NETSCOUT Integrates Smart DDoS Protection With Cortex XSOAR

Smart Security Solution Increases Service Availability

Distributed Denial of Service (DDoS) attacks and cyber threats are a major risk to the availability and security of any business. The power, sophistication, and frequency of both DDoS attacks and threats continue to increase daily. To combat this, businesses need a defense that is effective, cost-efficient, and easily managed. NETSCOUT's Arbor Sightline and Arbor Threat Mitigation System™ (TMS) are industry leading DDoS protection solutions trusted by service providers, cloud providers, and large enterprises everywhere. Integrating NETSCOUT's DDoS solutions with Palo Alto Network's Cortex XSOAR platform maximizes protection for security teams across the globe.

As cyber threats have evolved, so too has the cyber security stack. Multiple stateful network enforcement devices such as Next Generation Firewalls, IPS, DLP, sandboxes, and more comprise the modern network security stack. Additionally, Next-Gen Fire Walls (NGFW) have taken on additional security functions beyond simple network access control. For example, IDS/IPS and sandboxing functions, once standalone devices, are now performed by NGFWs. Because of the variety of tasks that NGFWs assist with--stateful session and user tracking, URL filtering, VPN tunneling, IPS and other high-resource functions--keeping the firewalls and other stateful devices free from the burden of attack traffic is crucial for operational stability.

The best way to maintain stability is by having DDoS and threat mitigation happen as close to the network edge as possible, alleviating the risk and burden on downstream security devices and applications which may be susceptible to service impacts or compromise.

Before the era of orchestration, the NETSCOUT DDoS and Cortex XSOAR solutions would operate completely independently. Detection, mitigation, and reporting would be performed by both, neither having the benefit of knowing what the other was doing. In addition to having a heavy burden on security teams, this method would increase operational overhead of network and security operations and potentially impact services. The addition of orchestration in the modern security stack allows businesses to combine the intelligence, messaging, and enforcement capabilities of their tools. This will maximize their effectiveness and minimize the impacts on load.

Arbor Sightline's integration with Palo Alto Networks Cortex XSOAR ingests Sightline-generated incident reports of endpoint alerts, TMS and FlowSpec mitigations. Once informed, Cortex XSOAR can perform actions or trigger automation for immediate changes to enforcement. Additionally, operators can utilize indicators within Cortex XSOAR to manually perform mitigation, providing security teams the flexible responses they need.

HIGHLIGHTS

- Solution for enterprises integrates smart DDoS protection with the power of SOAR to reduce corporate risk and increase service availability.
- SOC teams can benefit from cross-platform visibility and decrease the operational overhead of their network and security programs through orchestration and automation for DDoS use cases.
- Organizations get an improved security posture and faster time to detect and respond to threats.
- Arbor Sightline integration with Cortex XSOAR certified through Palo Alto Networks.[1]

[1] Availability of the Arbor Sightline content pack through the Cortex XSOAR Marketplace is targeted by end of Q2 2021. AED integration is targeted for second half of 2021.

Use Cases

Inbound DDoS Attack

Arbor Sightline detects a DDoS attack from the Internet and reports the ongoing event. This prompt ingestion by Cortex XSOAR and automates mitigation to Arbor TMS and other mitigation devices across the infrastructure. This automation will free up time for the security team to minimize outage time.

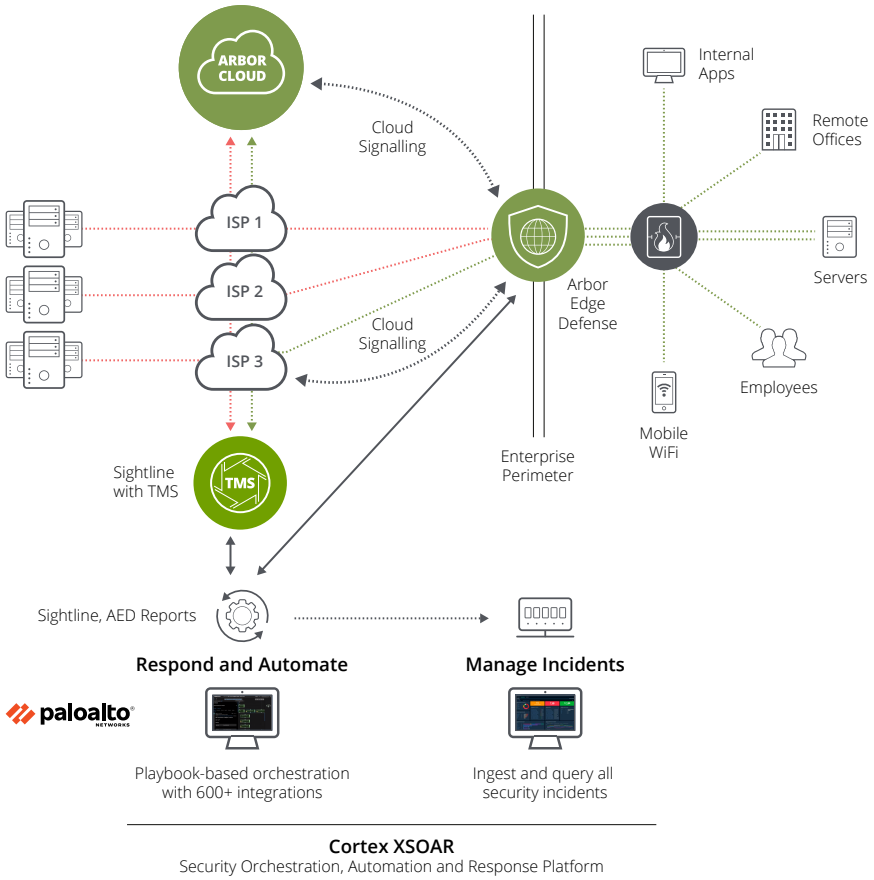
Outbound DDoS Attack

Arbor Sightline will identify traffic originating within the environment as resources that are participating in a DDoS attack on the Internet. Arbor Sightline reports the event which is ingested by Cortex XSOAR. Cortex XSOAR will instruct a Palo Alto Networks NGFW to block that traffic near the source, protecting resources and reclaiming SecOps time.

Outbound Threat Indicator

Arbor Sightline is able to identify C2 traffic as it occurs in the environment. Arbor Sightline will report the event to Cortex XSOAR. After ingestion, Cortex XSOAR will instruct a Palo Alto Networks NGFW to block traffic near the source. Cortex XSOAR then instructs the EDR solution to quarantine the specific host for remediation. This allows security teams to approach remediation on their time rather than being overwhelmed by the number of events.

By integrating Arbor Sightline with Cortex XSOAR, operations teams can leverage the capabilities of Arbor Sightline to enhance operational efficiencies--such as detection, response time, and mitigation--by coordinating the response across security tools in the enterprise. Through intelligent reporting and orchestration, DDoS attacks and other cyber threats can be detected and blocked both at the edge and through any other enforcement devices under the orchestration environment, improving the security, resilience, and availability of the network and services.



NETSCOUT + Palo Alto Networks

Arbor Sightline + Cortex XSOAR integration takes security assurance to a new level by combining the world's best DDoS protection with the most comprehensive SOAR platform by connecting technology, process, and people. The Arbor Sightline integration has achieved full security and functionality testing through Palo Alto Networks and is available on the Cortex XSOAR Marketplace. The Cortex XSOAR Marketplace is a built-in digital storefront for security orchestration content found within the Cortex XSOAR platform. Don't have Cortex XSOAR? Download the free Community Edition.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Their mission is to be the cybersecurity partner of choice, protecting the digital way of life. They help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, they are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Their vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

About NETSCOUT Arbor DDoS Protection

At a time when availability has never been more important, a DDoS attacks have never been more innovative, dynamic or consequential. It won't come as any surprise to security professionals that the modern DDoS attack is increasing in sophistication, scale, and frequency. NETSCOUT provides the industry's most comprehensive suite of DDoS attack protection products and services for the Enterprise, Cloud / Hosting, and Service Provider markets. For more information, visit https://www.netscout.com/ddos-protection.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECSB_028_EN-2101 04/2021