Trustwave®

DATA SHEET

Trustwave Threat Detection and Response Consulting

EMPOWERING THREAT DETECTION AND RESPONSE CAPABILITIES

Benefits

- Optimize security toolset
- Adapt to evolving threat landscape
- Drive business innovation and growth
- Address security talent shortage
- Communicate business value through analytics

In response to the increasing likelihood of a breach, organizations are looking for ways to optimize their existing security investments to increase their threat detection and response capabilities. Adding more technology is no longer the only answer. But any new plan must also be agile enough to address the rapid changes in modern attacks. Security teams have a new challenge: Detect faster, respond quicker, adapt sooner.

Trustwave Threat Detection and Response (TDR) consulting partners with organizations to tailor an approach to enhance their threat detection and response capabilities. CISOs often have the vision of where they want to go but struggle with the investment required to make it real. Taking in to account current people, processes and technologies, Trustwave TDR Consulting works with organizations to create an agile, go-forward plan tailored to their evolving needs.

People

Security talent is in high demand, creating an environment where organizations are looking for security "superheroes" versus "key players". Optimizing the "people" resource is crucial to minimize the lag in security execution.

Process

For many organizations, security processes have been developed ad-hoc over a period of years. Processes must be structured, agile and able to demonstrate effectiveness to meet the demands of modern cybersecurity.

Technology

There is no shortage of security technology. As CISO's review their budgets, questions on risk mitigation, value, and effectiveness is top-of-mind. Technology is vital, but it must be aligned to the business cyber risks in addition to enhancing threat detection and response capabilities.

Advise, Transform, Operations – A Transformation Methodology for Success.

Organizations are looking for agile partners that provide subject matter leaders in cyber threat detection and response transformation. Trustwave delivers an adaptive engagement model, applying our security expertise to the problem statement to craft a project scope and engagement. Each project may reflect one, or more, elements of the advise, transform, operations methodology.

Advise

Trustwave combines best practices from over 20 years of security experience with well-known capabilities and maturity models to help an organization understand their current, target and future security state.

- SOC maturity benchmarking vs industry
- Gap analysis and project roadmap
- Capacity forecasting and cost impacts

Transform

SOC, SNOC, ISOC, CSDC, Fusion center…whatever the name, the Trustwave TDR Consulting team works closely with the existing security team to put the new capabilities to work.

- People optimize the operating model, establish and enhance the governance program
- Process Create and optimize the service catalog, playbooks, and KPIs
- Technology Streamline the workbench to support the people and the process. Develop metrics and reporting that communicates the business value of the prevention, detection, and response program. Deploying and optimizing cyber workbench, including SIEM, SOAR, Threat Intelligence, and Business

Operations

In-house, hybrid or outsourced; ongoing operations that enhance an organization's threat detection and response capabilities

- Capacity analysis and forecast
- Training and enablement
- Strengthening the culture

Engagement tracks

- SOC build and optimization
- Threat Intelligence build and optimization
- Vulnerability and patch management program build and optimization
- Use case framework and attack surface mapping
- Security maturity benchmarking and gap analysis
- Transformation roadmap
- Technology workbench deployments and optimization

For more information: www.trustwave.com