AGIO

CYBERSECURITY OPERATIONS

Cybersecurity is top of mind as cybercrime matures and escalates. According to the Gartner 2023 CIO Agenda Survey, cybersecurity is the main priority for new spending, with 66% of those surveyed increasing investment in cyber/information security in 2023.

When it comes to protecting your firm's data (and its dollars), your strategy needs to be bulletproof. Layering detection and response on top of a solid security posture is the first step.

Agio's Cybersecurity Operations portfolio uses AI and human brilliance to predict and preempt critical threats to deliver secure, fast, reliable technology support 24x7x365.

When you sign up for our Cybersecurity Operations portfolio, you get:

- **Agio Open Extended Detection & Response**
- **Agio Incident Response Service**
- **Agio Endpoint Detection & Response**
- **Agio Phishing Protection**
- **Agio Mobile Web Security**
- **Agio Executive Privacy Monitoring**

The second step is bringing managed IT under the same roof. Integrated cybersecurity and managed IT provides a holistic view of your environment to decrease the time it takes to resolve an issue.

When Cybersecurity Operations and managed IT aren't under one roof, time to resolution takes up to 40% longer. As your single partner, we can recover that time and resolve issues in hours, not days. This means you're 80% less likely to see a vulnerability escalate into an incident.

AGIO OPEN EXTENDED DETECTION & RESPONSE

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

SECURITY INCIDENT & EVENT MANAGEMENT (SIEM)

Mitigating risk depends on threat prediction, incident prevention, and quick response times.

Our intelligent system monitoring learns across the board to create automations that give context to alerts and incidents while our engineers analyze that data and apply industry-specific detections. The result is faster threat hunting and fewer blind spots so we can work smarter and give you unparalleled prioritization and mitigation responses.

What's more, our scalable SIEM can live anywhere—on prem, in the cloud, or a hybrid. It's easy to set up access controls and tenant structures that match your needs.

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 analysts 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)

We've invested heavily in advanced predictive technology. We use AI and machine learning automations to assess large datasets and identify patterns across organizations so we can prevent issues before they become a problem.

Our follow-the-sun SOC offers event and alert analysis 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 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 will work to establish a meeting and reporting cadence that fits your organization's needs. The reports will summarize traffic trends, attacks, and anomalies we're seeing. We conclude each of our 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 skilled security analysts and best-in-breed platforms 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 ready at all times.

AGIO SHIELD

We've made domain alerting smarter by putting up a force field around client environments, identifying new malicious domains set up by bad actors, and then leveraging AI to categorize the risk those domains pose to client organizations — all before the incident even reaches our analysts. This means you can rest easy knowing that your organization and employees are protected from the malicious links we've intercepted across our entire client base, not just those targeting your firm.

AGIO STING

Agio Sting is a next-generation deception technology service designed to identify, deceive and neutralize cyber threats throughout your environment. Specifically, our cybersecurity engineers will learn the ins and outs of your network architecture, identify your critical assets (both production and non-production), and then design a deception deployment that is customized to your specific needs. Each deployment consists of a complete managed service that integrates a honeypot to resemble the personality of your network architecture or critical assets. Honeypot tokens can be distributed on laptops, servers, and anywhere in your network or cloud to act as a tripwire that will detect malicious activity quickly with a high-quality signal.

AGIO INCIDENT RESPONSE SERVICE

Agio Incident Response Service is a planned solution designed for the unplanned. We onboard, organize, prep and continually test your ability to respond when a breach happens.

Specifically, the program includes:

- Onboarding
  - Environment Discovery
  - Data Mapping
  - Incident Response Plan Development & Review
    - › Incident Response Policy
    - › Data Classification Policy
    - › Incident Response Procedure
    - › Incident Response Communication-Chain of Command Procedure
  - Tactical/Operational Incident Response Tabletop Exercise
- Monthly Incident Response Readiness Review
- Quarterly Status Review (monthly for first three months after going live)
  - Intelligence Briefings
  - Cybersecurity Events & Incidents Statistics Review
- Annual Executive IR Tabletop Exercise
- Incident Response Annual Review & Report
- Red Team Security Assessment* (annually, if applicable)

And when a breach does happen, we mobilize immediately and effectively to neutralize the threat and contain your exposure. Here is our cadence for you:

- We respond within 15 minutes of discovery.
- We send updates every 2 hours and hold conference calls every 4 hours, for critical incidents.
- We work the incident until it's contained, and eradication and remediation plans have been defined.
- We send a full incident report, including recommendations, within 2 weeks of an incident being resolved.

AGIO ENDPOINT DETECTION & RESPONSE

We combine the most sophisticated endpoint detection technology with our 24x7x365 SOC to hunt, investigate and eradicate attacks before they damage your business. We go beyond no missed alerts, and proactively recommend changes to keep your environment more secure, always. Specifically, our service includes:

- Zero-Day Prevention
- 24x7x365 Detection & Response
- Threat Hunting
- Industry-Specific Configuration Baseline
- Script Management
- USB Mass Storage Management

AGIO PHISHING PROTECTION

Phishing is the #1 cyber-threat to your organization, which means you need a specific service designed to combat this specific beast. Our solution is a holistic, AI-driven solution to ensure your email stays protected as the threat landscape continues to evolve. We partner with Inky's best-in-breed Phish Fence technology, leveraging machine learning, behavior profiling and advanced heuristics forgery detection to uncover even the most sophisticated deep-sea phishing attacks that both trained users and conventional email filters miss. Once implemented, here's a run-down of what you can expect:

- State-of-the-art spam and anti-malware protection for both spear phishing and brand forgery attacks, while HTML sanitization blocks XSS, JavaScript, CSS attacks
- Incoming mail automatically checked against over two dozen computer vision and text analysis models that "see" the message much like a person would — so even very convincing forgeries get blocked
- Malicious mail automatically quarantined, while questionable mail is delivered with a clear, prominent warning your users will understand
- Users can click on the "Report Phish" link in an email to send the message to Agio's client support team for further analysis.

Bottom line, we've got you covered when it comes to the #1 threat to your users – phishing.

AGIO MOBILE WEB SECURITY

Agio Mobile Web Security protects your mobile workforce from advanced threats wherever they are - in the office or on the road - offering you visibility while securing traffic both on and off your networks. Our service specifically leverages DNS and IP layer enforcement to stop threats over all ports and protocols, preventing malware from reaching your endpoints. Content enforcement also utilizes 80+ content categories to ensure your workforce is adhering to firm policies in and out of the office. Finally, command and control callback blocking prevents infected machines from reaching the attackers' servers to thwart exfiltration of data and execution of ransomware.

AGIO EXECUTIVE PRIVACY MONITORING

Executive accounts are highly targeted by bad actors. To stop them in their tracks, Agio XDR Executive Privacy Monitoring provides 24x7x365 security analyst-driven monitoring to proactively monitor executive environments for abnormal behavior relating to their accounts, data, sensitive files, access and more. Our analysts then deliver automated reports that clearly identify alert conditions, baseline behaviors, trends, anomalies, and actionable recommendations.

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