Do you know your risk score ?

Now more than ever, IT Leaders struggle with how to understand, prioritize, and analyze the overall risk posture for their entire IT environment. Whether reacting to a breach, preparing for an audit or compliance regulation, or proactively looking to improve visibility and control across the organization, IT leaders are looking for expertise and assistance.

94% of enterprises lack visibility or have inaccurate information on up to 20% of endpoints [1]

1.Vanson Bourne research study & Tanium

The Avanade Security Risk Assessment powered by Tanium is a 5-day activity which can help provide IT security leaders a comprehensive view of risk posture across their enterprise and proactive ways to protect their organizations from growing cyber threats like ransomware, insider threats and vulnerabilities.
The assessment is a lightweight consulting service that examines key risk vectors as well as cyber hygiene metrics and deployed security or compensating controls to achieve a repeatable and objective assessment of the IT landscape.

Develop a strategy that will provide real time data & actionability at scale

- Complete & Real-Time Visibility
- Patching with Speed & Scale
- Reducing Silos between Operations & Security
- Cost Savings

avanade

©2023 Avanade Inc. All Rights Reserved.

TANIUM

How will this Assessment help me ?

Avanade's Security Risk Assessment will provide a comprehensive report of risks and vulnerabilities, and a prescriptive remediation and implementation plan to help CIOs/CISOs:

- Identify, prioritize and address security risks
- Support and contextualize their priorities and associated budget asks when communicating with their executive team and Board

Our Approach

We follow a multi-stage approach:

- In pre-execution, we prepare the client environment for agent deployment
- During the execution phase, the agent gathers data from the PoC environment
- Post-execution of the data collection, we generate an analysis and report with key findings

Outcomes Include

- Business process and technology roadmap for Microsoft maturity structure inclusive of functions, activities & integration best practices
- Maturity and value of Microsoft implementation and utilization in customer enterprise architecture
- Identified gaps in cybersecurity architecture
- Roadmap for enhanced Microsoft maturity program

Solution

Services

- Avanade Security and advisory consulting

Software

- Tanium Cloud POC environment
- Microsoft Defender for Endpoint Health dashboard

Activities

Day 1:
Verify AV/firewall/VPN, deploy Tanium clients, and configure Tanium platform for the assessment

Day 2:
Configure Asset SIU, Validate Comply and Reveal scan status

Day 3:
Validate Reveal scan status

Day 4:
Assign asset criticality to endpoints

Day 5:
Assessment data collection (automated)

Outcomes

- **Executive Summary**: composite risk score, asset inventory, proposed implementation plan, and Log4j exposure analysis.
- **Risk vector analysis**: detailing your risk posture by diving into system vulnerabilities, system compliance, lateral movement assessment, sensitive and protected data exposure, insecure transport security protocols, and encryption and mutual authentication.
- **Report: i**dentifying compensating controls & asset criticality, endpoints without controls (such as credential guard), endpoint hardening, antivirus/antimalware and more. Explanation of the criticality level assigned to the assets within the scope of the assessment.
- **Cyber hygiene metrics**: asset inventory, patch status, and risk exposure to vulnerabilities. What applications are running/what software you are not actually using.

Start your journey to build cyber resilience, prevent breaches and detect ransomware attacks.

Contact MicrosoftOfferings@avanade.com to get started

avanade

©2023 Avanade Inc. All Rights Reserved.

TANIUM