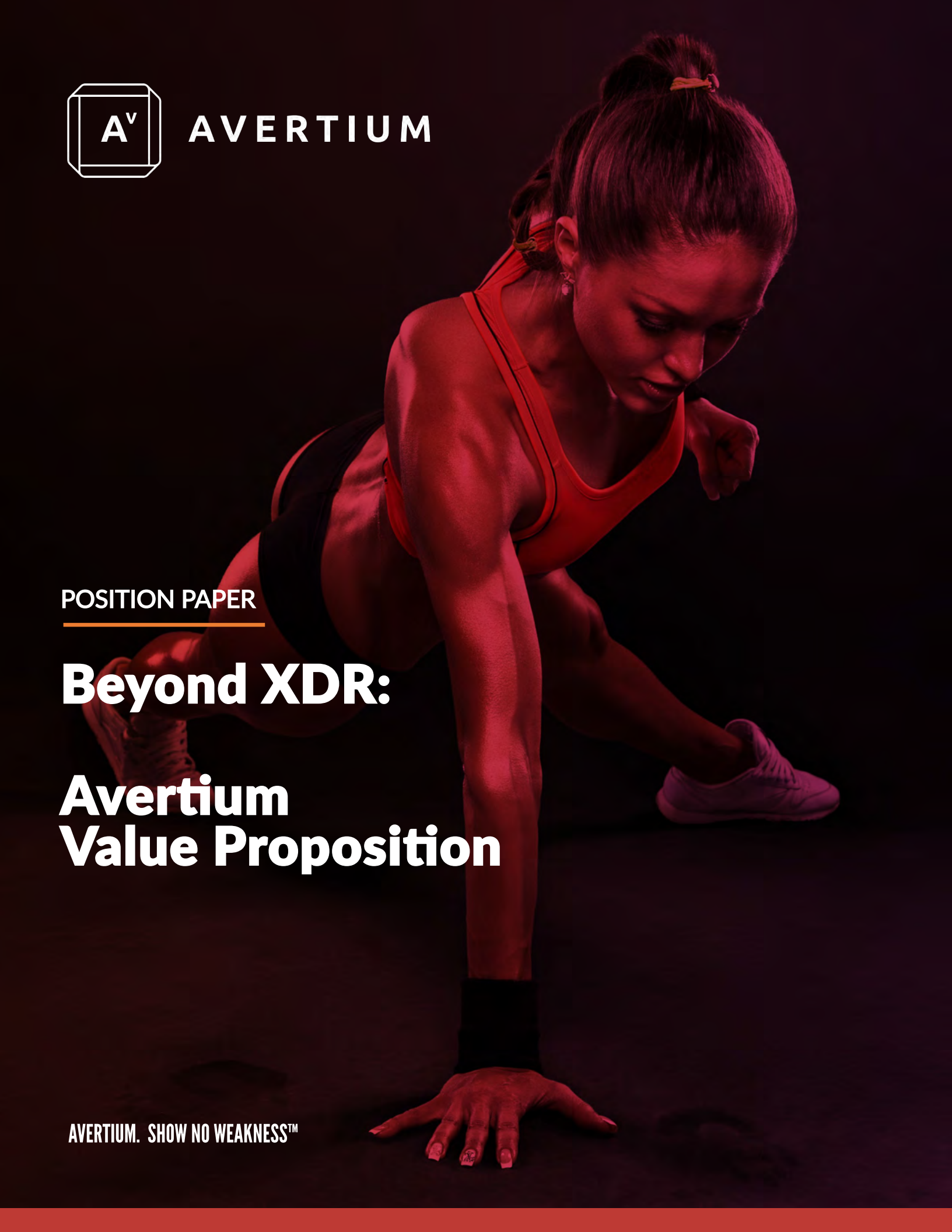


AVERTIUM

POSITION PAPER

Beyond XDR:

Avertium Value Proposition

AVERTIUM. SHOW NO WEAKNESS™

> The security industry has gotten so focused on security threats and this, in fact, is one of our greatest weaknesses... We need to fundamentally be reducing the attack surface as opposed to chasing after the latest threat.

- Pat Gelsinger, CEO, VMware

Table of Contents

INTRODUCTION 2

UNIQUE VALUE POSITION 3

INSIGHT THAT GUIDES ACTION: AVERTIUM CONSULTATIVE ENGAGEMENT 4

TURNKEY PROTECTION: AVERTIUM MANAGED SECURITY SERVICES 6

STRATEGIC GUIDANCE & HANDS-ON SUPPORT: AVERTIUM PROFESSIONAL SERVICES 8

CONCLUSION 10

Avertium reimagines the dynamics of cybersecurity in an organization to create a cohesive environment and tailor each unique implementation by applying breadth of experience and certified expertise to develop a long-term cyber strategy and integrate it with day-to-day tactical measures. This proprietary, holistic approach distinguishes Avertium among cybersecurity providers, creating a "show-no-weakness" security posture to would-be intruders.

Introduction

With the increased prominence of public cloud assets, remote users on uncontrolled networks and, data exchange among partners, the network perimeter has become difficult or (often) impossible to define. Cybercriminals are capitalizing on the opportunities this new frontier is creating with more intensity, making navigating this complex landscape without boundaries perilous. For example, 51 percent of decision makers believe their remote workers are not sufficiently protected, and breaches due to cloud misconfigurations cost companies worldwide $3.18T in 2019 alone.

> 51% of decision makers believe their remote workers are not sufficiently protected, and breaches due to cloud mis-configurations cost companies worldwide $3.18T in 2019 alone.
>
> - TechRepublic and DivvyCloud

In response to these challenges, Avertium offers a proprietary methodology to help customers shift their cybersecurity focus from a reactive and vulnerable state to a proactive show-no-weakness approach.

This paper examines the Avertium methodology and how this unique approach binds the elements of business and cybersecurity to generate an advanced security posture for each customer, built for the specific environment to maximize protection and mitigate vulnerabilities with more rigor, more relevance and more responsiveness.

XDR Reimagined

Traditional extended detection and response (XDR) enables cybersecurity through a technology focus by collecting, correlating and analyzing event data from any source on the network, such as endpoints, applications network devices and user interactions.

Avertium builds on this multi-dimensional model by combining deep knowledge of these capabilities in best-in-class technologies, its proprietary engagement methodology, and decades of certified expertise and broad experience in managed security and professional services. Avertium reconceives customer relationships by creating, in collaboration with the customer, a methodical and disciplined forward motion by which to improve an organization's security posture.

> "The pandemic, and its resulting changes to the business world, accelerated digitalization of business processes, endpoint mobility and the expansion of cloud computing in most organizations, revealing legacy thinking and technologies."
>
> - Peter Firstbrook, VP Analyst, Gartner

This consultative approach begins with a comprehensive cybersecurity and technology program review; an investigation of each customer's individual environment, risk management strategy, and available resources as well as other business, technical and human factors to establish a baseline. This baseline is translated into a maturity model, measured against an industry framework, and peer organizations. Then, both parties set a course to deliberately drive the customer's security path forward to arrive at where it needs to be. This shared understanding and partnership forms a deep commitment to achieving a common goal to improve every Avertium customer's security posture by applying best practices, experience and expertise.

Unique Value Position

Few cybersecurity companies offer the breadth of services of Avertium: Fewer still have the depth of experience and expertise in each of those disciplines. Avertium's services range from 24/7/365 managed security and related services from its award-winning CyberOps Centers of Excellence to risk and security assessments, advisory and compliance from its Professional Services.

Operating from the initial maturity model, Avertium's decades of experience empower its teams to map the customer's overall needs to its managed security and professional services that enable a layered approach in delivering capabilities to answer the highest priority needs first, then, following the path laid out before them, continue to address challenges to arrive at a more secure state and mature program.

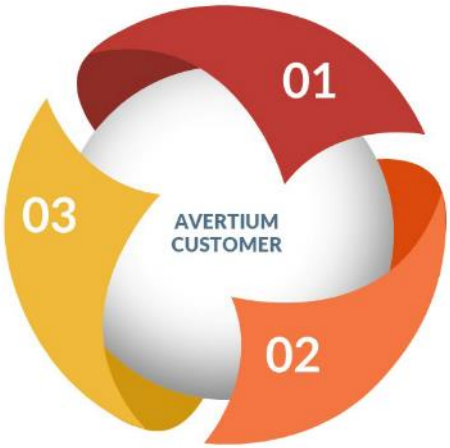
Avertium Managed Security Services crafts and delivers on a strategic cybersecurity roadmap for each customer that informs day-to-day prevention, monitoring and response services enabling teams to triangulate on threats that would otherwise remain obscure.

Avertium Professional Services align strategic requirements with tactical dimensions of the solution through ongoing security assessments, audit and compliance services and broad-based engineering.

> "Part of the reason [we use Avertium] is because they can consult from top to bottom. They can do a good job of assessing in extreme detail, but they can also sit at a board table and help articulate what risks are associated with major acquisitions."
>
> - Avertium Customer

Avertium provides a unique holistic approach that combines day-to-day tactical measures with a deep connection to individualized long-term, roadmap-based strategy. This value proposition is made possible through the marriage of Avertium Managed Security Services and Professional Services.

Combined, Avertium Managed Security Services and Professional Services provide a dynamic engagement model that Avertium uses to constantly optimize for changing customer needs. In this way, Avertium ensures the whole is greater than the sum of its parts as it relates to the customer's security posture to provide more rigor, more responsiveness and more relevance.



1. More Rigor. Deep capabilities in every cybersecurity specialty from monitoring and detection to training and compliance, plus the commitment to work more closely with every single client.

2. More Relevance. Beyond check-the-box solutions and standard compliance measures to true best practices that match the specific threat environment and security requirements.

3. More Responsiveness. Highly experienced professionals who can act faster because they know you, know your systems, know your business, and know security.

This holistic approach is unique to Avertium, and it provides an added dimension to cybersecurity not available from competing providers or in-house teams, which typically stop at the level of managing alerts and alarms and check-the-box solutions.

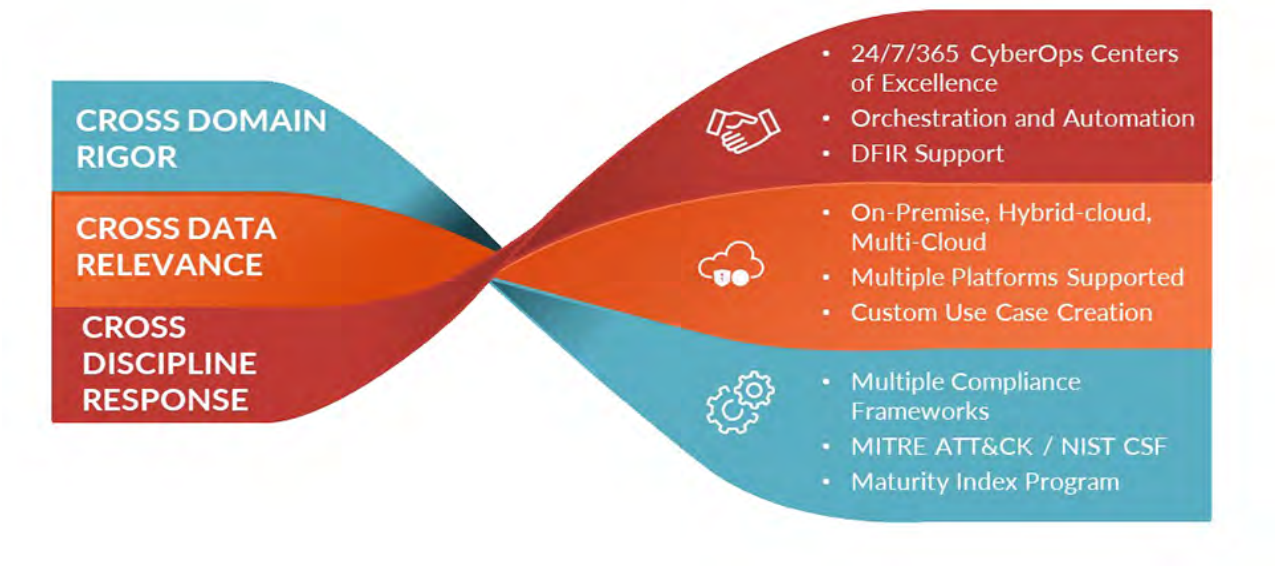
This places Avertium in a unique position to work cohesively and consistently toward a secure and compliant state on behalf of its customers.

Insight that Guides Action: Avertium Consultative Engagement

Engagements with security providers typically begin with vendor tools and solutions at the center of the discussion. While Avertium values automation and software capabilities, this tools-first approach can easily distort overall requirements by attempting to fit customer needs to a particular product. This forces a focus on aspects of the threat landscape most relevant to the solution instead of the wiser course of taking a broader, more objective view of the customer's environment.

By beginning each engagement with a health check examining the customer organization's individual requirements and its current security program from a tools-agnostic perspective, Avertium views the customer needs objectively, then assigns the proper solution - or set of solutions - according to its range of chosen best-in-class technologies.

This comprehensive analysis includes factors such as business processes, the threat environment, regulatory requirements, existing security measures and in-house level of expertise.



Avertium applies the insights it gathers from this process to assign a health score and then enables an approach to XDR tailored to the specific customer's needs, based on three tenets:

- ✓ **Cross-domain rigor.** Avertium brings deep capabilities across cybersecurity specialties, from monitoring and detection to training and compliance.
- ✓ **Cross-data relevance.** Custom use cases based on overarching best practices match security requirements to specific threat profiles across on-premises, multi-cloud and hybrid infrastructures.
- ✓ **Cross-discipline response.** Highly experienced professionals provide 24/7/365 monitoring and coverage informed by deep understanding of each client's business and IT environments as well as the ability to conform to all relevant compliance and regulatory standards.

Avertium develops custom use cases as part of its engagement strategy that articulate opportunities to maximize the value of a company's investments and knowledge base to foster more secure, efficient and successful operations. Avertium's consultative approach works to make security measures resonate with higher-level business considerations and instantiates those use cases with its proprietary approach to XDR.

Turnkey Protection: Avertium Managed Security Services

Fueled by customer engagement, Avertium Managed Security Services applies certified expertise in best-in-class technologies to interpret security data from across the on-premises, cloud, remote and endpoint environment to efficiently detect and analyze threats.

Core services bring together a range of capabilities to perform continuous real-time analysis:

- Managed SIEM
- Managed Detection & Response (MDR) with Endpoint Detection & Response (EDR)
- Zero-Trust Networking
- Vulnerability Scanning as a Service

Combining certified expertise in these technologies with threat-based security maturity analysis and modeling informs the total context of the threats encountered during day-to-day operations. Optimizing visibility and insight across all elements of the environment, regardless of source, complement a deep understanding of the business and technical requirements that underlie it.

Aggregate Knowledge

Recognizing the benefit of shared knowledge, Avertium aggregates all data from the expanse of its customer base ranging in unique or trending experiences, scenarios and industry-specific situations to create a playbook from which to operate. This manual informs and provides strategic insight to map overarching business and security requirements to specific aspects of the organization's security posture.

Avertium CyberOps Centers of Excellence

To ensure mission-critical cyber protection for its customers on a 24/7/365 basis, Avertium rigorously holds itself to a gold-standard state of security maturity. Using its geographically distributed, cloud-based security framework, Avertium's CyberOps Centers of Excellence (CCOE) continually assess and refine every policy, process and procedure to iteratively strengthen customer security postures. Highly efficient operations drive fast response and resolution of threats.

OmniQ Cloud-Native Cyber Integration and Orchestration

Avertium security analysts maintain an overarching view of its customers and tools at the same time. Rather than dividing attention between customer environments, devoting only a slice to each, Avertium's proprietary OmniQ platform uses APIs to unify SIEM, EDR and other tools across customers with a single interface. OmniQ helps Avertium analysts sort through floods of alerts to

quickly eliminate false positives, escalate incidents automatically when needed and facilitate advanced analysis and threat hunting.

Rigorous Approach

Managing alerts and responding to incidents are the most dramatic and visible aspects of cybersecurity. However, maintaining the tactical actions of a buzzing "alert factory" is not enough to protect a business on its own. Avertium's security ops function at a deeper strategic level through industry frameworks and best practices for threat-based security.

Avertium applies the National Institute of Standards and Technology (NIST) Common Security Framework (CSF) to assess the strengths and weaknesses of each individual organization's security architecture and to assign a score on that basis.

The NIST CSF is based on a lifecycle approach that models security maturity based on prioritized opportunities for improvement. Avertium uses these capabilities to characterize and compare the present and target (ideal) states, enabling a gap analysis to guide ongoing development of the organization's security posture, which fuels a customer-specific three-year roadmap toward the target state. That roadmap navigates the following progression across the security lifecycle:

- ✓ **Baseline state.** The security posture as defined at the beginning of the engagement provides the baseline from which Avertium develops the security roadmap.
- ✓ **Enhancement phase.** Measuring the baseline state against the desired target state reveals key risks that Avertium addresses with high-priority mitigation controls.
- ✓ **Optimization phase.** Having dealt with the most-critical concerns, Avertium iteratively implements additional controls, processes and technologies that integrate pervasive security throughout IT and business functions.
- ✓ **Target state.** The fully-realized target state represents full implementation of the strategic security program, highly automated and integrated across workstreams.

> **Note:** Avertium security analysts tailor the analysis and modeling to individual customers, including the use of other industry standards or frameworks as alternatives to CSF.

Leveraging MITRE ATT&CK

Complementary to the roadmap, Avertium uses the MITRE ATT&CK framework, a comprehensive knowledge base of tactics and hundreds of associated methods that attackers leverage to

compromise enterprises, to characterize and give context to specific potential attacks in terms of relevant tactics, techniques and procedures (TTPs). In this conception, tactics refer to attacker objectives, while 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, Avertium provides rigorous, relevant and responsive detection and response optimized across data, clouds, applications and endpoints. The comprehensiveness of this approach unifies geographically distributed assets into a coherent security landscape.

Complementary to that day-to-day operational coverage, Avertium provides a range of professional services that optimize cyber strategy on an ongoing basis.

Strategic Guidance & Hands-On Support: Avertium Professional Services

> "It's been outstanding [working with Avertium]. I trust implicitly the leadership and the quality of resources that are brought to the table. [They] always advise us in the direction of a strong balance between how you mitigate risk and how you also keep the business going."
>
> - Avertium Customer

Cyber strategy must continually assess the state of the specific risks and threats that face an organization, and then respond to that situational analysis. Those strategic concerns are distinct from the tactical dimension because they focus on the overall threat landscape that persists over time, as opposed to detection of and response to individual attacks.

While Avertium Professional Services also provide specific tactical elements, they consist primarily of a comprehensive structured approach that gives customers clarity around the factors that feed into strategic planning. The subsets of this set of offerings are security assessments, compliance and audit, and professional consulting.

Security Assessments

To determine the state of an organization's security posture over time, Avertium offers robust, repeatable security assessments. This type of analysis is designed to be broad enough to encompass the full threat landscape while also being tuned to reveal strengths and weaknesses of the individual organization's security program.

Direct assessment of vulnerabilities in elements such as the organization's architecture, systems and organizational business practices culminates in active threat hunting, where Avertium analysts identify specific threats and proactively mitigate them.

Penetration testing is another proactive measure that simulates attacks by both insiders and outsiders, against various types of resources that include websites, applications (including mobile apps), networks and endpoints.

Finally, Avertium vulnerability and architecture assessments include identifying specific risks to an organization from social engineering and mitigating them by means of detection and prevention tools, as well as training and education to prepare end users to resist these attacks.

Compliance & Audit

Directly related to the protection of assets and business continuity, organizations are commonly compelled to demonstrate readiness by conforming to standards and controls related to security. A specialty in itself, conforming to these requirements can be onerous for businesses of any size, and they also tend to vary by geographical region. Avertium maintains the expertise not only to facilitate compliance, but also to do so efficiently across various compliance standards and frameworks required by PCI, HIPAA, HITRUST, NIST, SOC, personal data privacy, ISO and many others.

Avertium also takes the burden off its customers in terms of proving compliance for audit purposes, providing modeling and reports to both prepare for and respond to internal and external audits. When audits dictate remediation requirements, Avertium also provides the expertise to meet them efficiently and comprehensively.

Professional Consulting

Security requirements inevitably arise that outstrip any organization's ability to address them using existing internal resources and skill sets. Avertium provides professional consulting services to fill those gaps in a timely and robust manner.

This category includes both tactical and strategic service offerings. Tactically, for example, Avertium's services can give peace of mind by providing emergency surge resource capacity for response to specific incidents as well as advisory services, tabletop wargaming and litigation support.

At a more strategic level, Avertium helps organizations develop programs, roadmaps and procedures as well as strategize around cyber reporting mechanisms. More broadly, these services include Digital Forensics and Incident Response (DFIR), strategic consulting and engineering services.

Conclusion

Avertium 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. Avertium draws on its broad experience and deep expertise, bolstered by best-in-class toolsets 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 managed security and professional services.

With Avertium, your business can meld rock-solid day-to-day tactical defense with long-term cyber strategy that protects for the long term. This unique holistic approach shows no weakness to potential attackers, so you can safely focus on making your business more competitive and more successful.

About Avertium

Avertium, one of the largest cybersecurity services providers to the mid-to-enterprise market, is redefining the landscape with its distinctive show-no-weakness approach. Forged out of three award-winning cybersecurity services companies, each with a unique perspective on the security landscape, Avertium brings enterprise-level security to the many mid-sized and larger organizations that don't have access to comprehensive, specialized protection. More than 2,500 organizations in industries ranging from financial services and manufacturing, to technology and healthcare benefit from Avertium's managed security, consulting and compliance services delivered with more rigor, more relevance, and more responsiveness. The company's dual security operations centers are located in Arizona and Tennessee.

Avertium. Show No Weakness.™

AVERTIUM

+1 (877)-707-7997
hello@avertium.com
www.avertium.com