Unassigned U St97 SMB: User Password Brute Force Attempt' generated by PAN NGFW detected on host pc1 involving user nt authority'system	'Behavioral Threat' along with 95 other alerts genera Alerts Sources: () ⓒ 쇼 4 역	ted by PAN NGFW, XDR Agent, XDR BIOC, XDR Analy	vtics BIOC and XDR Analytics detected on 4 hosts invol. 5 Users 2 Wildfire H	Legocy view Advanced view Feedback We'd love to hear your feedback on the x advanced Incident View
□ pc1	Overview 🖈 Timeline Alerts & Insight	ts Key Assets & Artifacts Executions		
Updated 12 hours ago	Incident by MITRE ATT&CK* 7 Tactics and 12 Techniques 0 0 0 Reconnaissance Resource Development Initial Access E	11 0 0 7 Execution Persistence Privilege Escalation Defense Evasi	18 23 0 ion Credential Access Discovery Lateral Movement C	Include Incident Insights O S I Command and Control Exfittration Impact
□ pc1 + 3	Timeline	v		Show More
Updated a day ago	Created on Sep 24th 2021 08:52:08	Last alert added on S	Sep 28th 2021 14:22:34	Our Unassigned on Oct 31st 2021 11:28:39
ID 1558 'Suspicious Input Deserialization' along with 1 other alert generated by XDR Agent detected on host ubuntu16-test-ran involving	Alerts Show More	Sources Show More	Hosts Show More	Users Show More
Ubuntu16-test-ran & tomcat8	Total 96	Total 5	Total 4	Total 5
Updated a day ago		Image: block of the state of the	⊘ ^Щ pc1 ★ :	A nt authority\system
ID 1384 'Behavioral Threat' along with 14 other alerts generated by XDR Agent and XDR Analytics detected on host ec2amaz-i0jrv0d involving 3			pc2	demo-corp\wsanchez ★
c2amaz-l0jrv0d			ws-it10	demo-corp\cshadwick 🖈
Updated a day age Image: Image: Score 275 & Unassigned Image: Im			172.16.20.110	∴ demo-corp.local\ccollier ★
Updated a day ago	Low 3	Alers Sources PAN NGF/Y 6 Q XDR Analytic 3		
Key Cloud Infrastructure Breach - Admin Endpoint ID 1313 'Quasar RAT Command and Control Traffic Detection' along with	Medium 59 High 34	<u>+ 2 More</u>		e

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

Figure 8. Incidents Tab with Focus on a Detected Spearphish 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.

High 🗸 🖞 ID - 1366 Spear-Phish w/Quasar and DarkCornet	Score 365 & Unassigned V New v I
'Behavioral Threat' along with 95 other alerts generated by PAN NGFW, XDR Agent, XDR BIOC, XDR Analytics BIOC and XDR Analytics de	etected on 4 hosts invol Legacy view 💽 Advanced view Feedback
Sources: () () () () () () () () () () () () ()	We'd love to hear your feedback on the × advanced Incident View
Overview 🖈 Timeline 🖈 Alerts & Insights Key Assets & Artifacts Executions	
Filter: All > 1 Sep 28th 16:07 Quasar RAT Command and Control Traffic Detection from 172.16.20.110 was added to the incident because it involves the same remote IP a	address: 2.2.2.199
 Sep 27th 13:52 2 alerts from pc1 were added to the incident because they relate to the same processes causality chain 4 Additional artifacts found > 	
 Sep 27th 13:50 2 alerts from ws-it10 were added to the incident because they relate to the same processes causality chain 4 Additional artifacts found > 	
 Sep 27th 13:49 2 alerts from pc2 were added to the incident because they relate to the same processes causality chain 4 Additional artifacts found > 	
Sep 27th 13:47 Windows Event Log cleared using wevtutil.exe from pc1 was added to the incident because it relates to the same processes causality chain Additional artifacts found >	
 Sep 27th 13:45 Windows Event Log cleared using wevtutil.exe from ws-it10 was added to the incident because it relates to the same processes causality cha Additional artifacts found > 	in

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.

Figure 9. Timeline from the Spearphishing Incident 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.

High V 🏠 ID - 1366 Spear-Phish w/Quasar and DarkComet 'Behavioral Threat' along with 95 other alerts generated by P.	AN NGFW. XDR Agent. XDR BIOC. XDR	Analytics BIOC and XDR Analytics of	Score 365 & Unas	ssigned Vew I Equation I Advanced view Feedback
Alerts Sources: 1 @ A 24 Q	4 Hosts	5 Users	2 Wildfire Hits	We'd love to hear your feedback on the × advanced Incident View
Overview 🖈 Timeline Alerts & Insights	Key Assets & Artifacts 🦸 Exect	utions		
Artifacts (33) Search Q		Hosts (4) Search	٩	
QuasarClient.exe (b7b62d74 🖻) 🛆 25	× Unsigned	Select All		
WF 💂 Malware 🕜	VT Unknown • 15 • 9 • 1	🗆 🎯 📜 pc1 🖈		:
DogBark.exe (1037a554 🕅) 🛆 24	× Unsigned	172.16.20.110 AD Grou	<u>ps</u> demo-corp.local/Domain Computers	• 15 • 25 • 1
WF 💂 Malware 🕜	VT Unknown • 9 • 15	□ ⊚		:
cmd.exe (e5cc891e)) △ 41	✓ Microsoft Corporation	172.16.20.102 AD Grou	<u>ps</u> demo-corp.local/Domain Computers + 1	• 10 • 17 • 1
WF Benign @	VT 0/65 • 18 • 22 • 1	□ o [∰] ws-it10		:
7zFM.exe (e81b7316) △ 38	× Unsigned	172.16.30.100 AD Grou	<u>ps</u> demo-corp.local/Domain Computers + 1	• 8 • 17 • 1
WF Benign 💷 🕜	VT 0/67 • 14 • 23 • 1	172.16.20.1	10	÷
cmd.exe (4d895e22) △ 19	✓ Microsoft Corporation			•1
WF Benign @	VT 0/66 • 7 • 11 • 1	Users (5) Search	Q	
net.exe (a0d21f56) △ 15	✓ Microsoft Corporation	A nt authority\syste	m	:
WF Benign @	VT 0/67 • 14 • 1			•1 •2
procdump64.exe (16f475a5 ۗ) △ 10	✓ Microsoft Corporation	A demo-corp\wsanc	hez \star	:
WF Benign @ AF 34445.gsrt_malim_enum_thre +3	VT 0/67 • 6 • 4	AD Groups demo-corp.loca	al/Human Resources + 8	•7 •17 •1
net.exe (7c4cff42ⓑ) △ ⁸	✓ Microsoft Corporation	A demo-corp\cshad	wick 💌	:
WF Benign @	VT 0/62 • 7 • 1	AD Groups demo-corp.loca	al/Domain Admins + 8	• 6 • 17 • 1

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.

B	ligh ↓ ehavioi	☆ ID - 1366 Spear-Phish ral Threat' along with 95 o	h w/Quasar and DarkCome	t d by PAN NGFW, XDR Agen	nt, XDR BIOC, XDR Ana	lytics BIOC and XDR Analyti	Score 365	🐁 Unassigned 🔹 New Legacy view 💽 Advanced vie	w Feedback
(96 Alerts	Sources: 🗊 🍥 🛕 🏕 Q		4 Hosts		5 Users	2 Wildfire Hit	We'd love to hear your feedback o advanced Incident View	on the \times
01	verview	★ Timeline	Alerts & Insights	* Key Assets & Artifa	ects Executions	5			HI E
	96 Ale	rts 131 Insight	S					a	© 🕝 :
		TIMESTAMP 🕽 🔭	HOST T	USER NAME Y	SEVERITY T	ALERT SOURCE T	ACTION T	CATEGORY	ALERT NAM
		Sep 28th 2021 14:22:34		demo-corp\ccollier	High	PAN NGFW	 Detected (Raised An Alert) 	Spyware Detected via Anti-Spyware profile	Quasar RA1
•		Sep 27th 2021 13:47:41	PC1	DEMO-CORP\ccollier	High	A XDR Analytics BIOC	O Detected	Impact	Windows E
		Sep 27th 2021 13:47:32	PC1	DEMO-CORP\ccollier	High	A XDR Analytics BIOC	O Detected	Impact	Windows E
		Sep 27th 2021 13:47:17	PC1	DEMO-CORP\ccollier	High	A XDR Analytics BIOC	O Detected	Impact	Windows E
•		Sep 27th 2021 13:44:57	WS-IT10	DEMO-CORP\cshadwick	High	A XDR Analytics BIOC	O Detected	Impact	Windows E
		Sep 27th 2021 13:44:53	WS-IT10	DEMO-CORP\cshadwick	High	A XDR Analytics BIOC	Oetected	Impact	Windows E
		Sep 27th 2021 13:44:47	WS-IT10	DEMO-CORP\cshadwick	High	A XDR Analytics BIOC	O Detected	Impact	Windows E
•		Sep 27th 2021 13:44:17	PC2	DEMO-CORP\wsanchez	High	A XDR Analytics BIOC	Oetected	Impact	Windows E
•		Sep 27th 2021 13:44:10	PC2	DEMO-CORP\wsanchez	High	A XDR Analytics BIOC	O Detected	Impact	Windows E
•		Sep 27th 2021 13:44:04	PC2	DEMO-CORP\wsanchez	High	A XDR Analytics BIOC	Oetected	Impact	Windows E
•		Sep 27th 2021 13:11:51	WS-IT10	DEMO-CORP\cshadwick	Medium	O XDR Agent	Oetected (Reported)	Malware	WildFire Ma
•		Sep 27th 2021 13:11:48	WS-IT10	DEMO-CORP\cshadwick	Medium	XDR Agent	 Detected (Reported) 	Malware	Suspicious I
•		Sep 27th 2021 13:11:48	WS-IT10	DEMO-CORP\cshadwick	Medium	O XDR Agent	Oetected (Reported)	Malware	WildFire Ma
•		Sep 27th 2021 13:11:45	WS-IT10	N/A	High	XDR Agent	 Detected (Reported) 	Malware	Behavioral*
		Sep 27th 2021 13:11:45	WS-IT10	DEMO-CORP\cshadwick	Medium	O XDR Agent	Oetected (Reported)	Malware	WildFire Ma
•		Sep 27th 2021 13:11:45	WS-IT10	DEMO-CORP\cshadwick	Medium	XDR Agent	 Detected (Reported) 	Malware	Suspicious I
		Sep 27th 2021 13:11:44	WS-IT10	DEMO-CORP\cshadwick	High	▲ XDR BIOC	O Detected	Credential Access	* Comman
		Sep 27th 2021 13:11:44	WS-IT10	DEMO-CORP\cshadwick	High	▲ XDR BIOC	O Detected	Credential Access	★ Mimikat
		Sep 27th 2021 13:11:42	WS-IT10	DEMO-CORP\cshadwick	Medium	XDR Agent	Detected (Reported)	Malware	Suspicious I
•		Sep 27th 2021 13:11:41	WS-IT10	DEMO-CORP\cshadwick	Medium	▲ XDR BIOC	Oetected	Credential Access	* Dumpin
		Sep 27th 2021 13:11:41	WS-IT10	DEMO-CORP\cshadwick	High	A XDR BIOC	O Detected	Credential Access	* Possible
		Sep 27th 2021 13:11:38	WS-IT10	DEMO-CORP\cshadwick	Low		Detected	Discovery	Multiple dis
		Sep 27th 2021 13:11:38	WS-IT10	DEMO-CORP\cshadwick	Medium	A XDR Analytics BIOC	O Detected	Discovery	Uncommon
		Sep 27th 2021 13:11:38	WS-IT10	DEMO-CORP\cshadwick	Medlum	A XDR Analytics BIOC	O Detected	Discovery	Uncommon
		Sep 27th 2021 13:11:38	WS-IT10	DEMO-CORP\cshadwick	Medium	A XDR Analytics BIOC	O Detected	Discovery	Uncommon
		Sep 27th 2021 13:11:38	WS-IT10	DEMO-CORP\cshadwick	Medium	A XDR Analytics BIOC	O Detected	Discovery	Uncommon
		Sep 27th 2021 13:11:38	WS-IT10	DEMO-CORP\cshadwick	Medium	A XDR Analytics BIOC	Oetected	Discovery	Uncommon
		Sep 27th 2021 13:11:38	WS-IT10	DEMO-CORP\cshadwick	Medium	A XDR Analytics BIOC	O Detected	Discovery	Uncommon
		Sep 27th 2021 13:11:37	WS-IT10	DEMO-CORP\cshadwick	Medium	A XDR Analytics BIOC	O Detected	Discovery	Uncommon

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. Figure 11. Alerts & Insights Tab from the Spearphishing Incident 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.



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-bystep 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.

Figure 12. Causality Chain for an Investigation

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.

CORTEX XDR Reporting - Investigation - Res	esponse - Endpoints - Rules - Add-ons - Assets - MTH	Quick Launcher 🕥 🔞 🕼 Upset 03 SE-Demo Corp
Managed Threat Hunting Found 6 results	Managed Threat Hunting	Type your search here C
Sort: Type 🗸 🔐	Hun Threat Report #1095901	Threat Report
Threat Report #1084439 Sep 14th 2021 00.28 Dear SE-Demo Corporation. The Cortex XDR Managed Threat Hunting team is constantly searching for suspicious Threat Report	Dear SE-Demo Corporation, The Cortex XDR Managed Threat Hunting team has detected the execution of Quasar malw. The malware was executed by user ' DEMO-CORPIjmiller ' Throughout Sep 9th 2021 17:24:5	are in your environment on host ' PC4 '. 9 - Sep 9th 2021 17:24:59.
ManageEngine ADSelfService Plus Vulnerability (CVE-202 Sep 17th 2021 16:13 Status: Not Impacted Dear team, As we continue to identify new threats in the wild, we understand that your first concern is whether these threats have impacted your environment. To address this, whenever such threats are identified, we automatically Impact Report	This malware is known to connect to command and control servers, use persistence mechani Attachments Threat Report SE Demo Corp.pdf 273KB	isms, and executes reconnaissance commands and dumps credentials.
Monthly Status Report #1089811 Oct 4th 2021 12:19 Dear SE-Demo Corporation team,	Comments Add Your comment here	
Please find the attached report for summarizing the Cortex XDR Managed Threat Monthly Status Report		Attach File Add
Threat Inquiry #1090527 Sep 22nd 2021 03:37 Dear SE-Demo Corporation.		
The Cortex XDR Managed Threat Hunting Team has identified suspicious activity in yo Threat inquiry		
It Threat Report #1095901 Oct 4th 2021 08:30 Dear SE-Demo Corporation, Item Corporation, Item Corporation,		
The Cortex XDR Managed Threat Hunting team has detected the execution of Quasar		

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. Figure 13. Managed Threat Hunting Capabilities

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.

CORTEX XDR	Reporting -	Investigation -	Response - Endpoints - Rules - Add-ons - Assets -	MTH Quick Launcher	o 🔅 🔑	Jpset 03 SE-Demo Corp
ACTION CENTER	All Actions Found	302 results	Managed Threat Hunting		e,	() + New Action () :
All Actions	CREATION TIME J	ACTION TYPE T	DESCRIPTION	STATUS Y	CREATED BY T	EXPIRATION DATE T
Currently Applied Actions	Nov 24th 2021 04:06:55	Live Terminal	Initiate Live Terminal on LR-Win10-03	Completed Successfully	L Oykun Satis	
File Quarantine Block List	Nov 24th 2021 01:18:38	Live Terminal	Initiate Live Terminal on LR-Win10-01	Completed Successfully	👤 Yi Mo Cai	
Allow List	Nov 23rd 2021 15:54:14	Live Terminal	Initiate Live Terminal on centos-desktop7	Completed Successfully	L Kyle Chugg	
Endpoint Isolation	Nov 23rd 2021 13:42:52	Live Terminal	Initiate Live Terminal on PC-NTA-100	Completed Successfully	2 David Englert	
External Dynamic List	Nov 23rd 2021 09:45:26	Support File Retrieval	Retrieve support file from bradshaw-dev20	Completed Successfully	1 John Bradshaw	
Endpoint Blocked IP Addresses	Nov 23rd 2021 09:01:57	Agent Uninstall	Uninstall agent on bradshaw-dev20	Completed Successfully	2 John Bradshaw	
	Nov 23rd 2021 03:19:44	Live Terminal	Initiate Live Terminal on LR-Win10-07	Completed Successfully	L Oykun Satis	
	Nov 22nd 2021 13:51:06	File Search	File search by hash: 8f163384 on 38 endpoints (eligible for file search)	In Progress (2 Pending, 36 Completed Successfully)	Ryan Whalen	Nov 26th 2021 13:51:06
	Nov 22nd 2021 13:34:23	File Search	File search by hash: a6b023c7 on 37 endpoints (endpoint status = Connected, Disconnected)	In Progress (2 Pending, 35 Completed Successfully)	Ryan Whalen	Nov 26th 2021 13:34:23
	Nov 22nd 2021 13:31:22	File Search	File search by hash: 1037a554 on 38 endpoints (endpoint status = Connected, Disconnected)	C In Progress (2 Pending: 36 Completed Successfully)	2 Ryan Whalen	Nov 26th 2021 13:31:22
	Nov 22nd 2021 13:16:30	Live Terminal	Initiate Live Terminal on PC7	S Completed Successfully	L Ryan Santeco	
	Nov 22nd 2021 08:48:49	Agent Uninstall	Uninstall agent on EXECUTIVE-4	S Completed Successfully	2 John Bradshaw	
	Nov 19th 2021 12:29:33	Live Terminal	Initiate Live Terminal on ip-192-168-60-154.us-east-2.compute.internal	S Completed Successfully	Raymond DePalma	
	Nov 19th 2021 11:56:33	Live Terminal	Initiate Live Terminal on centos-desktop7	S Completed Successfully	L Wanjiru Allen	
	Nov 19th 2021 11:26:31	Agent Uninstall	Uninstall agent on ip-10-99-2-10 and 6 other endpoints	Completed Successfully (7 Completed Successfully)	1 John Bradshaw	
	Nov 18th 2021 09:38:57	Live Terminal	Initiate Live Terminal on PC7	S Completed Successfully	Ryan Santeco	
	Nov 17th 2021 15:49:47	Live Terminal	Initiate Live Terminal on LR-Win10-01	Completed Successfully	Barry Rosenberg	
	Nov 17th 2021 14:56:33	File Search	File search by hash: 4d895e22 on 38 endpoints (eligible for file search)	Completed with partial success (35 Completed Successfully, 3 Expired)	Raymond DePalma	
	Nov 17th 2021 14:43:44	File Search	File search by hash: $61a92b58 \mbox{ on } 38 \mbox{ endpoints}$ (eligible for file search)	Completed with partial success (35 Completed Successfully, 3 Expired)	Raymond DePalma	
	Nov 17th 2021 14:34:52	File Search	File search by hash: 4d895e22 on WS-IT20 and 37 other endpoints	Completed with partial success (35 Completed Successfully, 3 Expired)	2 Raymond DePalma	
	Nov 17th 2021 14:33:16	Live Terminal	Initiate Live Terminal on PC7	Completed Successfully	2 Ryan Santeco	60
	Nov 17th 2021 14:07:54	File Search	File search by hash: 4d895e22 on 38 endpoints (eligible for file search)	Completed with partial success (35 Completed Successfully, 3 Expired)	2 Raymond DePalma	U

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.

Figure 14. Action Center

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.

De	ailed Results - File Search (I	D 294)				×							
Ai Fil	Action Parameter Include Deleted Files Creation Time Status Target File Search Hosh: 4d89(r54d5)(079babd022271:58509477b/41e834e46b991deau0530)(db2527 Fale Nov 17th 2021 14:56:33 Completed with partial success (35 Completed Successfully, 3 Expired) WS-IT20 and 37 other endpoints (eligible for file search)												
F	ile Search Found 9 results	(Showing first 100 file instances fro	n every endpoint)		BY FILE BY ENDPOINT	•							
	ENDPOINT NAME T	IP ADDRESS T	FILE PATH T	FILE NAME T	5HA256 T	MD5							
	PC-NTA-100	172.17.20.52	C:\Windows\SysWOW64\cmd.exe	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22	d0fce3afa							
	WS-IT10	172.16.30.100	C:\Windows\System32\cmd.exe	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22	d0fce3afa							
	RND-LAB-WIN01	172.16.90.51	C:\Windows\SysWOW64\cmd.exe	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22	d0fce3afa							
	PC7	172.16.20.108	C:\Windows\WinSxS\wow64_microsoft-windows-commandprompt_31bf3856ad364e35_10.0.19041.746_none_735abbdba	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22	d0fce3afa							
	PC4	172.16.20.104	C:\Windows\System32\cmd.exe	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22								
	WS-IT20	172.16.30.103	C:\Windows\System32\cmd.exe	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22 d0								
	PC5	172.16.20.105	C:\Windows\System32\cmd.exe	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22								
	PC6	172.16.20.107	C:\Windows\SysWOW64\cmd.exe	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22	d0fce3afa							
	GP-PC1	3.3.3.11 + 1 More	C:\Windows\WinSxS\wow64_microsoft-windows-commandprompt_31bf3856ad364e35_10.0.19041.746_none_735abbdba	cmd.exe	4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22	d0fce3afa							

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.

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

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.

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.

			Reporting -	Inv	vestigation +	Respons	se - En	dpoints ·	Rules -	Add-or	ns -	Assets -	мтн			Quick Launcher 🕥 🕼 🕼 Upset 03 SE-Demo Corp				
FORENSICS	<	S	earch Found 9 results	s						Manager	d Threat Hur	nting				€, Ø () :				
Searches			CREATED L	٣	NAME	т	TYPE	т	RESULTS COUNT	Ŧ	HOSTS	SEARCHED	т	LAST UPDATED	Ŧ	SUMMARY				
Search Collections			Nov 17th 2021 07:36:41		Authentication Ev	ents	Event Logs							Oct 21st 2021 19:10	:20	Event Channel: "Security", Event ID: "4624", "4625", "4634", "4648", "4672", "4768", "4769"				
Host Timelines Process Execution			Nov 17th 2021 07:36:16	5	PSExec Service		Event Logs							Oct 21st 2021 19:11	:34	Event Channel: "System", Event ID: "7045"				
Process Execution Artifacts	>		Nov 17th 2021 07:36:16	5	RDP Events		Event Logs							Oct 21st 2021 19:14	:49	Event Channel: "Microsoft-Windows-TerminalServices-LocalSessionManager/Operational", Event ID: "21"				
File Access			Nov 17th 2021 07:36:16	5	Large File in Temp		File							Oct 21st 2021 19:22	:48	Path: "C:\Windows\Temp*", "C:\Users*\AppData\Local\Temp*", Greater or equal to: "314572800"				
File Access Artifacts	>		Nov 17th 2021 07:36:16	5	PSExec Key		Registry							Oct 21st 2021 19:15	:58	Path: "HKEY_USERS\"\SOFTWARE\SysInternals\PSEXEC\""				
Persistence Persistence Artifacts	,		Nov 17th 2021 07:36:15	5	Exes in Temp		File							Oct 21st 2021 19:19	:39	Path: "C:*.exe", "C:\Users*\AppData\Local\Temp*.exe", "C:\Windows\Temp*.exe"				
Command History			Nov 17th 2021 07:36:14	1	WMI Persistence		Event Logs							Oct 21st 2021 19:17	:10	Event Channel: "Microsoft-Windows-WMI-Activity/Operational", Event ID: "5861"				
Command History Artifacts	>		Nov 17th 2021 07:36:14	1	Malicious Service		Event Logs							Oct 21st 2021 19:24	:39	Event Channel: "System", Event ID: "7045", Message: "COMSPEC"				
Network			Oct 21st 2021 19:05:18		Authentication Ev	ents	Event Logs							Oct 21st 2021 19:04	:10	Event Channel: "Security", Event ID: "4624", "4625", "4634", "4648", "4672", "4768", "4769"				
Network Artifacts	,																			
Remote Access Artifacts	>																			
Triage	>																			

Copy Files / Directories Download Delete 2 Open in VirusTotal Get WildFire verdict Get file hash Mark as interesting Copy Value

Rename

Move

Figure 17. Actions in Live Terminal File Explorer

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.

		Reporting -	Investigation -	Respor	nse - Endp	oints -	Rules -	Add-ons	- Assets -	мтн	Quick Launcher 💽 🕸 🕼 Upset 03 SE-Demo Corp							
FORENSICS	K	Host Timeline	e Found 3,639,942 results					Managed Th	Managard Theorem Phonology 💿 🕞 🗇 🕞									
Searches Search Collections		HOSTNAME T PC-NTA-100	GENERATED TIME Oct 22nd 2021 15:29:38	Ŧ	TIMESTAMP 🚦	T CC:C	DESCRIPTION Expiration Time	т	TYPE T Windows Activi	USER T	DATA Y							
Host Timelines		PC-NTA-100	Oct 10th 2021 14:07:44		Dec 16th 2026 13:4	2:14	Link Date		Amcache		c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.1081_none_7e3d47227c69							
Process Execution		PC-NTA-100	Oct 10th 2021 14:07:44		Oct 27th 2026 23:0	5:04	Link Date		Amcache		c:\windows\system32\mousocoreworker.exe							
File Access	,	PC-NTA-100	Oct 22nd 2021 15:29:38		Aug 7th 2026 12:47	:47	Expiration Time		Windows Activi		microsoft.default.default							
File Access Artifacts	,	PC-NTA-100	Oct 22nd 2021 15:29:38		Jul 7th 2026 07:49:3	35	Expiration Time		Windows Activi		microsoft.default.default							
Persistence		PC-NTA-100	Oct 22nd 2021 15:29:38		Jul 7th 2026 05:25:1	15	Expiration Time		Windows Activi	PC-NTA-100\root	microsoft.default.default							
Persistence Artifacts	`	PC-NTA-100	Oct 22nd 2021 15:29:21		Oct 17th 2025 23:4	5:24	Link Date		Amcache		c:\windows\system32\compattelrunner.exe							
Command History		PC-NTA-100	Oct 10th 2021 14:07:44		Oct 17th 2025 23:4	5:24	Link Date		Amcache		c:\windows\system32\compattelrunner.exe							
Network		PC-NTA-100	Oct 24th 2021 10:44:35		Nov 17th 2021 08:0	9:57	Expiry Time		Internet Explore	ccollier.NTA-DE	:2021102220211023: ccollier@windowsdefender://threat/							
Network Artifacts	>	PC-NTA-100	Oct 24th 2021 10:44:35		Nov 17th 2021 08:0	9:57	Expiry Time		Internet Explore	ccollier.NTA-DE	Visited: ccollier@windowsdefender://threat/							
Remote Access		PC-NTA-100	Oct 24th 2021 10:44:35		Nov 17th 2021 08:0	9:57	Expiry Time		Internet Explore	ccollier.NTA-DE	:2021102220211023: ccollier@windowsdefender://account/							
Remote Access Artifacts	`	PC-NTA-100	Oct 24th 2021 10:44:35		Nov 17th 2021 08:0	9:57	Expiry Time		Internet Explore	ccollier.NTA-DE	Visited: ccollier@windowsdefender://account/							
All		PC-NTA-100	Oct 24th 2021 10:44:35		Nov 16th 2021 15:1	7:10	Expiry Time		Internet Explore	ccollier.NTA-DE	:2021102120211022: ccollier@windowsdefender://network/							
File		PC-NTA-100	Oct 24th 2021 10:44:35		Nov 16th 2021 15:1	7:10	Expiry Time		Internet Explore	ccollier.NTA-DE	Visited: ccollier@windowsdefender://network/							
Registry		PC-NTA-100	Oct 24th 2021 10:44:35		Nov 16th 2021 15:0	9:35	Expiry Time		Internet Explore	ccollier.NTA-DE	:2021102120211022: ccollier@windowsdefender://account/							
Event Logs Browser History		PC-NTA-100	Oct 24th 2021 10:44:35		Nov 16th 2021 07:5	0:45	Expiry Time		Internet Explore	ccollier.NTA-DE	Visited: ccollier@https://login.live.com/oauth20_authorize.srf?client_id=00000000480728C5&scope=service::ssl.live.com::M							
Volatile		PC-NTA-100	Oct 24th 2021 10:44:35		Nov 16th 2021 07:5	0:45	Expiry Time		Internet Explore	ccollier.NTA-DE	:2021102120211022: ccollier@https://login.live.com/oauth20_authorize.srf?client_id=00000000480728C5&scope=service:							
Configurations		PC-NTA-100	Oct 24th 2021 10:44:35		Nov 16th 2021 07:5	0:45	Expiry Time		Internet Explore	ccollier.NTA-DE	:2021102120211022: ccollier@https://login.live.com/oauth20_desktop.srf?lc=1033							

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. Figure 19. Host Timeline from the Forensics Add-On 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	ound 166 results			Managed	hreat Hunding		🗐 🔿 🕞 :
HOSTNAME T	GENERATED TIME	EVENT GENERATED	Ŧ	EVENT ID T	MESSAGE T	SOURCE T	USER
PC-NTA-100	Nov 17th 2021 07:36:16	Sep 14th 2021 23:04	09	23	Remote Desktop Services: Session logoff succeeded:	${\it Microsoft-Windows-TerminalServices-LocalSessionManager/Operational}$	NTAUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Oct 21st 2021 08:49:	26	21	Remote Desktop Services: Session logon succeeded:	${\it Microsoft-Windows-Terminal Services-Local Session Manager/Operational}$	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:	${\it Microsoft-Windows-Terminal Services-Local Session Manager/Operational}$	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:	${\it Microsoft-Windows-Terminal Services-Local Session Manager/Operational}$	NT AUTHORITY\SYSTEM
PC-NTA-100	Nov 17th 2021 07:36:16	Aug 5th 2021 13:30:4	1	21	Remote Desktop Services: Session logon succeeded:	${\it Microsoft-Windows-Terminal Services-Local Session Manager/Operational}$	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:	${\it Microsoft-Windows-Terminal Services-Local Session Manager/Operational}$	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:	${\it Microsoft-Windows-Terminal Services-Local Session Manager/Operational}$	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:	${\it Microsoft-Windows-Terminal Services-Local Session Manager/Operational}$	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:	${\sf Microsoft-Windows-TerminalServices-LocalSessionManager/Operational}$	NT AUTHORITY\SYSTEM

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 -	Respon	se - Endpoints -	Rules -	Add-on	s - Assets -	MTH	ł	Quick Launs	her 🔿 🔯 🕼 s	lpset 03 E-Demo Corp	
FORENSICS	4	Remote Access Found 47,374 results													
Searches			HOSTNAME T	TIMESTAMP 💱	٣	DESCRIPTION T	TYPE	٣	USER	٣	SOURCE HOST	CONNECTION TYPE	CONNECTION ID T	MESSAGE T	DURAT
Search Collections			EXCHANGE-01	Nov 23rd 2021 18:00	:00	Access Date	User Access Loggi	ing	nt service\sqltelemetry		127.0.0.1		N/A	Access Count: 76	N/A
Process Execution			EXCHANGE-01	Nov 23rd 2021 18:00	:00	Access Date	User Access Loggi	ing	nt service\sqlserveragent		127.0.0.1		N/A	Access Count: 8	N/A
Process Execution Artifacts	,		llweb2012	Nov 23rd 2021 18:00	:00	Access Date	User Access Loggi	ing	sedemo\llweb2012\$::1	File Server	N/A	Access Count: 297	N/A
File Access			WINServer	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing	demo-corp\pc-win11-51\$		172.16.20.112		N/A	Access Count: 7	N/A
File Access Artifacts	`		DC1	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing	demo-corp\ccollier		172.16.40.20		N/A	Access Count: 8	N/A
Persistence Persistence Artifacts	,		DC1	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing	demo-corp\ws-it10\$		172.16.30.100	File Server	N/A	Access Count: 9	N/A
Command History			DC1	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing			172.16.20.110	DHCP Server	N/A	Access Count: 332	N/A
Command History Artifacts	,		WINServer	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing	demo-corp\pc2\$		172.16.20.102	File Server	N/A	Access Count: 57	N/A
Network			DC1	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing	demo-corp\pos-7286\$		172.16.25.52		N/A	Access Count: 182	N/A
Remote Access	,		WINServer	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing	demo-corp\ltodd		172.16.30.103		N/A	Access Count: 1	N/A
Remote Access Artifacts	÷		DC1	Nov 22nd 2021 18:00	0:00	Access Date	User Access Loggi	ing	demo-corp\jlacey-ctr\$		3.3.3.10		N/A	Access Count: 34	N/A
LogMeln			DC1	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing			172.16.20.105	DHCP Server	N/A	Access Count: 331	N/A
TeamViewer			DC1	Nov 22nd 2021 18:00	0:00	Access Date	User Access Loggi	ing			172.16.25.50	DHCP Server	N/A	Access Count: 330	N/A
Triage	,		WINServer	Nov 22nd 2021 18:00	00:00	Access Date	User Access Loggi	ing	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 Loggi	ing			172.16.25.51	DHCP Server	N/A	Access Count: 331	N/A

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

RDP Activity

Figure 20. Forensic Search of



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:



