## Secure the Future - Cortex

Cortex is an artificial intelligence-based, continuous security platform. Cortex allows organizations to create, deliver, and consume innovative new security products from any provider, without additional complexity or infrastructure.

Security teams are constantly challenged to prevent data breaches. The issues originate from too many alerts, too few security analysts, narrowly focused tools, lack of integration, and lack of time. The more they react, the further behind they get. Palo Alto Networks has developed a breakthrough approach to SOC visibility, investigation, and speedy resolution called Cortex XDR. Cortex XDR brings visibility to the security team across all aspects of the infrastructure, breaking down silos and presenting a holistic picture of the organization’s activity in order to improve security operations and posture.

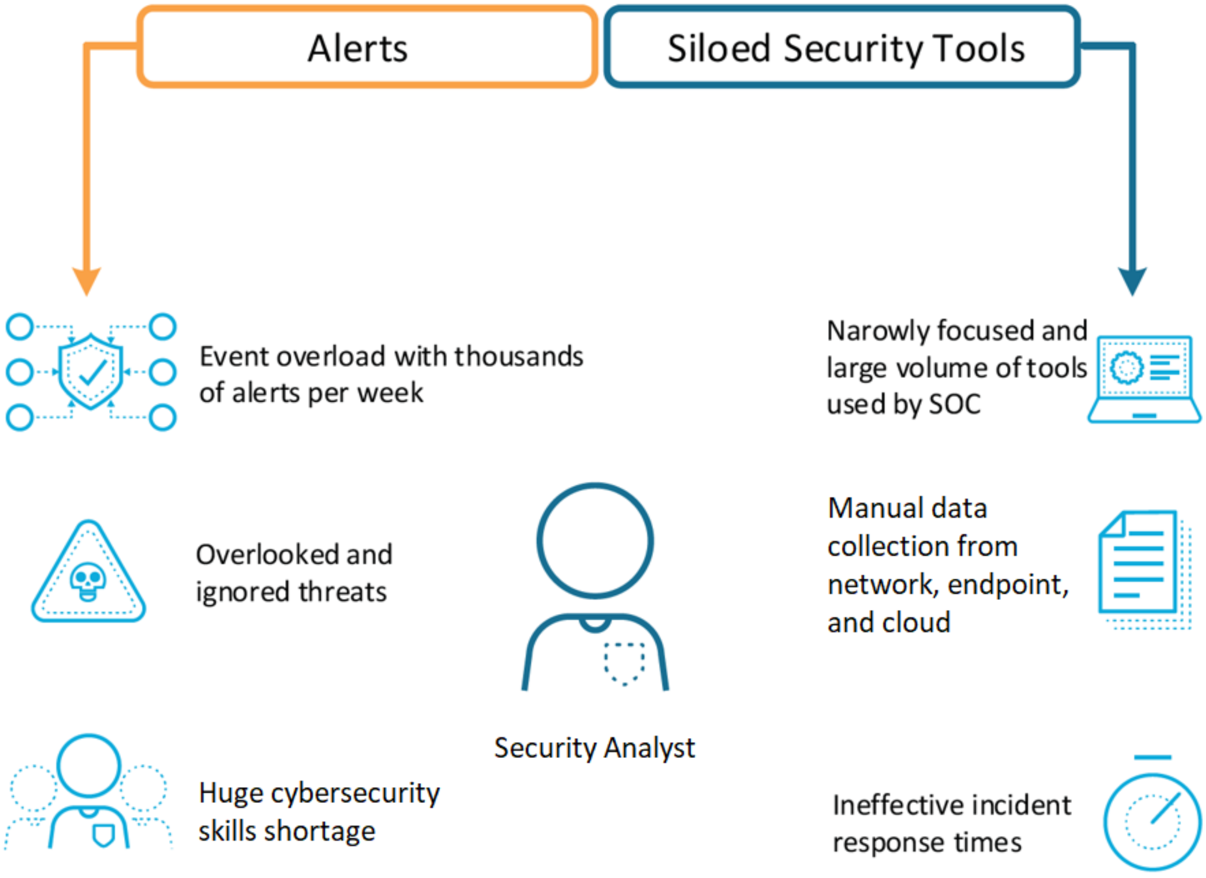
From a business perspective, Cortex XDR enables organizations to prevent successful cyberattacks as well as simplify and strengthen security processes. This capability, in turn, enables them to better serve users and accelerate digital transformation initiatives – because when users, data, and applications are protected, companies can focus on strategic priorities. With Cortex XDR, you can uncover stealthy threats with behavior analytics, investigate events, and hunt down threats with powerful search tools.

Security operations (SecOps) is a joint effort between IT teams such as security and operations working to prevent threats and detect and respond to security incidents. The goal of any security team is to defend an organization’s infrastructure and data from damage, unauthorized access, and misuse. Larger organizations operate a security operations center (SOC), where a team of dedicated security staff detect, investigate, and respond to threats with tools to determine the extent of the threat through analysis and threat-hunting techniques.

For organizations, as threats continue to escalate in sophistication and numbers, SecOps is put under increased pressure by the large number of alerts that they receive, which makes it impossible to effectively deal with them. Another challenge that SecOps faces when dealing with all the alerts they receive is the lack of overall context for their investigations when dealing with multiple separate platforms that are generating alerts. As a result, the SecOps teams have to manually integrate multiple data sources and tools to understand the attack, causing investigations to take too long and potential threats to be missed.

Achieving 100 percent prevention is extremely difficult for any organization. Security operations centers (SOCs) purchase many niche security products today, which creates the disadvantage of having to track and manage so many alerts coming in from different platforms and tools. It can take days to weeks for one SOC engineer to investigate a single suspicious activity or alert, which may lead to nothing in the end (see Figure 4-3).

**Figure 4-3** *Struggles of a security analyst*


Alerts
Siloed Security Tools
Event overload with thousands of alerts per week
Narowly focused and large volume of tools used by SOC
Overlooked and ignored threats
Manual data collection from network, endpoint, and cloud
Security Analyst
Huge cybersecurity skills shortage
Ineffective incident response times

Palo Alto Networks has a different approach for SecOps teams:

1. First, you prevent all of the threats you can with Cortex XDR endpoint protection and our next-generation firewalls.
2. Everything you can't prevent you need to detect and investigate rapidly. You achieve this with Cortex XDR and AutoFocus.
3. Then you continuously automate responses with Cortex XSOAR. Cortex XSOAR allows security teams to ingest alerts across multiple sources and then execute automatable playbooks for accelerated incident response.

Cortex is the platform for SecOps. Think of Cortex as your one-stop shop for SecOps, solving all key challenges in a more efficient way with higher security outcomes. With Cortex you can speed up investigations by having the right data – integrated across network, endpoint, and cloud – with all the context needed for security analysts. The platform has two primary SecOps elements:

- **Cortex XDR for detection and response.** Cortex XDR was the first to market and the defining product in the XDR ("anything" detection and response) market category, which leapfrogs endpoint protection and response (EDR) with its narrow focus on just the endpoint.
- **Cortex XSOAR for security orchestration, automation, and response.** Cortex XSOAR provides playbooks with 300+ multivendor integrations that help solve any security use case.

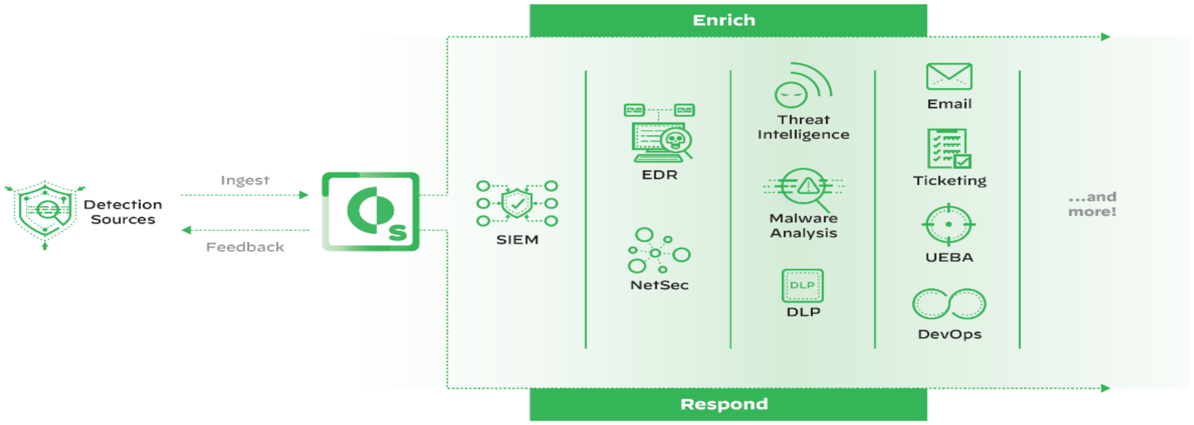
## Cortex XSOAR

Security teams lack the people and scalable processes to keep pace with an overwhelming volume of alerts and endless security tasks. Analysts waste time pivoting across consoles for data collection, determining false positives, and performing manual, repetitive tasks throughout the lifecycle of an incident. As they face a growing skills shortage, security leaders need time to make decisions that matter, rather than drown in reactive, piecemeal responses.

Cortex XSOAR supercharges security operations center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and native threat intel management in the industry's first extended security orchestration, automation, and response (SOAR) offering. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case, resulting in up to 90 percent faster response times and as much as a 95 percent reduction in alerts requiring human intervention.

Cortex XSOAR ingests aggregated alerts and indicators of compromise (IoCs) from detection sources – such as security information and event management (SIEM) solutions, network security tools, threat intelligence feeds, and mailboxes – before executing automatable, process-driven playbooks to enrich and respond to these incidents (see Figure 4-12). These playbooks coordinate across technologies, security teams, and external users for centralized data visibility and action.

**Figure 4-12** *Cortex XSOAR ingests alerts and IoCs from multiple detection sources and executes playbooks to enrich and respond to incidents.*



Cortex XSOAR empowers security professionals to efficiently carry out security operations and incident response by streamlining security processes, connecting disparate security tools, and maintaining the right balance of machine-powered security automation and human intervention.

## Cortex Data Lake

Organizations often lack the visibility they need to stop attacks. Data is typically locked in silos across cloud, endpoint, and network assets, preventing tools from effectively finding, investigating, or automating threat response.

Deploying massive data collection, storage, and analysis infrastructure is complex. You need to plan for space, power, compute, networking, and high availability needs; increasing costs; and operational burden. After it's deployed, the infrastructure needs ongoing maintenance and monitoring, taking time away from activities that drive your business forward.

Cortex Data Lake is built to benefit from public cloud scale and locations. The cloud-based service is ready for elastic scaling from the start, eliminating the need for local compute and storage. As your needs grow, you can add more capacity with the push of a button. The public cloud architecture enables you to take advantage of global locations to solve local data residency and privacy requirements. Infrastructure – including storage and compute – is handled for you, letting you focus on solving new security challenges with apps built on Cortex.

Cortex Data Lake automatically collects, integrates, and normalizes data across your security infrastructure. With unified data, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Tight sensor integration allows new data sources and types to be continually added to evolve your defenses.

Cortex Data Lake has strict privacy and security controls in place to prevent unauthorized access to sensitive or identifiable information. Cortex Data Lake ensures the privacy of your data by limiting access to your authorized users and apps, which you can revoke at any time. The Cortex Data Lake infrastructure is secured with industry-standard best practices for security and confidentiality, including rigorous technical and organizational security controls.