Nanitor
Global CTEM leader

DEREK MELBER

Exposure Management

"By 2026, organizations that prioritize their security investments based on a continuous exposure management program will be 3x less likely to suffer a breach."
Gartner

Table of contents:

Exposure Management

Attacks and breaches are nearly an everyday occurrence. Many organizations are relying on antiquated vulnerability management solutions, which are just not robust enough to thwart attacks.

Gartner has slated Continuous Threat Exposure Management (CTEM) as the #2 trending technology for 2024. (https://www.sourcefuse.com/resources/blog/gartners-top-10-strategic-technology-trends-of-2024/)

Gartner has also stated that organizations that adopt CTEM will see a 2/3 reduction in breaches by the year 2026. (Gartner Identifies the Top Cybersecurity Trends for 2023).

CTEM is the hottest technology for any sized organization. Here, we will go into the various aspects of security hygiene and CTEM, giving you a clear view as to why you should adopt a solid and unified CTEM solution for your organization.

Is Vulnerability Management Enough to Prevent Ransomware?

Ransomware has proven to be the number one issue for organizations of all sizes and verticals in the past few years. Nearly all of the organizations that have been breached and ransomed had a vulnerability management solution or process in place. So, it begs the question whether vulnerability management alone is enough?

The Vulnerability Management Play

I think vulnerability management is a common and known solution. It is geared to find and prioritize all operating systems, applications, services, devices, etc. vulnerabilities. Nearly every electronic and systematic platform has vulnerabilities. From basic Windows OS to even the most sophisticated nuclear power plant system. Why? Well, these systems are running some program, which was designed, built, and tested by a human. Humans make mistakes and can't fully understand where there might be a vulnerability that can be exploited by an attacker.

Where Vulnerability Management Comes Up Short

There are many areas where vulnerability management solutions have let organizations down.

1. Everything can't be "critical"! – When organizations are given a voluminous list of vulnerabilities that need to be remediated, it be daunting to the point that nothing is fixed.
2. You can't fix everything! – The amount of effort, time, and dedication to fix every possible vulnerability is just too much. There is no way, in a normal business environment, that every vulnerability can be patched. It is just not possible.
3. Vulnerability management is just one piece! – Many organizations have been sold or convinced that vulnerability management is the most important security effort that can be performed to prevent breaches. That is just not true!

What Other Security Needs to be Considered?

We have learned a lot over the past few years of attacks and breaches regarding what attackers leverage to enter and move through an organization. It is this real-world experience and analysis that shows us exactly what we need to consider to truly secure an enterprise. In addition to vulnerability management, the following areas should be considered at the same level:

1. Misconfigurations – of everything! Operating systems, databases, network devices, communication platforms, remote connectivity platforms, etc.
2. Patching – Yes, patching is still a "thing" and still not given the effort it needs. Attackers look for unpatched systems to exploit well-known tactics against them
3. Identity – Gartner states that identity is one of the top 3 areas that attackers exploit to breach a network. From authentication attacks to complete credential impersonation, identities must be secured.
4. Network segmentation – Microsoft claimed years ago to "assume breach". If this is the case, then separating out networks from one another will help with the lateral movement between different networks.
5. External facing devices and networks – Attack surface management from the outside world into your network is real and common. Ensuring that your domains and devices that can be seen from the outside world are secured is essential in your overall quest to secure the network.

For MSSPs, Gartner clearly states that exposure management is a differentiator. (Emerging Tech: Threat Exposure Management as MSSP Differentiator (https://www.gartner.com/en/documents/5261163 (gartner.com))

Exposure Management: You can't secure what you don't know about!

It is not a new concept that IT is not fully aware of all the assets and devices that are on the network. Projects come and go, rogue devices are put on the network, legacy assets are forgotten about, etc. The other concept that is not new is that attackers love these assets and devices that have been orphaned and forgotten. These assets and devices are not updated, patched, configured, secured, or monitored.

Imagine you are building a new house, and a special side door is created to allow the crew in and out without mucking up the fancy wood flooring. When the house is finished, the side door is not removed and closes. It is forgotten! Tell me an intruder wouldn't target this door if they were trying to enter the house!

Asset and device discovery

Often the IT staff relies on documentation to track assets and devices. This is a poor process, as documentation is easily passed over for the "fires" that the IT staff must deal with daily. This means that documentation is outdated. New devices are not added, older devices are not removed.

Most organizations don't rely on a solution that will find their assets and devices. They might do periodic ping sweeps or manual inspections, but with virtual machines, small devices, IoT, and other easily hidden assets and devices, these measures are just not enough.

Automatic Asset and Device Discovery and Inventory

Ideally, organizations of all sizes need to have security solutions that automatically update the asset and device inventory to track everything that is connected to the network. This will ensure that IT is aware of every possible "entry point" into the network.

There are options like using ARP and routing tables, which will help uncover devices that might come-and-go from the network, but their communications are left behind on other static devices. ARP and routing tables can uncover "friends of friends" to give a blanketing effect on asset and device discovery.

"Nanitor was able to discover assets and devices that we never knew were on the network, which were brought into the organization from employees."

Another great option for automatic asset and device discovery is to use Active Directory, as you can see in Figure 1. When devices join Active Directory, they have a computer account that represents the device. Getting a full list of the computer accounts from Active Directory can uncover unknown or forgotten devices with ease.

"Nanitor uncovered over 100 computers that we thought were no longer on the network."

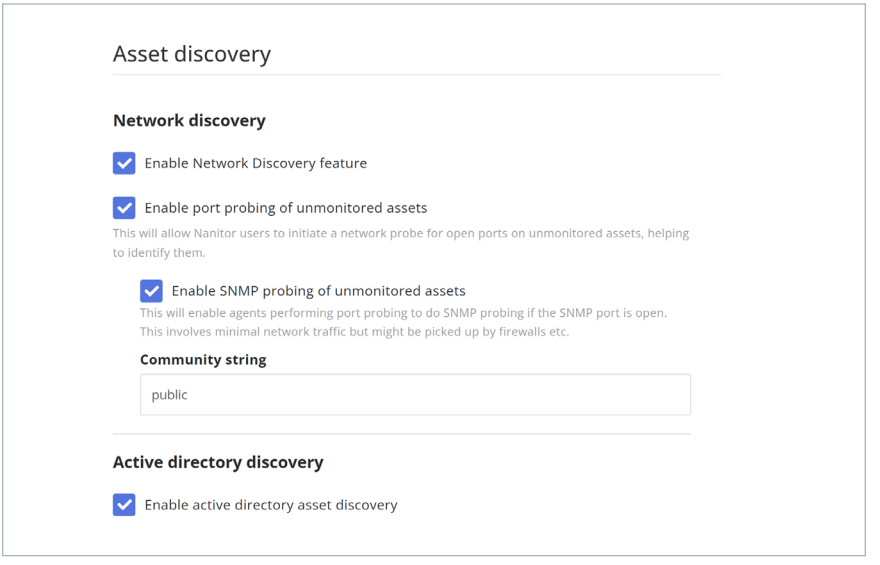


Figure 1. Automatic asset and device discovery using Active Directory.

Asset and device Prioritization and Labeling

Once an asset is found, it is essential to automatically label that asset. The labeling of an asset provides for easier prioritization, grouping, report filtering, and organizing of overall security prioritization.

Labels would include “Windows”, “Domain Controller”, “Printer”, “Cloud”, etc. By assigning a label when the asset is found, the system can then automatically know what to gather from the asset, know what analysis needs to be performed, and finally triage the security issues within the other asset security issues for a master prioritized list of issues.

Not prioritizing assets is a very bad decision and design for exposure management. Every asset must have a priority, so the IT and security staff know exactly what to remediate to give the best risk reduction from their efforts. Not every security issue can be resolved, so having as many analytical points to incorporate into the overall decision on what issues need to

be fixed on which assets can mean the difference from being breached or denied an attack.

Vulnerability Prioritization and Exploitation

At the core of most vulnerability management solutions is the concept of "prioritization". Prioritization is essential in triaging vulnerabilities since there are very few known vulnerabilities that have been exploited. According to NIST (from 1/1/1999-2/10/2024):

- Total vulnerabilities with CVSS > 9.0: 40,456
- Total vulnerabilities with CVSS between 7.0 and 9.0: 79,140
- Total known exploited vulnerabilities: 1085

This makes the % of high and critical vulnerabilities that have been exploited less than 1%. NIST has also reduced the value of KEV to just around 20, which has been proven to be in most enterprises (1).

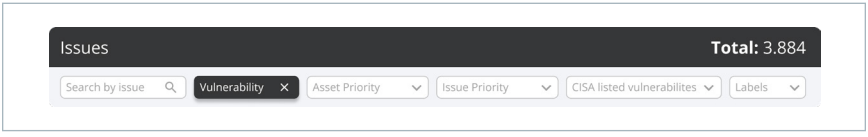
What does this mean for most organizations? Most vulnerabilities do not need to be addressed.

Combining Asset Priority with Vulnerability Priority

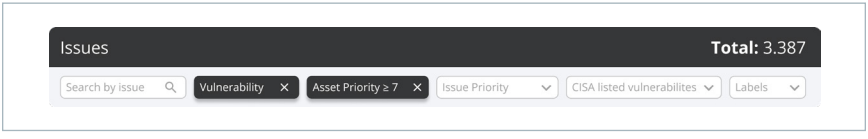
A key concept that most organizations can benefit from is the combination of asset and vulnerability priorities. With so many vulnerabilities to overcome, it would be ideal to know when high-value assets have the highest priority vulnerability.

A solution that can give you a list of the highest priority exploited vulnerabilities on the highest value assets can save time and have the biggest impact in reducing risk due to vulnerabilities. Look at this example:

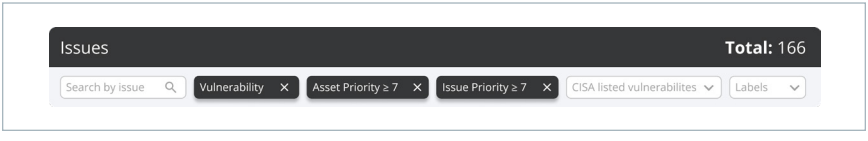
Here is a list of all vulnerabilities in this test environment (3884):



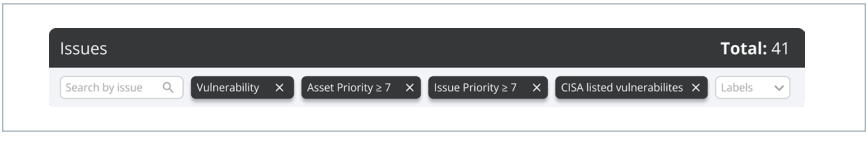
Now, looking at the assets that have a prioritization of at least 7, the vulnerabilities reduce (3387):



Next, focusing on the vulnerabilities that are between 7.0 and 10.0 (166):



Finally, looking at only the vulnerabilities that meet our criteria and are on the KEV (41):



Using this method, we reduced the total number of vulnerabilities from 3884 down to only 41 that are exploited and located on high-value assets! That is very manageable for any organization.

Configuration Monitoring

Organizations from as small as 10 users to large enterprises with 100,000 users all have the same concern when it comes to security configuration drift. There is just not enough time to monitor all changes and to know if the change results in a security gap or not.

This is why there are solutions that monitor security configuration changes specifically. Not only can a solid security configuration change monitoring solution check for changes, but the changes can be compared to “baselines” to ensure that the change is not negative. These baselines already exist in the form of CIS Benchmarks. Yes, CIS has already documented over 100 different platform security best practices and made them available for you to use.

This is what Nanitor does for you! Nanitor will gather all the security configurations from all your assets, then automatically compare the settings to the benchmarks to ensure the best security is in place. If there are any security configuration issues, Nanitor will report them back to you so you are aware of the security concerns, as you can see in Figure 1.

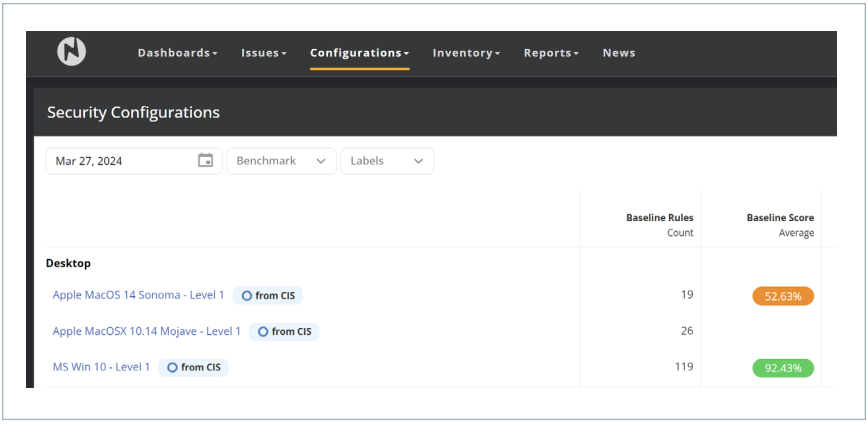


Figure 1. Nanitor shows where assets are not meeting the CIS Benchmarks.

Combining Asset and Misconfiguration Priorities

Attackers look for specific computers on the network to query and attack. They prefer high value assets like domain controllers, application servers, databases, etc. This is why it is essential to be able to establish asset priorities, so the high value assets are looked at closer than the lower value assets. Combine the asset priority with the security configuration priorities and you have a clear view as to which configurations you need to address on each asset... with a prioritized list, as you see in Figure 2.

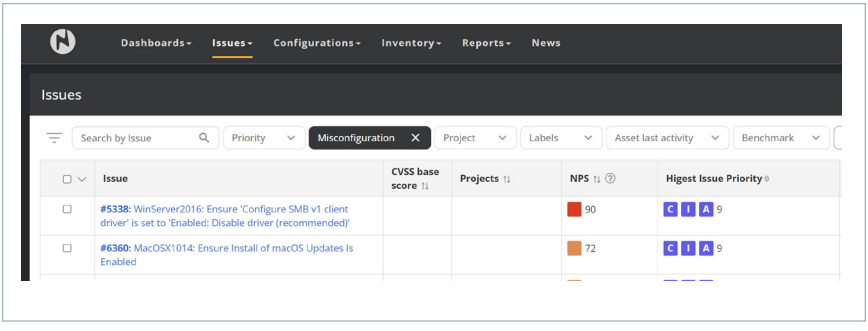


Figure 2. Asset and misconfiguration priorities give an efficient list of what needs to be addressed.

Most organizations can't remediate every security configuration, due to the massive volume of assets and configurations possible. However, with a combination prioritized list, organizations can go after the settings that will give them the best overall security in an efficient manner.

Identity Security

It is often thought that identities can be secured and protected by using layered solutions like PAM, MFA, etc. This is just not the case, as the identity itself needs to be secured. In every identity store (on-prem Active Directory, Entra ID (AKA Azure AD), AWS, Google Cloud, Okta, etc.) the identity has

configurations that grant it abilities beyond just a standard user. In many cases these configurations can be attacked, providing the attacker with immediate information that can be used to impersonate or leverage the account in other ways.

For on-prem Active Directory, the list of identity properties and attributes is very well known. Thus, it is a simple process to verify if any identities have exploitable configurations and then flag them for remediation. The problem is that these queries are not well known, nor is the ability to analyze the output from them.

In addition to identity security for configurations, there is another significant concern for identities in every organization. When an administrative user account that is designed to administer domain controllers logs onto a workstation, this breaks the "tiering model" which is geared to protect the identity and its credentials. Being able to track when a user from a lower tier (tier 0 or 1) logs into a machine in a higher tier (tier 1 or 2) is vital in knowing when there is a potential for credential theft.

Combining and Normalizing Asset, Identity, and Issue Priorities

There is a significant gap in every organization when it comes to protecting identities, assets, and knowing which settings need immediate attention. When looking at a single security issue, such as vulnerabilities, it is rather easy to know which vulnerability to remediate first, based on that vulnerability's priority.

However, when identity security issues are combined with vulnerabilities, patching, misconfigurations, cloud security, and identity priority, it can be an extremely complex analytical problem to know what needs to be remediated first, to reduce the attack surface the most.

A solution like Nanitor can do this with ease, due to the fact it is built on a common codebase. Every security issue has a priority, which is normalized against the other issues. So, identity security is just one of many security issues, so a single prioritized list of security issues can be analyzed and generated so the organization knows exactly which issue needs to be done first, second, etc, as you can see in this figure.

Patch Prioritization

Patching is a necessary task that can bring the entire IT department to a halt. There can be such a volume of patches to cover all platforms, devices, and hardware. Patching can be automated, but in most cases the patch can have such negative effects, it is best to keep things either in small, automated bunches, or even use manual patching techniques.

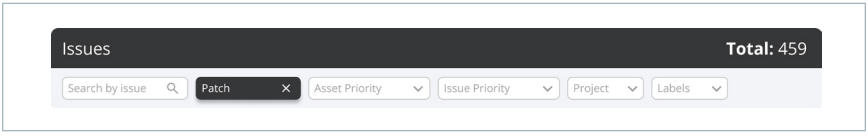
This is why patch priority is so important, so that the most critical patches can be addressed first, followed by patching that might only be for internal requirements.

Combining Asset Priority with Patch Priority

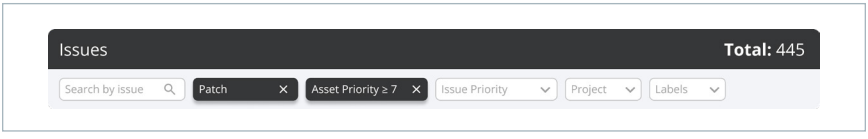
Combining asset and patch priority can make a radical difference in how long it will take to get all assets and the environment from a risky state to a more manageable secured environment.

A solution that can give you a list of the highest priority patches on the highest value assets can save time and have the biggest impact in reducing risk due to required patches. Look at this example:

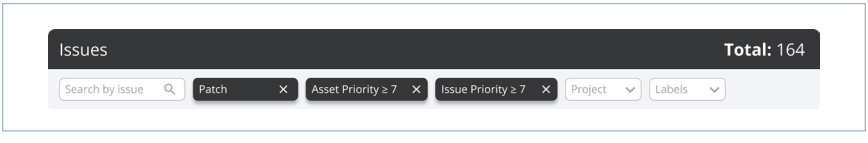
Here is a list of all patches in this test environment (459):



Now, looking at the assets that have a prioritization of at least 7, the patches reduce (445):



Finally, focusing on the patches that are between 7.0 and 10.0 (164):



Using this method, we reduced the total number of patches from 459 down to 164, which will take dramatically less time to deploy.

Leveraging Industry Standards for Security Hygiene

Often, I see security solutions that are just "guessing" at what needs to be secured. Sure, there is knowledge, experience, and expertise behind the solution. However, when industry standards can be incorporated, it proves that the security solution is considering the massive expertise and analysis that has gone behind the security standardization and recommendations.

At the core of a good Continuous Threat Exposure Management (CTEM) platform should be industry standards. Why? Mainly because it makes the most sense! Secondly, many compliance regulations require these industry standards and even frameworks are built on these industry standards.

Industry Standards for Each CTEM Component

With Gartner giving CTEM such emphasis in their "Gartner Top 10 Strategic Technology Trends for 2024" report, this is where many organizations should be spending their time to truly secure their environment. What Gartner does not clearly define is where the security analysis foundation should come from. That is where this blog comes in handy!

- Vulnerability management – NIST has a feed for obtaining the latest and greatest vulnerabilities daily.

- Misconfigurations – CIS benchmarks are the ideal place to get industry proven and standards for all platform security settings and recommendations.

- Patches – Microsoft, Apple, Cisco, etc. all have their own feeds for the latest info on patching their devices and systems.

- Identity – Well, here is where there is no dedicated feed or list of what needs to be secured per identity platform. The good thing is that Microsoft, AWS, Google Cloud, and others do have suggested security for identities.

About Nanitor

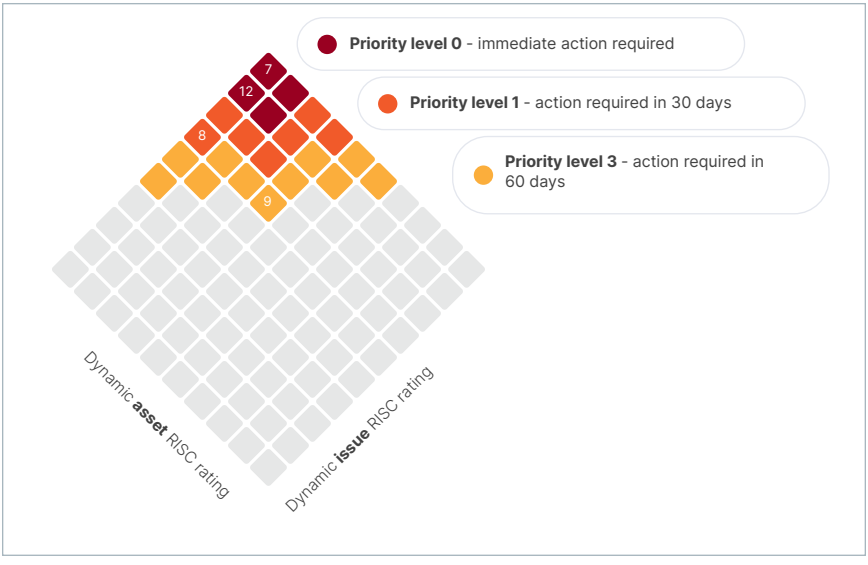
Founded by a team of cybersecurity experts passionate about technology's potential to improve lives, Nanitor has grown into a leading force in the cybersecurity landscape. Our journey began with a simple question: How can we make the digital world safer for businesses of all sizes? The answer lay in developing a solution that not only addresses current threats but also anticipates future vulnerabilities. Thus, the Nanitor continuous threat exposure management (CTEM) platform was born, embodying our commitment to innovation, excellence, and customer-centricity.

The Nanitor Difference: Our CTEM Platform

Nanitor's CTEM platform is not just a product; it's a paradigm shift in cybersecurity management. It offers an integrated, 360-degree view of an organization's cyber health, combining sophisticated scanning technologies with actionable intelligence. This enables real-time detection, assessment, and prioritization of threats.

The Nanitor Prioritization Diamond

Central to our approach is the Nanitor Prioritization Diamond, a unique framework that revolutionizes how threats are assessed and prioritized. This model considers various dimensions of risk to ensure that resources are allocated efficiently, focusing efforts where they are needed most. By balancing the severity of vulnerabilities with their potential impact, we help businesses optimize their security strategies for maximum effectiveness.

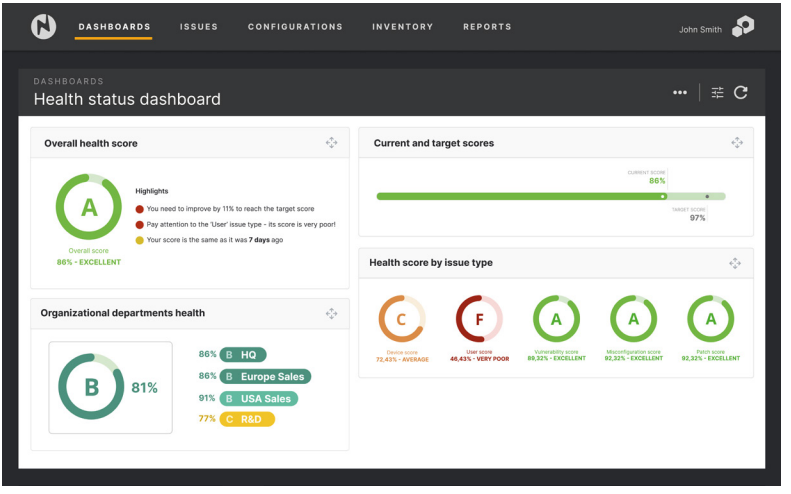


The Nanitor Diamond

The Nanitor Health Score

Understanding your cybersecurity health is paramount. That's why our CTEM platform features an intuitive health score metric—a clear, quantifiable measure of your security stance. This dynamic score provides at-a-glance insight into your organization's resilience against threats, facilitating informed decision-making and continuous improvement.

At Nanitor, we believe in a proactive approach to cybersecurity. Our suite of tools, highlighted by the Nanitor CTEM platform, the Prioritization Diamond, and the Health Score, empowers organizations to not only respond to threats but to anticipate them, ensuring a safer digital future.
dimensions of risk to ensure that resources are allocated efficiently, focusing efforts where they are needed most. By balancing the severity of vulnerabilities with their potential impact, we help businesses optimize their security strategies for maximum effectiveness.



Health status dashboard

The Nanitor Continuous Threat Exposure Management (CTEM) Platform

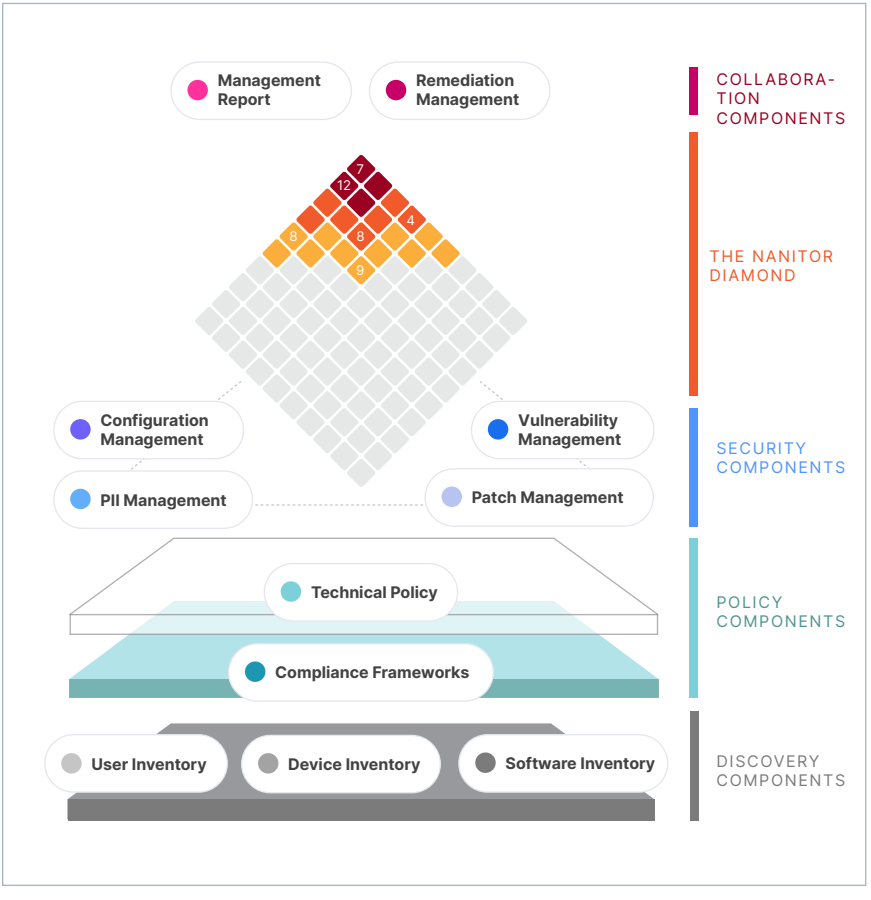
Nanitor's Continuous Threat Exposure Management (CTEM) platform builds a collective understanding of security challenges and quantifies cyber risk in real-time.

It forms a solid foundation for long-term security strategy, aligned with policy and compliance. Prevent information loss, service disruptions, and reputational damage from the evolving cyber threat landscape.

Nanitor's discovery engine collects real-time data on all assets, filtered through policy and compliance frameworks. Get detailed insights on a wide range of security issues through the prioritized Nanitor diamond. Collaborate effortlessly, strengthen organization-wide security, and track progress with

printable reports and managed projects.

Our market-leading system automatically prioritizes all known security issues across your entire infrastructure in order of criticality through our Diamond Vision. This empowers your team to simply and effectively focus remediation efforts on the biggest cyber threats in real-time.



The Nanitor Continuous Threat Exposure Management (CTEM) Platform

DEREK MELBER

19X MICROSOFT MVP

Derek is the Chief Strategist at Nanitor, where he helps drive the marketing, product, and sales to deliver the best Continuous Threat Exposure Management (CTEM) platform on the market. Derek has built a career out of public speaking, content creation, sales, marketing, and enterprise design around a core set of technologies like identity security, Active Directory/Azure Active Directory, cloud identity, PAM, CIEM, MFA, SSO, Group Policy, and other integrated technologies.

Derek has authored over 15 books, including The Group Policy Resource Kit and Auditing Windows Active Directory. Derek is a master at oral and written content, as well as mastering the art of communicating to audiences of all sizes to intertwine his knowledge, communication skills, and enterprise design understanding. You can reach Derek at **derekm@nanitor.com** and **@derekmelber** on LinkedIn.