UNDERSTANDING RISK-BASED VULNERABILITY MANAGEMENT

Devices, tools and users are constantly being added to your network and widening the attack surface. Every new addition adds another possibility for misconfiguration and vulnerabilities. The longer a vulnerability goes undetected, the greater the risk. Sound familiar? Security teams across industries all live this reality every day.

That's where risk-based vulnerability management can help.

You can't protect what you can't see. Gaining broad coverage and thorough assessment of traditional and modern assets allows you to create a clear map of your attack surface. This lifecycle provides complete visibility into the attack surface and provides the necessary visibility to prioritize remediation efforts. Then the continuous assessment (because cybersecurity is never set it and forget it) allows for monitoring of new and transitory assets when they become active.

The nuances of risk-based vulnerability management can be summarized in Tenable's five-stage lifecycle. Each stage makes tackling devices straightforward.

STAGE 1 | DISCOVER: Identify and map every asset across and computing environment.

STAGE 2 | ASSESS: Understand the state of all assets. This includes the status of vulnerabilities, misconfigurations and other health indicators.

STAGE 3 | PRIORITIZE: Understand exposures in context to prioritize remediation based on asset criticality, threat context and vulnerability severity.

STAGE 4 | REMEDIATE: Prioritize which exposures to fix first and apply the appropriate remediation or mitigation technique.

STAGE 5 | MEASURE: Calculate, communicate and compare cyber exposure and key maturity metrics to drive risk reduction.

The real gem is in the machine learning capabilities. Prioritization of which vulnerabilities to remediate first will drastically lower risk. This is achieved through machine learning models that automatically combine vulnerability severity data with threat intelligence and asset criticality to predict each vulnerabilities impact on your organization.

As with most tools today, all this information is summarized in tailored dashboards. At the end of the day, your team can remediate high-priority vulnerabilities while delivering business system risk (not vulnerability counts) to stakeholders.

ABOUT BRITEPROTECT

BriteProtect is an advanced managed security service that solves the problem of tedious alert management leading to missed critical alerts and employee fatigue. We leverage decades of cybersecurity experience to provide our customers with unprecedented visibility, swift response and expert insights delivered via people, process and technology. Now, organizations can leverage existing security tools by partnering with Brite's team utilizing new, next-generation technology to elevate its security posture and better utilize internal resources.