Tailored Security Engagements

Solution brief

Cybersecurity assessments built around an audit or compliance approach can be effective for a variety of companies and conditions. But what if your organization's needs don't fit neatly inside of the compliance lines? Today's rapidly changing industries may require a more tailored look at your cybersecurity posture.

Unlike traditional assessments built around an audit or compliance approach, Tailored Security Engagements are not limited to a single framework such as NIST or PCI. Instead they focus on identifying the specific elements that will provide the greatest actual security value to the organization within the cybersecurity operations ecosystem. Each Tailored Security Engagement has a focus area designed to address a prevalent and common challenge faced by cybersecurity programs and Security Operations Centers (SOCs).

Tailored Security Engagements.

Verizon's Tailored Security Engagements are focused on improving the effectiveness of the cybersecurity operations ecosystem. This is achieved by partnering with the client organization to understand what actions the client is performing/not performing, and how effective those specific processes and technologies are in providing actual operational security value to the organization.

The Tailored Security Engagement deliverable is a meeting to review Verizon's written report containing prioritized recommendations that are immediately actionable, and focus on the specific steps necessary to mature and enhance the client's cybersecurity operations ecosystem.

67%

of breaches studied in the 2020 Data Breach Investigations Report were caused by credential theft, social attacks (i.e., phishing and business email compromise) and errors

Applicable to every organization.

Tailored Security Engagements can be relevant to public and private institutions in both regulated and unregulated industries, and for companies of all sizes. They are often valuable when organizations are faced with one or more of the following scenarios:

- Looking to enhance operational cybersecurity posture, but unsure of where to start
- Needing to standardize security operational posture after a merger/acquisition
- Ensuring that the cybersecurity operations program is aligned with the current threat landscape
- Optimizing SIEM capabilities, or incident remediation processes, due to perceived deficiencies
- Improving the efficiency and effectiveness of SIEM content development, and security use case management

Methodology.

There are four traditional engagements that a client can consider:

Cybersecurity Risk and Security Operations Alignment

This engagement addresses the questions "Does your cybersecurity monitoring program detect attacks involving the most common threats faced by your industry?" and "How can you be sure?" We evaluate whether your security monitoring is aligned with your industry's current threat landscape, and identify the gaps between types of threats faced and your capabilities to detect and respond to those threats.

SIEM Development Engagement

"Are you receiving the value you expect from your SIEM platform? Are you confident in the detection capabilities of your security monitoring program?" We evaluate your Security Information and Event Management (SIEM) platform in the context of threat landscape and organizational needs, and offer recommendations on how to enhance overall effectiveness.

verizon

Cyber Response and Development Engagement

"Are your incident response policies and processes effective in responding to attacks against your organization? Are your security analysts able to effectively respond to all tickets within an acceptable time frame?" This engagement offers a detailed evaluation of your current threat detection and response processes and procedures, identifying capabilities and functions that will help the Security Operations Center (SOC) and Incident Response environment.

Security Use Case Process Development and Categorization

"How effective is your security monitoring content library in detecting threats to your industry? How can you be sure that security monitoring requests that are time-sensitive or highly impactful are implemented first?" We categorize your existing SIEM content rules and identify gaps in the security monitoring based on Verizon's Data Breach Investigation's Report (DBIR). Clients are given detailed recommendations on how to enhance their cybersecurity use case capabilities.

At the beginning of each engagement, Verizon will meet with the client to discuss the organization's current environment and their goals. This helps us scope some of the tailored elements.

After the engagement is scoped, the Verizon team reviews initial client documentation before meeting with client stakeholders and subject matter experts to gather the additional information required. Reviews typically require client environmental and operational information such as SOC/CIRT policies and procedures, cybersecurity policies and standards, event logging, network operations and engineering, vulnerability management, incident response processes, security tools and devices such as firewalls and IDS/IPS, etc. At no stage in the engagement should a client's business be impacted.

After analyzing the information collected and capturing our recommendations we create a report with actionable, prioritized recommendations for client review.

TAILORED SECURITY ENGAGEMENT OUTCOMES

- Tailored report with prioritized recommendations that are immediately actionable
- Improved cyber resiliency by identifying the most significant gaps, and remediation options
- Guidance for optimizing the utilization of existing cybersecurity and organizational resources
- Performed by a highly experienced team that has worked with organizations in all industries around the globe

Why Verizon.

As an award-winning leader in cybersecurity, we keep up with the rapidly changing nature of cyber threats by processing billions of security events each year, analyzing evolving threats at our global security operations centers, performing forensic investigations for companies around the world, and sharing our knowledge through industry-recognized content like the annual Data Breach Investigations Report.

We differ from other security service providers because of the extensive practical experience of our personnel. The global team that delivers security engagements has many years invested in building, running and maturing cybersecurity monitoring programs across all industries. And, our substantial risk and incident experience lets us understand the real-world security controls that are effective, and not effective. When it comes to cybersecurity, our priority is your long-term success.

Learn more.

For more information on Verizon's Tailored Security Engagements, contact your account representative.

For the 2020 Data Breach Investigations Report, go to: enterprise.verizon.com/resources/reports/dbir

verizon