AGIO

AGIO OPEN EXTENDED DETECTION & RESPONSE

powered by Stellar & Tenable

Most Extended Detection & Response services (XDR) have a SIEM and scan for vulnerabilities. But most services don't have industry-focused security analysts sitting behind the screen with knowledge of what to look for and the initiative to apply industry-specific detections across client environments. We do.

Our Open Extended Detection & Response (XDR) service lies at the heart of our Detection & Response portfolio, and it includes a number of elements:

ASSET DISCOVERY

We begin our Open XDR service with an asset discovery process within your environment, which provides a referenceable inventory of all your protected endpoints. This is critical, given most firms struggle to ever map their endpoints thoroughly and accurately. Our assessment also ensures that changes to your environment, like adding or removing servers, security appliances, network devices, etc., are always captured so no endpoints ever fall through the cracks.

SECURITY INCIDENT & EVENT MANAGEMENT (SIEM)

We use a discovery-driven approach designed to prevent future security blind spots, adding user, application, and business service context to events. Whether your information lives in your own data center, a hosted environment or the cloud, our engineers collect, aggregate and normalize logs, providing unparalleled threat monitoring, prioritization and mitigation responses. We look at data across the full spectrum – from security devices, to network devices, Active Directory, Windows and Linux servers, database servers, storage, and applications – to cross-correlate all of your security event data in real-time. What's more, we offer industry-specific custom alerts and correlation rules so our service works smarter and faster for your unique business.

ACTIVE THREAT DETECTION

We defend against ever-evolving, sophisticated evasion techniques, even when they are applied on multiple protocol levels. Through deep packet analysis at the internet perimeter and business critical network segments, signature-based attack recognition, content analysis of your data stream, and best-in-class subscription-based threat intelligence, as well as Open Threat Exchange (OTX), our security engineers are armed with everything they need to see the forest through the trees, detecting movement and threats of malicious execution.

VULNERABILITY SCANNING

Our automated scans assess network assets for vulnerabilities on a weekly (or monthly) basis to clearly identify potential areas of exploitation and increased security risk. We track these ongoing vulnerabilities and provide continual remediation recommendations. Finally, we also do the dirty work of eliminating the false positives, so your internal teams don't have to – reporting to you on the operating system, patch levels, and running services on all monitored systems.

SECURITY OPERATIONS CENTER (SOC)

Our 24x7x365 SOC offers event and problem management along with unlimited support; troubleshooting and diagnosis of system alerts and outages; root-cause analysis including workarounds for immediate resolution as well as longer-term permanent remediation; threat hunting; and finally, real-time access to your security dashboard, events and alerts so you can always see what we see. Our CISSP and SANS GSEC-certified security team then create weekly reports on your environment and meet with you monthly to summarize the traffic trends, attacks, and anomalies we're seeing. We conclude each of our monthly sessions by walking you through your specific and actionable recommendations, including how to quickly and efficiently implement those improvements.

It's this level of service, delivered by our level of security engineers, on top of the best-in-breed platforms we leverage that set Agio's Open XDR service apart from the market. Our solution is the definition of a true 360° cybersecurity service to keep you protected and at the ready at all times.

WHY AGIO?

#OneAgio

When you select Agio, you're investing in a relationship with everyone who's a part of this firm. Our teams operate in a symbiotic relationship, based on deposits and withdrawals, that creates a vehicle for delivering more than just service. We deliver an experience that reaffirms to our clients we've got them covered. From clean, concise implementations; to consistent support backed by automation and tools that work the way they're supposed to; to value-add reporting; to accurate, timely invoicing; and content on the latest IT and cybersecurity trends, we bring the full breadth and depth of our talent to bear. We deliver #OneAgio.

For more information, please contact:

877.780.2446 | sales@agio.com