SEDARA™

Sedara’s Approach to

Redefining XDR

Sedara is Your

Cybersecurity Sidekick.

There is no longer the concept of "boundaries to your network."

The perimeter is dead, and it takes a multi-faceted approach to make up for it.

In the past, cybersecurity has focused on network perimeter defense. You had a finite attack surface because your employees, applications, and data all lived and worked within a controllable environment. Now you have employees using public cloud assets, SaaS products, and uncontrolled networks due to the increase of remote work.

The fact is not that a network perimeter is difficult to defend, it's that it has expanded and changed so much that you no longer have a definable boundary to the data that you are responsible for protecting.

Cybercriminals are capitalizing on this new reality - to the tune of $4.1 billion in reported losses within the U.S. in 2020 alone - according to the FBI's IC3 report.

As a response to this new reality and the challenges it brings, Sedara has developed an innovative XDR methodology to help customers shift from a reactive cybersecurity strategy to a proactive approach.

What is XDR?

XDR is an architecture that enables enterprise-wide threat detection and response capabilities. This holistic architecture embodies the fundamental detect and response mission in the most comprehensive way.

X = Any data and any threat
D = Detection, with context
R = Response, appropriate to the threat

An effective XDR approach includes tools across different vendors, systems located at various points across your attack surface, and both cloud-based and on-premise security technologies and capabilities

There is no one-size-fits-all XDR implementation or blue-print. A powerful XDR solution must include detection and response capabilities at multiple attack vectors specifically identified for the organization. On top of having the appropriate ensemble of technology, it needs to be implemented and managed properly to deliver the best results.

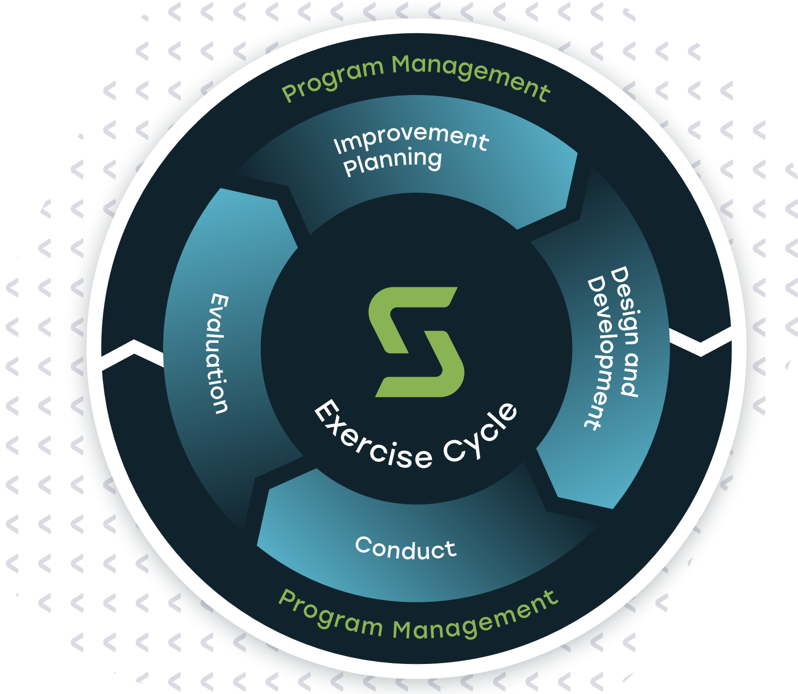
Sedara Approach to Extended Detection & Response

Many current security solutions approach cybersecurity through a focus ONLY on the technology. This entails collecting and analyzing event data from a static list of predetermined applications or devices from inside the network. Since there is no longer a definable network, this method lacks flexible proactivity, presenting additional challenges, and obvious shortcomings. Cybersecurity visibility is about analyzing what's important, from the right viewpoints. If you aren't considering the **angle of visibility** or **key business practices** in your analytics, you are already putting yourself at a disadvantage.

Sedara's approach to an XDR architecture resolves this challenge by integrating visibility and response technology with real-time, intelligent analysis of what exists within your environment, while continuously adjusting to how it changes day-to-day.

This allows us to identify any gaps that may exist and create a continuous lifecycle of increased visibility and security enhancements.

This is not a single tool or product. This is a collaborative approach to cybersecurity where our certified, experienced security engineers work with your organization to create a roadmap for this critical piece of your cybersecurity program. Such proactivity is achieved through a combination of real-time assessments of your organizational cybersecurity posture and vulnerabilities to identify technical and non-technical gaps. With this new strategy, we continuously provide hands-on management and execution of this lifecycle.



This process is repeatable by design, because the challenges raised by the new attack surface are not one-and-done. New devices, cloud assets, and remote networks are constantly being added, so your cybersecurity strategy needs to be fluid.

Sedara's Managed XDR (MDR) provides hands-on monitoring, management, detection, remediation, and response. It's designed to be customizable to your preferred technologies while keeping budget constraints in mind.

Results of Sedara Managed XDR:

- Increase network and behavioral visibility
- Provide specific analysis of key systems and accounts
- Regularly analyze completeness of coverage
- Improve network security posture
- Reduce risk
- Maximize the efficiency of certain technology investments and staff
- Reduce your mean time to detect, respond to and remediate threats

Cohesive multi-vendor support on a 24x7x365 basis

Our Unique Methodology

Monitoring alerts and responding to incidents are the most dramatic and visible parts of a cybersecurity strategy. However, maintaining a buzzing "alert factory" on its own isn't enough to protect a business. Through threat-based security frameworks, best practices and experience, Sedara's security operations exist at a deeper strategic level.

Sedara applies a proprietary methodology that is a culmination of years of real-world cybersecurity experience combined with industry accepted frameworks and best-practices.

The frameworks and best-practices that feed into our proprietary methodology include the following.

- **NIST Cybersecurity Framework v1.1 (NIST CSF 1.1)**
- **NIST SP 800-207 Zero Trust Architecture**
- **MITRE ATT&CK**

This methodology also utilizes cyber threat data that Sedara receives first-hand on a daily basis across our customer base and from multiple industry-leading threat feeds.

Our methodology assesses and scores the strengths and weaknesses of client security architecture while mapping to any and all governance, compliance, and regulatory requirements.

Based on a lifecycle, Sedara models security maturity based on prioritized opportunities for improvement. We use those capabilities to characterize and compare the present and target (ideal) states, enabling a gap analysis that guides the development of the organization's security posture, which in turn fuels the longer-term roadmap to get an organization to its target state. That roadmap navigates the following progression across the security lifecycle.

Prepare

Sedara uses years of experience combined with millions of events logged and analyzed to prepare your organization for when (not if) a threat occurs.

Detect

Sedara utilizes behavioral analytics and machine learning to detect critical threats as well as suspicious activity on your network.

Eliminate

When a threat is detected, Sedara deploys blue team SOC analysts and incident response experts to neutralize and eliminate the attack.

Enhance

Once a threat has been eliminated, Sedara will then utilize the data and behavior of that attack to ensure your network is immune to similar threats.

End-to-End Detection & Response

Sedara's Managed Detection and Response (MDR) Program simplifies and streamlines your ability to monitor, detect, respond, and remediate cyber threats throughout your entire network and cloud infrastructure 24x7x365.

Our cross-layered approach leverages industry-leading threat intelligence and existing or new internal resources to provide best-in-class, end-to-end cyber threat detection and response, maximizing your investments across all environments.

MDR Components

Security Operations
SIEM
UEBA
SOAR with Machine Learning

Network
Network Detection and Response (NDR)
Intrusion Detection and Response (IDS)

Endpoint
Advanced EDR with Machine Learning
Endpoint Protection
Vulnerability Management

Sedara's MDR program integrates seamlessly into your Cybersecurity Program to bridge the largest operational gaps we commonly find.

Leveraging MITRE ATT&CK

Complementary to your roadmap, Sedara uses the MITRE ATT&CK framework. MITRE ATT&CK is a comprehensive knowledge base of tactics and hundreds of associated methods that attackers leverage to compromise enterprises. It characterizes and gives context to specific potential attacks in terms of relevant tactics, techniques and procedures (TTPs). In this conception, tactics refer to attacker objectives. Techniques and procedures identify the means that attackers use to achieve them.

ATT&CK uses a series of matrices to associate tactics with actions that have been taken in the past by bad actors as well as mechanisms that are effective to detect and mitigate them.

Drawing on this deep understanding of the individual threat landscape as well as real-time threat intelligence, Sedara provides rigorous, relevant, and proactive detection and response optimized across data, clouds, applications and endpoints. The comprehensiveness of this approach unifies geographically distributed assets into a coherent security landscape.

Strategic Guidance & Hands-On Support

To further integrate the operational cybersecurity coverage that Sedara brings to the table through MDR, Sedara also provides Cybersecurity Development Programs (CDP) for the optimization of cybersecurity culture, strategy and execution.

For these programs, Sedara provides an experienced and dedicated cybersecurity team to build a long-term strategic roadmap that aligns people, process, culture, and technology to accomplish security and compliance goals with risk reduction.

The program develops and integrates a cohesive technical cybersecurity posture with processes, policies, and procedures - all tailored specifically for the organization. Sedara doesn't just build the program, but we also provide hands-on expertise to implement and help manage it on an ongoing basis.

The programs that we build with our customers encompass all five functions of NIST CSF 1.1 to ensure complete cybersecurity lifecycle development and management.

Conclusion

Sedara broadens the definition of XDR by offering a proprietary approach that gives structure to its customers' efforts to address the full spectrum of threats they face. Sedara draws on its broad experience and deep expertise, bolstered by best-in-class tech and solutions, to deliver a consultative approach that begins with a health check that launches a concerted and organized effort to elevate the customer's security posture with a combination of programs and services.

With Sedara, your business can blend solid day-to-day tactical defense with long-term cyber strategy that protects far into the future. This unique, holistic approach shows no weakness to potential attackers.

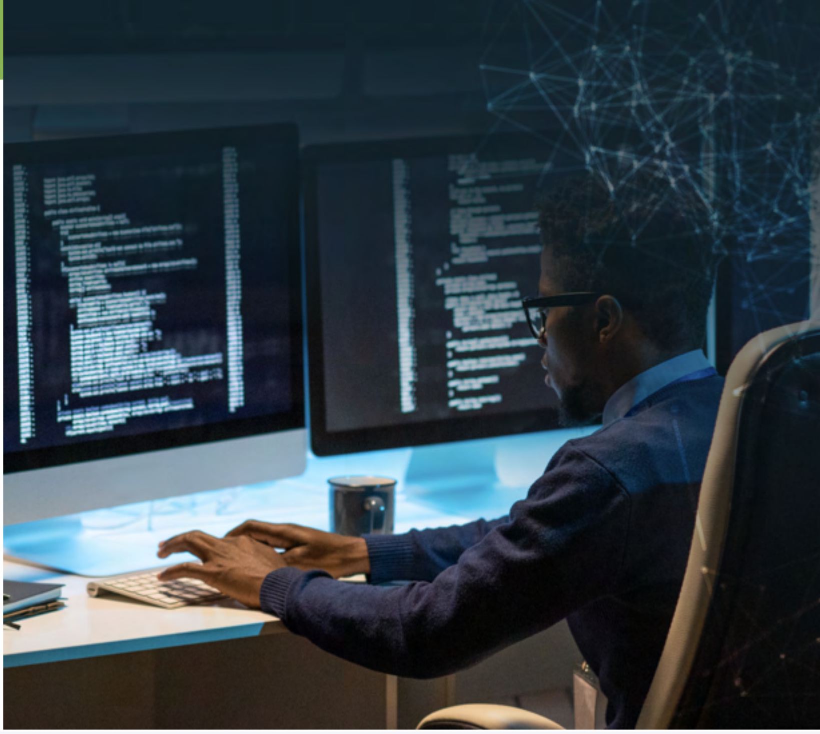
About Sedara

Sedara was founded in 2013 to streamline practical and effective cybersecurity for organizations of all sizes. We are headquartered in Buffalo, NY and live and breathe cybersecurity. Our communities are adopting technology faster than they can keep everything secure and this fundamental problem currently does not have an easy solution. This uphill battle drives us to bring honed cybersecurity expertise, strategies, and manpower to as many organizations as possible.

We know that it takes an innovative and flexible approach to provide meaningful, value-added security services to today's businesses, and help them protect what's important.

All Specialized Sedara Services

- Managed Security
- Pentesting
- Security Engineering
- Social Engineering
- Cyber Programs
- Assessments
- Virtual CISO
- Phishing Training



Trusted by Companies You Trust

LogRhythm CERTIFIED PARTNER TITANIUM

Carbon Black. FORTINET tenable RAPID7 SOPHOS CROWDSTRIKE

844.473.3272 • info@sedarasecurity.com • SedaraSecurity.com

SEDARA™