CORTEX XDR

Breaking the Security Silos for Detection and Response

Security teams face a dizzying array of threats, from ransomware and cyberespionage to fileless attacks and damaging data breaches. However, the biggest headache for many security analysts is not the endless number of risks that dominate news headlines but the frustrating, repetitive tasks they must perform every day as they triage incidents and attempt to whittle down an endless backlog of alerts.

This paper describes the thorniest challenges security analysts confront, including a deluge of alerts and complex investigation processes that can overwhelm even the most mature security operations centers. It then proposes a framework to tackle every stage of security operations with Cortex XDR™ for detection and response. As the specters of malware, targeted attacks, and insider abuse continually escalate, tools like Cortex XDR can be your secret weapon to eliminate threats and simplify operations.

Analysts Under Siege

Security teams today face two daunting challenges: a continual barrage of attacks and an endless sea of alerts. Security teams know threat actors can launch an unlimited number of attacks, consequence-free, until one succeeds. To reduce the possibility of an intrusion, teams typically deploy multiple layers of security, but these tools generate a massive number of alerts—174,000 alerts per week on average.[1]

To keep up with all these alerts, analysts often operate in firefighting mode, attempting to triage as many alerts as possible every day. Because these alerts often lack essential context needed for investigations, analysts are forced to waste valuable time chasing down additional details. Overwhelmed by inaccurate and incomplete alerts, security teams can only review 12,000 alerts per week,[2] leaving 93% of alerts ignored and increasing business risk.

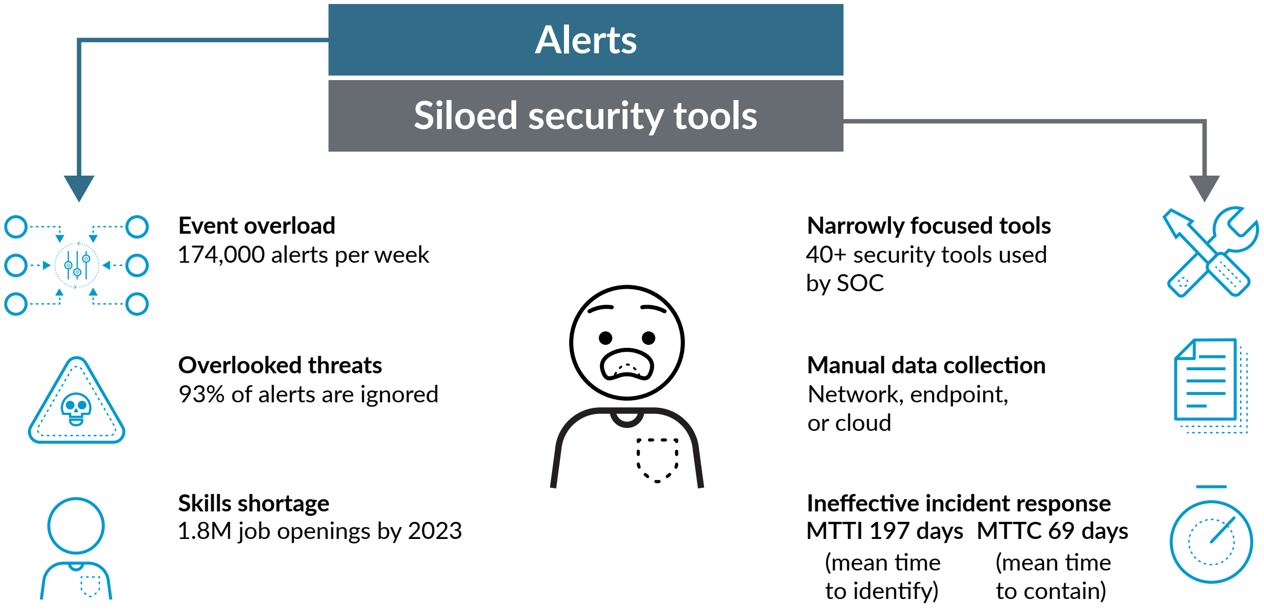

Alerts
Siloed security tools
Event overload
174,000 alerts per week
Overlooked threats
93% of alerts are ignored
Skills shortage
1.8M job openings by 2023
Narrowly focused tools
40+ security tools used by SOC
Manual data collection
Network, endpoint, or cloud
Ineffective incident response
MTTI 197 days (mean time to identify)
MTTC 69 days (mean time to contain)

Figure 1: A security analyst's many burdens

Looking for Threats in All the Wrong Places

The rising tide of attacks has convinced organizations of all sizes to embrace detection and response. To address this newfound demand, the IT security industry has introduced a slew of siloed tools, such as endpoint detection and response (EDR), network traffic analysis (NTA), and user and entity behavior analytics (UEBA). However, these tools provide a narrow view of activity and require years of specialist experience to operate.

Organizations are left with two unappealing choices: deploy a jumble of disconnected detection and response products or rely solely on existing prevention products to identify hard-to-detect threats in real time.

Organizations that choose to provision siloed tools will be burdened with the costs of deploying and maintaining new network sensors and endpoint agents everywhere. On the other hand, organizations that depend on their prevention tools for detection will likely overlook stealthy attacks, such as highly evasive malware, malicious insiders, or targeted attacks. This is because advanced attacks often do not incorporate traditional indicators of compromise (IoCs), such as attack signatures or malicious domains. The only way to detect these threats is to examine activity—not just alerts—over time and across data sources with machine learning and analytics.

Manual Investigations Increase Attacker Dwell Times

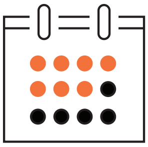
Detecting attacks is only half the battle. Analysts must also investigate alerts and assess the "who, what, when, why, and how" details to determine what action to take. Unfortunately, many of today's security tools only present high-level alerts with limited user, endpoint, network, application, and threat intelligence information.

These high-level alerts rarely provide all the context needed for investigation and response. As a result, analysts must pivot from console to console and manually piece together data to get a clear understanding of an attack. To investigate a network alert, for example, an analyst may need to perform painstaking analysis and correlation to identify the endpoint, network activity, and user associated with each incident. With today's complex and siloed tools, only specialized experts can navigate the labyrinth required for investigations.

[1] "The State of SOAR Report, 2018," Demisto, September 2018, https://go.demisto.com/the-state-of-soar-report-2018.
[2] Ibid.

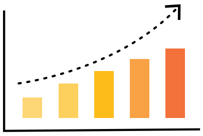
Since these tools rarely work together, analysts cannot easily coordinate response across all their enforcement points. Instead of instantly blocking an attack, they must submit a ticket or ask other team members to update security policies, which might take days or weeks. It's not surprising, then, that the average time it takes organizations to identify a breach, and then to contain it, has increased to 197 and 69 days, respectively.[3]

Faced with a shortage of cybersecurity professionals—which industry analysts expect to reach 1.8 million unfilled positions by 2022[4]—teams need to break down security silos and simplify incident response, or they will struggle to prevent successful cyberattacks.



Mean time to identify (MTTI)
a breach has increased to

197 days



Mean time to contain (MTTC)
a breach has increased to

69 days

What Is Needed

A new approach is required to solve today's security operations challenges—one that will ease every stage of security operations, from detection and threat hunting to triage, investigation, and response. This new approach requires the following three integrated capabilities, working together to lower risk and simplify operations.

- **Great threat prevention:** Great prevention allows you to stop everything you can—the more than 99% of attacks that can be blocked automatically in real or near-real time—without manual verification. You need consistent, coordinated prevention across all your digital assets.
- **AI and machine learning:** With the growing amount of data being collected, your analysts shouldn't be forced to manually analyze or correlate data to identify threats. You need machine learning and analytics to learn the unique characteristics of your organization and form a baseline of expected behavior to detect sophisticated attacks.
- **Automation:** To quickly confirm attacks, analysts need actionable alerts with rich investigative details. They should also be able understand the root cause of attacks easily without needing years of experience.

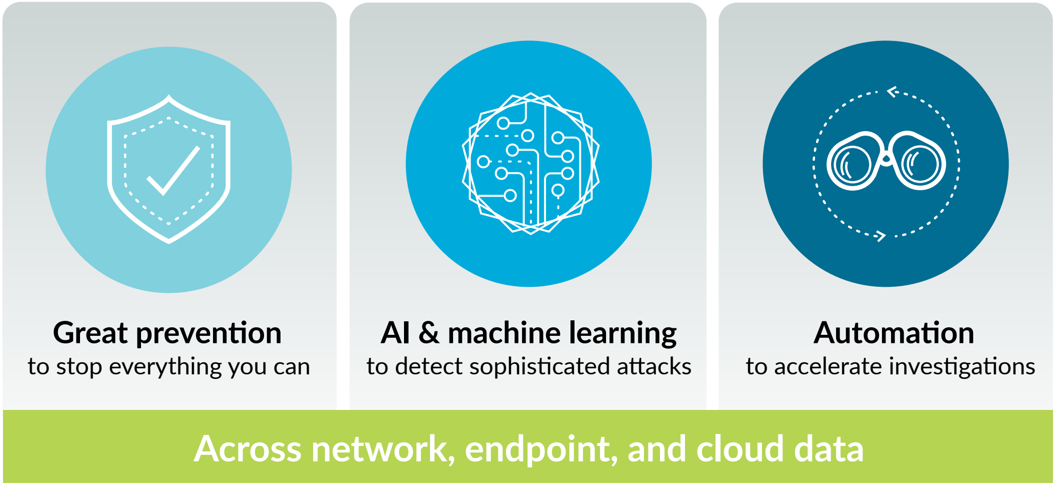

Great prevention
to stop everything you can
AI & machine learning
to detect sophisticated attacks
Automation
to accelerate investigations
Across network, endpoint, and cloud data

Figure 2: Critical integrated capabilities

With these three integrated capabilities coordinated across all your critical assets, including your network, endpoints, and clouds, you'll be able to defeat increasingly sophisticated threats.

Cortex XDR Detection and Response

Cortex XDR is the world's first cloud-based detection and response app that natively integrates network, endpoint, and cloud data to stop sophisticated attacks. Cortex XDR has been designed from the ground up to help organizations like yours secure your digital assets and users while simplifying operations. Using behavioral analytics, it identifies unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

[3] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018, https://www.ibm.com/downloads/cas/861MNWN2.

[4] "2017 Global Information Security Workforce Study," (ISC)2, 2017, https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf.

Cortex XDR helps you accelerate investigations by providing a complete picture of each alert. It stitches different types of data together and reveals the root cause and timeline of alerts, allowing analysts of all experience levels to perform triage. Tight integration with enforcement points lets you respond to threats quickly and apply the knowledge gained from investigations to detect similar attacks in the future.

With Cortex XDR, you can use your existing Palo Alto Networks network, endpoint, and cloud security as sensors and enforcement points, eliminating the need to deploy new software or hardware. You only need one data source—such as Palo Alto Networks next-generation firewalls or Traps™, our endpoint protection and response service—with Cortex XDR, but you would need multiple data sources to realize the benefits of data stitching and analysis. You can avoid provisioning cumbersome log infrastructure on-premises by storing all your data in Cortex Data Lake, a scalable and secure cloud-based data repository.

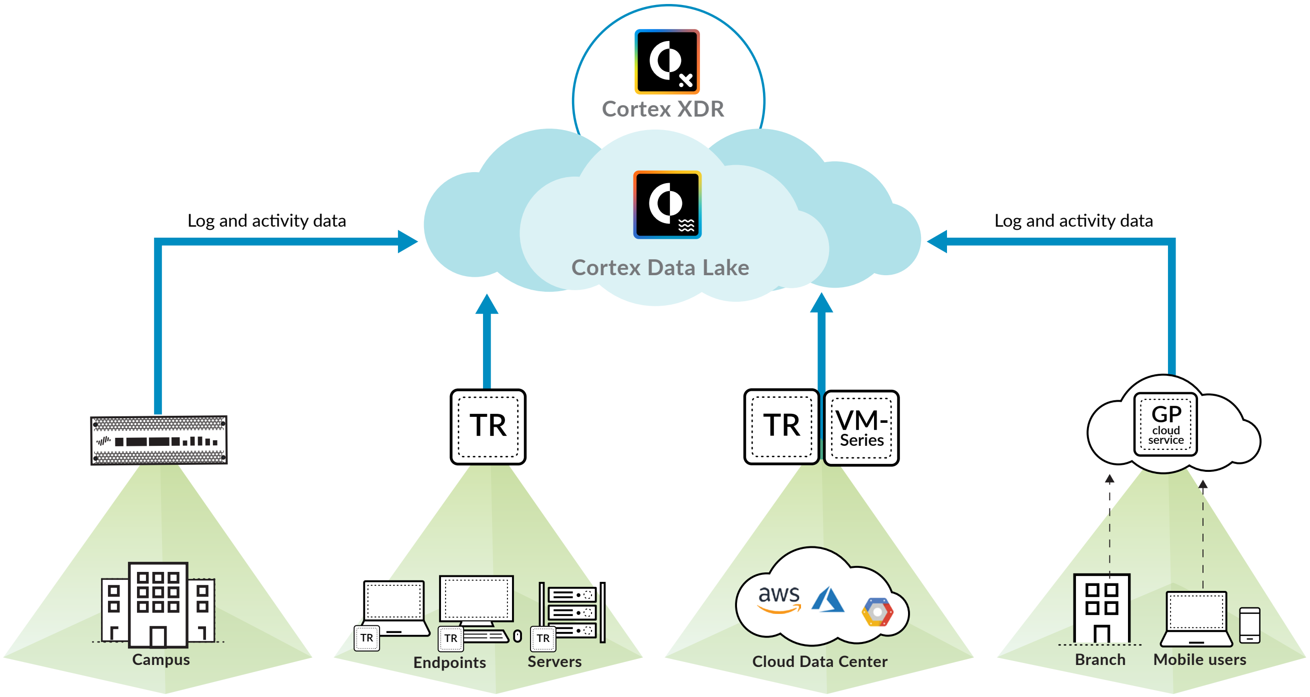


Figure 3: Analysis of data from multiple sources by Cortex XDR

Cortex XDR Protects You at Every Stage of Security Operations

Attackers continually innovate. To outpace them, security teams must implement a repeatable process to proactively block attacks with best-in-class prevention and to discover and stop active threats. Cortex XDR gives you the tools to accomplish four iterative steps:

1. Prevent
2. Automatically detect
3. Rapidly investigate
4. Respond and adapt

This framework provides everything you need to secure your organization today and in the future.

Achieve Closed-Loop Prevention, Detection, and Response with Cortex XDR

Prevent Known and Unknown Threats While Gaining Complete Visibility

Ironclad security starts with great prevention. To this end, all Cortex XDR subscriptions include Traps for endpoint protection and response, offering you the best endpoint security available. Traps is a lightweight agent that automatically blocks malware, exploits, and fileless attacks while simultaneously collecting event data for Cortex XDR.

Combining multiple methods of prevention, Traps stands apart in its ability to protect endpoints. Traps thwarts malware infections by blocking the exploits used by attackers to compromise endpoints and install malware. Traps protects hosts by identifying exploit techniques—not just exploit signatures—so it can stop zero-day threats. In addition, it identifies sequences of behavior unique to malware and ransomware with its powerful Behavioral Threat Protection engine. Traps integrates with Palo Alto Networks WildFire®, our malware prevention service, to analyze suspicious files in the cloud and coordinate protection across all Palo Alto Networks security products.

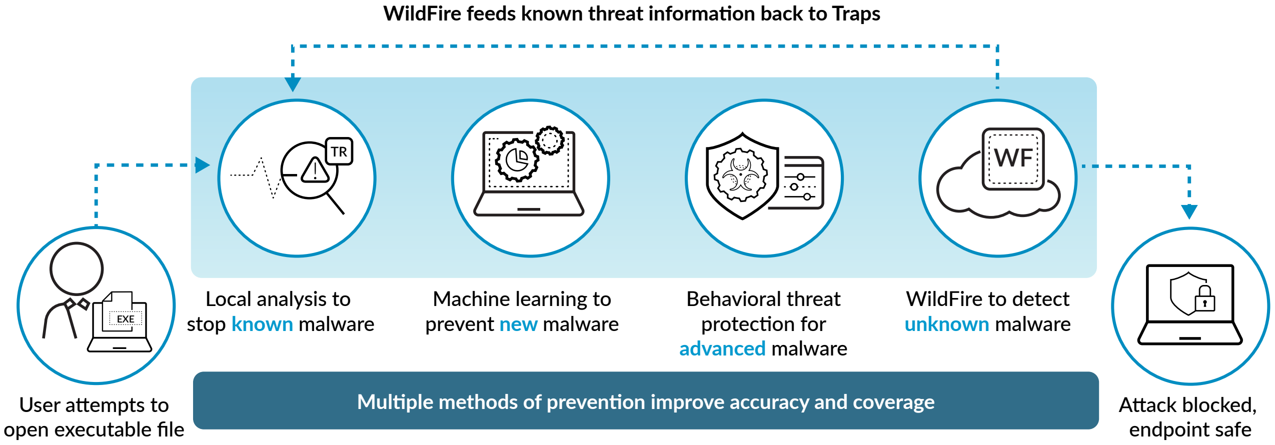
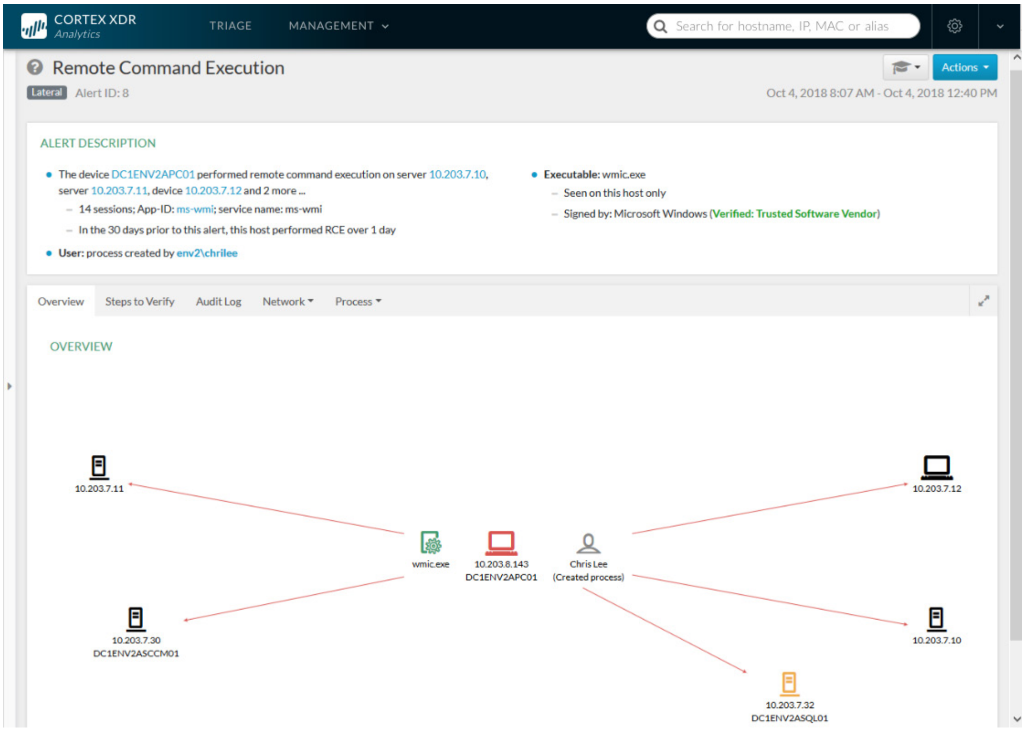

WildFire feeds known threat information back to Traps
TR
EXE
WF
User attempts to open executable file
Local analysis to stop known malware
Machine learning to prevent new malware
Behavioral threat protection for advanced malware
WildFire to detect unknown malware
Attack blocked, endpoint safe
Multiple methods of prevention improve accuracy and coverage

Figure 4: **Automatically preventing malware, exploits, and fileless attacks**

In addition to Traps, Palo Alto Networks provides a complete portfolio of security offerings that prevent attacks by combining the latest breakthroughs in security, automation, and analytics. Cortex XDR integrates with these world-leading technologies, including our physical and virtualized next-generation firewalls, and GlobalProtect™ cloud service, enabling you to prevent advanced attacks while also collecting data for detection and response.

Automatically Detect Attacks with Behavioral Analytics and AI

Cortex XDR uncovers stealthy attacks using analytics and machine learning, allowing your team to focus on the threats that matter. Cortex XDR starts by analyzing rich data gathered across the Palo Alto Networks platform, providing you complete visibility and eliminating blind spots. It stitches together data collected from your network, endpoints, and cloud assets to accurately detect attacks and simplify investigations.



Remote Command Execution

Lateral Alert ID: 8

Oct 4, 2018 8:07 AM - Oct 4, 2018 12:40 PM

ALERT DESCRIPTION

- The device DC1ENV2APC01 performed remote command execution on server 10.203.7.10, server 10.203.7.11, device 10.203.7.12 and 2 more ...
  - 14 sessions; App-ID: ms-wmi; service name: ms-wmi
  - In the 30 days prior to this alert, this host performed RCE over 1 day
- **User:** process created by env2\chrilee
- **Executable:** wmic.exe
  - Seen on this host only
  - Signed by: Microsoft Windows (Verified: Trusted Software Vendor)

OVERVIEW

Figure 5: **Automatic discovery of anomalies indicative of malware, targeted attacks, and insider abuse**

Cortex XDR tracks more than 1,000 dimensions of behavior, including attributes that are nearly impossible to ascertain from traditional threat logs or high-level network flow data. It then profiles user and device behavior by taking advantage of:

- **Unsupervised machine learning:** Cortex XDR baselines user and device behavior, performs peer group analysis, and clusters devices into relevant groups of behavior. Based on these profiles, Cortex XDR detects anomalies compared to past behavior and peer behavior to detect malicious activity, such as malware behavior, command and control, lateral movement, and exfiltration.
- **Supervised machine learning:** Cortex XDR monitors multiple characteristics of network traffic to classify each device by type, such as a Windows® computer, an Apple iPhone®, a mail server, or a vulnerability scanner. Cortex XDR also learns which users are IT administrators or normal users. With supervised machine learning, Cortex XDR recognizes deviations from expected behavior based on the type of user or device, reducing false positives.

Cortex XDR uses a pre-compute detection architecture to maximize speed, efficiency, and accuracy. The pre-compute framework processes the data stored in Cortex Data Lake to calculate the values it needs for machine learning. Its detection algorithms analyze these precalculated values, rather than raw data, to find attacks more quickly and incorporate multiple inputs in its detection algorithms to detect attacks with precision.

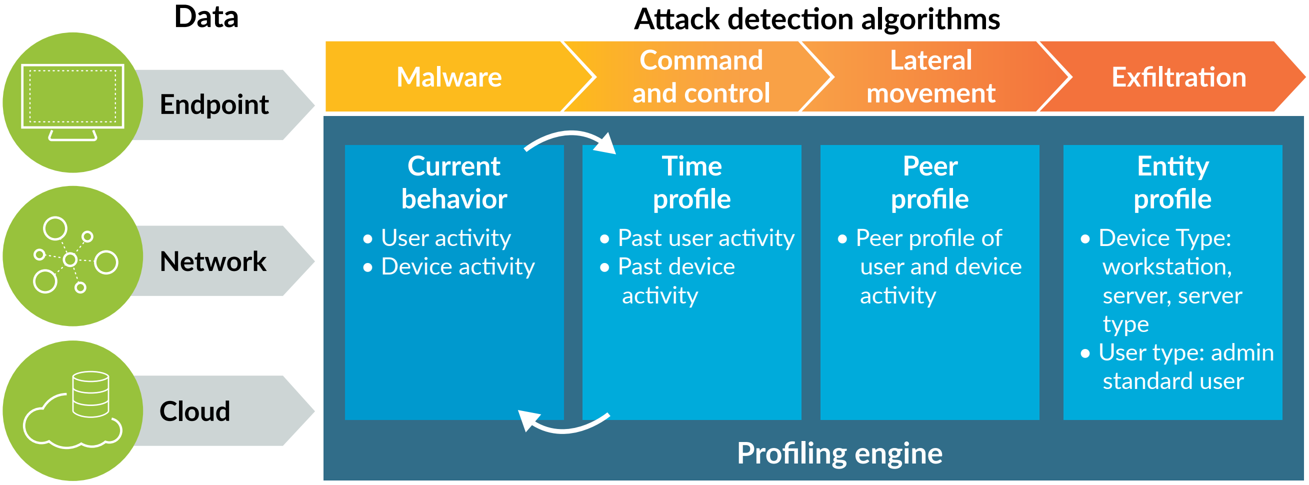


Figure 6: Behavioral analytics architecture for Cortex XDR

By examining rich network, endpoint, and cloud data, building behavioral profiles, and analyzing these profiles with a broad set of detection algorithms, Cortex XDR can pinpoint stealthy attacks with unparalleled precision.

Custom Rules

Your security team can identify threats unique to your environment with flexible custom rules. Triggering alerts against known IoCs, such as malware hashes, can help identify known threats, but attackers can easily evade these detection techniques. Cortex XDR provides custom rules that enable your security team to detect complex combinations of behaviors to expose specific attacker tactics, techniques, and procedures (TTPs). As a result, your team can close known security gaps and gain visibility into potentially malicious activity being performed on the most valuable assets. Your custom rules can identify misuse of systems and applications as well as detect zero-day attacks that thwart evasion techniques, ensuring you can uncover threats even if an adversary manipulates malware names, hashes, or IP addresses.

Your analysts can define rules based on dozens of different parameters, including process, file, network, or registry information. More than two hundred predefined rules detect a broad array of threats out of the box, including persistence, tampering, privilege escalation, and lateral movement.

These detection capabilities work all day, every day, providing you peace of mind.

Threat Hunting and IoC Searching

Threat hunting plays a vital role in security operations, whether analysts are performing an independent search or expanding from an investigation. With search queries, your team can uncover suspicious activity by searching for specific hosts, files, processes, registry updates, network connections, and more. Queries can be precise, such as, “What are the changes made to a specific file by a specific process on a host?” or open ended, such as “Show me all the processes running in the domain.” Your security team can search, schedule, and save queries as custom rules.

Your security team can search for attack behaviors as well as traditional IoCs without learning a new query language. Analysts can filter results to reduce the number of events to review and reveal covert threats. By incorporating threat intelligence with a complete set of network, endpoint, and cloud data, your team can find past attacks or uncover incidents in progress in seconds.

Data Inspected by Cortex XDR

Cortex XDR analyzes protocol-level metadata in traffic logs, enhanced application logs, and threat logs collected by Palo Alto Networks NGFWs, VM-Series virtualized NGFWs, and GlobalProtect™ cloud service. It also examines endpoint data from Traps. By building a profile based on more than 1,000 dimensions of behavior, including frequency of connections, source and destination of traffic, protocols used, and more, Cortex XDR can learn the expected behavior of users and devices. Cortex XDR also monitors internal traffic as well as outbound traffic from clients and servers to the internet.

Session-Level Data

Palo Alto Networks NGFWs extract the metadata needed to profile user and device behavior, including:

- Source IP, destination IP, source port, and destination port
- Bytes sent and received
- Connection duration
- Enhanced application logs with transaction-level data on DNS, HTTP, DHCP, RPC, ARP, ICMP, and more
- Application details from App-ID

User Data

Cortex XDR analyzes network traffic and endpoint data to extract user context, such as:

- Logged-in user
- Typical user of a machine
- User creating the process that initiated the communication
- User group and organizational unit from Directory Sync

Endpoint Data

Cortex XDR analyzes all endpoint activity, including:

- File creation, deletion, and update
- File hash
- File path
- Process name
- Registry change
- CLI arguments
- Hardware events, such as USB
- Event log manipulation
- Traps security alerts
- WildFire malware verdict

Host Data

Cortex XDR identifies machines by tracking:

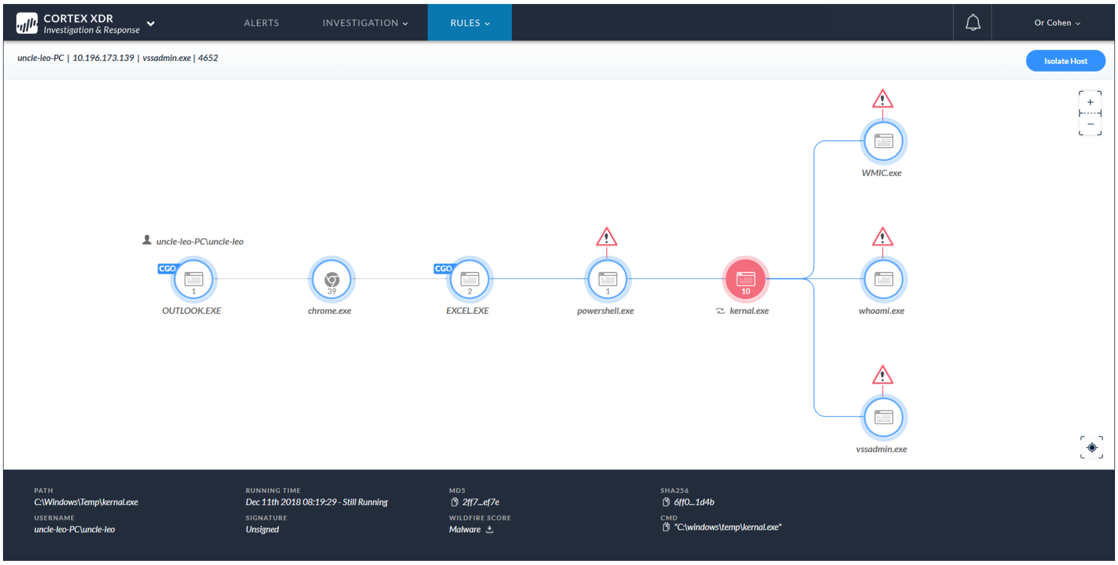
- Hostname
- MAC address
- Operating system

Data Retention

- Minimum 30 days

Rapidly Investigate Alerts

To expedite triage and analysis of any threat, your analysts need full investigative context at their fingertips. Cortex XDR delivers several key features that accelerate alert triage and incident response. An alert dashboard lets your team sort, filter, export, or even investigate alerts from any source with a single click. Your team can instantly understand the root cause, reputation, and sequence of events associated with each alert, lowering the experience needed to verify threats while ensuring fast and accurate decisions.



uncle-leo-PC | 10.196.173.139 | vssadmin.exe | 4652

PATH
C:\Windows\Temp\kernal.exe

USERNAME
uncle-leo-PC\uncle-leo

RUNNING TIME
Dec 11th 2018 08:19:29 - Still Running

SIGNATURE
Unsigned

MD5
2ff7...ef7e

WILDFIRE SCORE
Malware

SHA256
6ff0...1d4b

CMD
"C:\windows\temp\kernal.exe"

Figure 7: Find the root cause of any alert, including network and cloud security alerts

Your team can conclusively answer the questions posed by any event, using these analysis views:

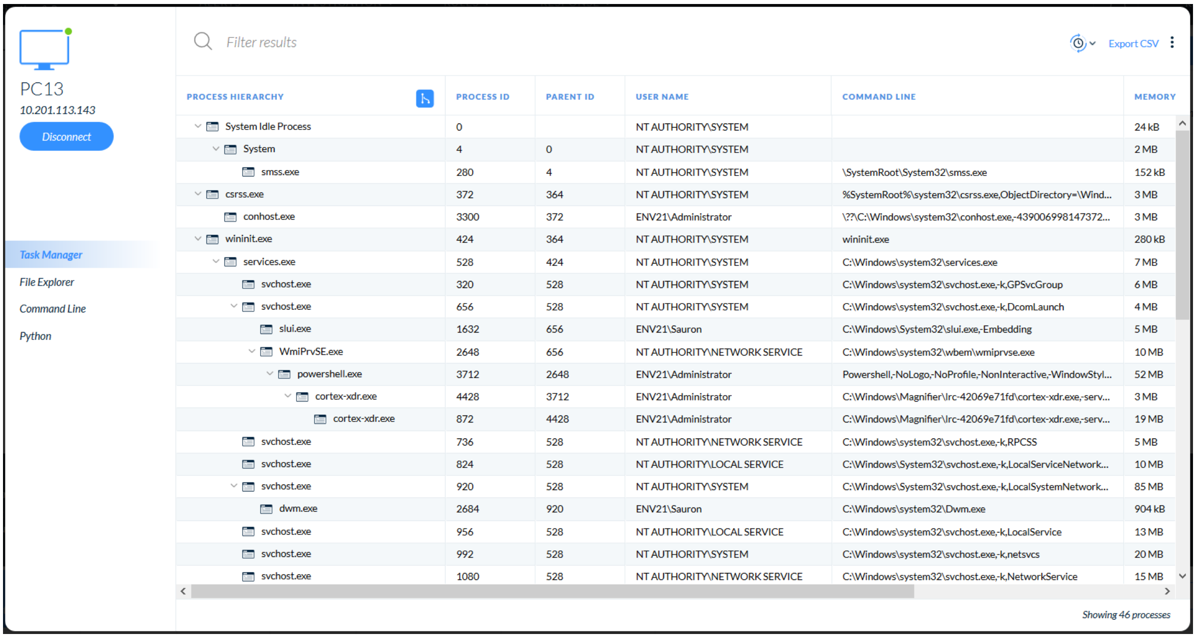
- **Root cause analysis view:** A unique, patented analysis engine continuously reviews billions of events to identify the chain of events behind every threat. It visualizes the attack sequence back to the root cause and provides essential details about each element in the sequence, making complex attacks easy to understand. Your analysts can instantly see which endpoint processes were responsible for network or cloud security alerts without manually correlating events or pivoting between consoles.
- **Timeline analysis view:** A forensic timeline of all attack activity provides actionable detail for incident investigations, allowing your analysts to determine the scope, impact, and next steps in seconds. Informational alerts improve timeline analysis by identifying suspicious behavior and making complex events easy to understand without cluttering your alert dashboard with low-risk events.

Cortex XDR offers relief to teams struggling with a backlog of alerts and difficult, time consuming analysis. Moreover, it simplifies alert triage and incident investigation with intuitive, visual, context-driven tools. Analysis that used to take hours, days, or weeks can be accomplished in seconds or minutes—all with less specialized expertise.

Respond and Adapt to Threats

Once you identify threats, you need to contain them quickly. Cortex XDR lets your security team instantly eliminate network, endpoint, and cloud threats from one console. Your team can quickly stop the spread of malware, restrict network activity to and from devices, and update threat prevention lists, such as bad domains, through tight integration with enforcement points.

With Remote Terminal, response and remediation can go beyond initial containment. Your analysts can remotely view alerts, upload tools, and interactively run commands or scripts using Python® or PowerShell® for in-depth forensic investigations. Your teams can also terminate and delete processes in a live environment on any host with full auditing occurring as they work. All the while, end users can continue to work without disruption or downtime while threats are eliminated.



PROCESS HIERARCHY	PROCESS ID	PARENT ID	USER NAME	COMMAND LINE	MEMORY
System Idle Process	0		NT AUTHORITY\SYSTEM		24 kB
System	4	0	NT AUTHORITY\SYSTEM		2 MB
smss.exe	280	4	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe	152 kB
csrss.exe	372	364	NT AUTHORITY\SYSTEM	%SystemRoot%\system32\csrss.exe,ObjectDirectory=\Wind...	3 MB
conhost.exe	3300	372	ENV21\Administrator	\??\C:\Windows\system32\conhost.exe,-439006998147372...	3 MB
wininit.exe	424	364	NT AUTHORITY\SYSTEM	wininit.exe	280 kB
services.exe	528	424	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe	7 MB
svchost.exe	320	528	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,GPSvcGroup	6 MB
svchost.exe	656	528	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,DcomLaunch	4 MB
slui.exe	1632	656	ENV21\Sauron	C:\Windows\System32\slui.exe,-Embedding	5 MB
WmiPrvSE.exe	2648	656	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe	10 MB
powershell.exe	3712	2648	ENV21\Administrator	Powershell,-NoLogo,-NoProfile,-NonInteractive,-WindowStyl...	52 MB
cortex-xdr.exe	4428	3712	ENV21\Administrator	C:\Windows\Magnifier\lrc-42069e71fd\cortex-xdr.exe,-serv...	3 MB
cortex-xdr.exe	872	4428	ENV21\Administrator	C:\Windows\Magnifier\lrc-42069e71fd\cortex-xdr.exe,-serv...	19 MB
svchost.exe	736	528	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe,-k,RPCSS	5 MB
svchost.exe	824	528	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe,-k,LocalServiceNetwork...	10 MB
svchost.exe	920	528	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe,-k,LocalSystemNetwork...	85 MB
dwm.exe	2684	920	ENV21\Sauron	C:\Windows\system32\Dwm.exe	904 kB
svchost.exe	956	528	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe,-k,LocalService	13 MB
svchost.exe	992	528	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,netsvcs	20 MB
svchost.exe	1080	528	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe,-k,NetworkService	15 MB

Showing 46 processes

Figure 8: Cortex XDR Remote Terminal Task Manager

Apply Knowledge Gained from Investigations

With Cortex XDR, your team can apply knowledge from each investigation to reduce your attack surface and streamline future investigations, transforming your security posture from reactive to proactive.

Your team can create granular custom rules based on the attack techniques identified in past incidents. You can also use the custom rules available for detection as context for future investigations. Rather than assigning a rule to alert on an event, it can notify your analysts that something has occurred that needs to be factored into a decision. Less experienced analysts can make educated decisions during investigations by viewing intuitive, informational alerts related to incidents, such as possible evasion, persistence, or credential abuse activity.

Cortex XDR continually evolves to anticipate threats and outsmart attackers. Traps and Cortex XDR integrate with WildFire to distribute malware findings to the industry's largest malware analysis community. Palo Alto Networks Unit 42 research, the Global Security Incident Response Team (GSIRT), and the Cortex XDR research team update protections based on a combination of automated and manual analysis of metrics and telemetry data.

The Silver Lining of Cloud Deployment

As a cloud-based app, Cortex XDR eliminates the need to deploy additional on-premises software or hardware. It uses your existing Palo Alto Networks products as sensors and enforcement points, streamlining deployment and management. The data collected from your Palo Alto Networks infrastructure is stored in Cortex Data Lake, a scalable, cloud-based data repository. Cortex Data Lake delivers efficient log storage that scales to handle the large volume of data needed for detection and response. You can quickly deploy Cortex XDR and Cortex Data Lake, avoiding the time-consuming process of setting up new equipment.

By eliminating on-premises log storage and additional sensors and enforcement points, Cortex XDR offers low total cost of ownership. Cortex XDR also boosts the productivity of your security operations team by automatically detecting attacks and accelerating investigations.

Conclusion

These are the times that try analysts' souls. To keep up with ever-increasing threats, organizations deploy more and more siloed tools that produce an avalanche of incomplete, inaccurate alerts. Instead of using cloud-based machine learning to cut through the noise and find hard-to-detect attacks, legacy security information and event management (SIEM) products focus on aggregating alerts for threats that were identified and typically stopped by security infrastructure. On the other hand, siloed detection and response tools force IT staff to deploy additional hardware and software, but they only offer a narrow view of threats, creating blind spots while forcing analysts to gather and correlate clues from multiple tools.

Cortex XDR provides your analysts the secret weapon they need to eradicate elusive threats anywhere in your environment by stitching together and analyzing all your network, endpoint, and cloud data. With Cortex XDR, you can:

- Prevent advanced malware, exploits, and fileless attacks with Cortex XDR, which includes Traps, ensuring complete coverage of every endpoint.
- Automatically detect stealthy attacks and anomalies unique to your organization, using machine learning and analytics.
- Accelerate alert triage and investigations to increase the productivity of all your security analysts by revealing the root cause of any alert.
- Quickly contain threats by coordinating response across enforcement points.
- Outpace attackers with up-to-date protections and research from WildFire, Unit 42, and GSIRT, powered by cloud scale and agility.

With Cortex XDR, you gain complete visibility across your network, endpoint, and cloud assets, so you can rest assured that all your users and data are secure.

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com