tenable

SOLUTION OVERVIEW

CYBERSECURITY INSURANCE CHECKLIST

Meet Insurance Requirements with Tenable

Business Challenge

Securing cybersecurity insurance policies is no longer guaranteed and increasingly expensive. It is referred to as a "hard market" industry-wide, with premiums increasing 30% or more in some cases year over year. Not only is it difficult for insurance companies to effectively price risk, it's an incredibly labor intensive process for organizations to provide underwriters with supporting information about their cyber programs and obtain policies. Most insurance companies rely on clunky questionnaires and security rating services, which do not always give the full story.

Solution

Tenable's exposure management platform is meant to be the foundation of your cybersecurity program, and provides risk information across important pillars such as vulnerability management, active directory, external attack surface management, cloud security and more. Therefore, Tenable is well-suited to provide richer cyber hygiene data to cyber insurance underwriters.

Cybersecurity Insurance Checklist

COMMON ELIGIBILITY QUESTIONS	TENABLE VALUE
Do you have a process for discovering and maintaining a complete inventory of your cyber assets?	With Tenable you can discover all your assets from IT to code repositories to clouds. Once you've discovered these assets, Tenable provides specialized assessment tools to find misconfigurations and vulnerabilities across IAC, Cloud, Active Directory, Container, IOT/OT/SCada, traditional IT assets and much more. To gather information, a variety of sensors are deployed across your environment. The sensors that connect to the platform play a major role in collecting security, vulnerability and asset information so that you can manage, monitor and track information systems, applications and user accounts. Tenable VM platforms support several sensors today: Nessus vulnerability scanners, passive scanners and Nessus Agents. Each sensor connects to the VM platform where asset and vulnerability information is collected and organized giving you a complete picture of the assets, applications, users, and their vulnerabilities on your network. Tenable supports over 200 different types of detections for systems and software no longer supported.

COMMON ELIGIBILITY QUESTIONS	TENABLE VALUE
Do you monitor your external attack surface - internet-facing systems?	With Tenable's External Attack Surface Management (EASM) capabilities found within Tenable One Enterprise and Tenable.asm organizations can continuously discover and monitor connections to their internet-facing assets so that they can assess the security posture of their entire external attack surface.
Are you regularly doing vulnerability assessments against all your known assets?	Tenable delivers visibility into all assets and vulnerabilities across your entire attack surface, so you can assess everything. Tenable enables security teams to focus on the vulnerabilities and assets that matter most, while deprioritizing the vulns that attackers are unlikely to ever exploit. With coverage for more than 74,000+ vulnerabilities, Tenable has the industry's most extensive CVE coverage and security configuration support to help you understand your security and compliance posture with confidence.
Do you regularly perform misconfiguration assessments against all your known assets?	Tenable can display misconfigurations when resources fail to comply with the configured policies. You can also view the resources impacted by these misconfigurations and remediate the impacted resources.
Do you have an appropriate SLA to remediate high and critical findings?	Tenable enables you to meet SLA's by combining real-time continuous assessment, event prioritization so you know where to start first, and detailed step-by-step remediation instructions for your mitigation.
Do you scan external facing (web) or cloud assets for known vulnerabilities and outdated software?	Tenable provides agentless scanning and assessment to quickly and easily discover and analyze all their cloud assets. Continuous protection is provided via live scans that are automatically triggered by any logged change event. Collected data is then integrated into the Tenable Research Vulnerability & Threat Library. When a new vulnerability is published to the threat library, Tenable allows security teams to see if a vulnerability exists in their current asset inventory, without needing to execute a new scan.
Do you regularly assess active directory for GPO misconfigurations?	Tenable immediately surfaces all GPO vulnerabilities and misconfigurations. We also prioritize which mitigation tasks are most critical, and include step-by-step instructions for remediation. Tenable is easily deployed, without the need for administrative access or agents, and instantly begins to provide context on how to secure Active Directory.
Do you regularly assess active directory for least privilege access requirement?	Tenable assists with assessing least privilege access by measuring the security exposure of an asset and evaluating all paths to and from the asset from any specific point. Tenable also helps prevent configuration drift and ensure that least privilege access remains in place in the environment.
Do you have a monitor active directory for signs of misuse?	Tenable provides real time attack detection and analysis. We are able to detect AD misuse attacks in real time and provide step-by-step mitigation tactics. Tenable's real-time detection allows you to monitor AD security posture at all times and analyze any active threats using templated and customizable dashboards.

About Tenable

Tenable® is the Exposure Management company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

How Tenable can help

An effective exposure management program helps organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate cyber risk to support optimal business performance. While the above questions have appeared on questionnaires, there are other considerations that cyber insurance underwriters take when evaluating your cybersecurity program. Tenable can help your organization with cyber insurance readiness across vulnerability management, identity security, cloud security, and more.

Cyber insurance companies recognize the importance of vulnerability and exposure management for minimizing risk, and preventing cyber attacks. Tenable is an AIG approved security vendor, preferred cybersecurity partner for Lockton, and insurance underwriting strategic partner with Measured Insurance.

For more information on how Tenable can help your organization, check out our Tenable Products and Cyber Insurance pages.

tenable®