Balbix®

Top 6 Vulnerability Management Mistakes to Avoid

Use this handy guide to evaluate your vulnerability management program and see if it is keeping up with the times.

Top 6 Vulnerability Management Mistakes to Avoid

Your vulnerability management program is the cornerstone of your cybersecurity initiative because you know that those CVEs, if left unidentified and unaddressed, can bring your business down. But as your enterprise advances with new innovation in technology and growing employee numbers, your vulnerability management needs to evolve as well to continue to protect your enterprise against diverse threats.

To ensure that your vulnerability management initiative is not lagging behind, it is imperative to evaluate it from time-to-time. Are you committing these 6 common vulnerability management blunders?

1

Mistake #1

Not monitoring continuously and in real-time

You have a huge number of assets including traditional IT and dynamic modern assets across all computing environments, and each asset can be breached in a variety of different ways. If you are not monitoring and analyzing your attack surface continuously and in real-time, you are setting yourself up for blind spots and delayed reaction time.

Fix It!

Continuous, real-time monitoring and analysis of your entire attack surface gives you the ability to quickly identify potential breach risk and proactively fix security vulnerabilities. Consider investing in a risk-based vulnerability management system that offers continuous, real-time monitoring, instead of intermittently network scans.

Ask yourself: “Are new devices discovered within minutes of plugging into our environment and monitored continuously thereafter?”

Mistake # 2

Thinking vulnerabilities = CVEs

Vulnerability management scanners were designed to look for unpatched software flaws or CVEs (publicly known common vulnerabilities and exposures in publicly released software packages). However, if you consider the dictionary definition of a vulnerability, it is anything that exposes you and puts you at risk. So, bad password hygiene – using weak or default passwords, reusing passwords, and not storing passwords correctly – is also a vulnerability. And so are misconfigurations, encryption issues, and risky online behavior of employees.

Is your vulnerability management tool looking for vulnerabilities or flaws across other attack vectors also?

Fix It!

Vulnerabilities are not just CVEs. Any breach methods that put your enterprise at risk are dangerous. Invest in a risk-based vulnerability management system that goes beyond just monitoring unpatched software and covers a broad range of other attack vectors and vulnerabilities as well.

Ask yourself: "Do we know our risk from weak or shared passwords, malware, phishing, encryption issues, online behavior of our admins and more?"

Mistake # 3

Not inventorying all your assets

The traditional “scan-the-network” approach was aimed at enterprises with mostly static, on-premises systems like network infrastructure, servers, managed PCs, etc. This does not work for the modern, multi-dimensional attack surface that hosts different types of assets including traditional IT (network infrastructure, servers, desktops) and dynamic modern assets (cloud instances, SaaS apps, mobile, BYO, operational technology (OT), and IoT devices).

Fix It!

Broad asset coverage is a core capability that is required to discover all potential vulnerabilities. If your vulnerability management system only “sees” a few types of assets, your coverage is insufficient. Consider a risk-based vulnerability management system that identifies all types of assets, including BYOD, and empower yourself to managing your risk across the entire attack surface.

Ask yourself: “Can we see all types of assets and devices – including unmanaged BYOD, IoT, etc. – that are on our network at any time?”

Mistake # 4

Not having *searchable* inventory of your IT assets

Having an automated, real-time, and accurate inventory of all your assets is a first – and critical – step, but if you are not able to search it and easily find what you need, that inventory is practically useless. You need to be able to craft complex queries like “iOS devices in Mountain View susceptible to Spectre” or “unpatched DNS servers in Texas” and get the answers quickly. Does your vulnerability management support that?

Fix It!

Invest in a vulnerability management solution that offers the ability to perform natural language search and easily find answers to questions like “how many IoT devices do I have” or “where will the attack start” or “what is my risk from Poodle”. Being able to quickly find the needle(s) in the haystack is a huge advantage.

Ask yourself: “If asked, how quickly and easily can we produce a list of all our assets susceptible to Wannacry? Can we even do it?”

“When Wannacry hit, it took my team of 3 people 48 hours to get a list of all assets that were susceptible to it. I would give anything to not go through that pain again!”

Mistake # 5
Not prioritizing based on risk

The decision about what to fix and when to fix it has to be based on more than just a roll of the dice or generic vulnerability severity ratings. Risk-based prioritization must reflect numerous factors such as vulnerabilities across 100+ attack vectors, business value of the asset, active threats, exposure due to usage, and existing compensating controls. If your vulnerability management system is not taking account all of these factors, the "prioritization" it may offer is of little to no value.

Fix It!

Moving from a vulnerability-focused mindset to a risk-based prioritization approach requires a vulnerability management platform that understands and learns your business context, considers the value of each asset to your business and takes into account vulnerabilities, active threats, exposure due to software usage and any mitigating controls already implemented in your enterprise to calculated risk. This risk-based prioritization helps you first focus on actions that are critical, and make smarter decisions to reduce your risk, both strategically and tactically.

Ask yourself: "Is my vulnerability management system ***really*** prioritizing vulnerabilities for me or is it just ***pseudo*** or incomplete prioritization?"

Mistake # 6
Not having the right tools

With the number of cybersecurity threats growing every day and increased digitization of assets/processes that could be vulnerable to those threats, it is mathematically impossible for humans to analyze the full attack surface. Not to mention continually monitor for threats and determine the right actions to most reduce breach risk. You need artificial intelligence (AI) to enable that scale of effort. Legacy tools designed to protect traditional IT assets such as servers and network infrastructure aren't designed to see, analyze and mitigate the modern attack surface and digital landscape.

Fix It!

An AI-powered platform that continuously monitors the full attack surface and proactively predicts what vulnerabilities are most likely to be exploited is necessary just to keep up with the constantly evolving attack methods employed by cyber criminals, as well as the ongoing digital transformation of enterprises.

Ask yourself: "Does my vulnerability management system make it easy for me to see my security gaps across all assets and attack vectors? Does it prescribe the necessary tactical and strategic mitigations to address them and minimize risk?"

Risk-Based Vulnerability Management with **Balbix BreachControl™**

Balbix BreachControl uses deep learning and advanced AI algorithms to enable you to:

Understand your attack surface

Balbix continuously observes your extended enterprise network inside-out and outside-in, to discover the attack surface and analyze the hundreds of millions (or more) of data points that impact your risk. It monitors all your enterprise assets across 100+ attack vectors (such as such as phishing, credential exposure, weak/shared passwords, and malicious behavior and not just unpatched software vulnerabilities) continuously and in real-time.

Get an accurate read on your risk

Balbix calculates your enterprise's real-time risk, taking into account open vulnerabilities, business criticality, applicable threats and the impact of compensating controls. Analysis of all possible breach scenarios – the various combinations of attack starting points, target systems and propagation paths – and precise determination of the riskiest scenarios is key. This real-time risk model is surfaced to relevant stakeholders in the form of highly visual drill-down risk heatmaps and Google-like natural-language search. You can ask questions like "where will attacks start" or "what is the risk to customer data", get a relevant, highly visual answer within milliseconds, and then drill-down into the details.

Create a prioritized actions list with prescriptive fixes

Balbix generates a prioritized list of actions that will tangibly reduce risk. Security posture issues with the greatest risk are addressed first before working down the list of smaller contributors. For each issue, responsible owners for the corresponding assets are identified and then prioritized tickets containing all relevant context are generated and assigned to these owners. Progress is closely tracked and fed back to relevant stakeholders.