THE CYBER EXPOSURE SCORE: HOW SECURE IS THE BUSINESS?

CYBER EXPOSURE SCORE

247
Executive Summary

Tenable Lumin enables organizations to effectively measure and benchmark their cyber exposure, providing comparisons both internally (e.g., business groups, geographies, asset classes) and externally against peer organizations.

The Cyber Exposure Score, a critical component of Tenable Lumin, is an objective rating of cyber risk derived through data science–based measurement. The score is automatically generated daily through machine-learning algorithms that combine vulnerability data with other risk indicators such as threat intelligence and asset criticality. Today, the score is calculated by combining the Tenable Vulnerability Priority Rating (VPR), for the likelihood of exploitability, with the Tenable Asset Criticality Rating (ACR), for the business criticality of the affected asset.

The Cyber Exposure Score can be applied to a single asset, a group of assets or an entire organization.

This whitepaper will:

- Demonstrate how the Cyber Exposure Score can help you improve your security posture over time
- Provide a technical walkthrough of the Cyber Exposure Score – including details about the data science behind the rating
- Highlight popular use cases that show how the Cyber Exposure Score can drive efficiency in your daily security practice

“By 2022 cybersecurity ratings will become as important as credit ratings when assessing the risk of existing and new business relationships.”

– Gartner

1 Innovation Insight for Security Rating Services, Gartner, July 2018
Turning a Technical Topic into a Business Conversation – with the Cyber Exposure Score

The Cyber Exposure Score is a new means to drive strategic decision-making about cybersecurity investment and risk management, providing clarity into these key questions:

- What is the overall organizational risk?
- Are we reducing our exposure over time? How can I frame risk and remediation performance in business terms?
- How do different business units, processes and geographies compare from an overall program effectiveness and exposure perspective?
- Is the business making the right levels of investment to effectively identify and address exposures?

“Lumin allows us to get a better view of how we compare against our peers and allows us to focus on true risk in our environments. With data constantly flowing in from many sources, [Tenable] Lumin gives us a clear picture of where we began, where we are today, and what to focus on tomorrow.”

– Evan London, Senior Consultant, IT Security at Virtustream - A subsidiary of Dell Technologies

CYBER EXPOSURE BENCHMARKING

Use the Cyber Exposure Score to benchmark your organization against industry peers and measure your overall cyber risk posture.

Tenable has the industry’s most extensive vulnerability intelligence, processing over 1.5 billion instances of vulnerabilities per week, which is coupled with data science to create its benchmarking knowledge base.

You can also drill-down to benchmark internal groups against each other by business unit, asset type or geography, for example.
Digging into the Cyber Exposure Score – Data Science Has the Answers

Falling between 0 (minimal risk) and 1000 (highest risk), the Cyber Exposure Score is the average of all the Asset Exposure Scores (AESs) in an organization (see Figure 1). This single score represents an organization’s overall cyber risk.

**Asset Exposure Score Calculation Process**

1. **Vulnerability Priority (VPR)**
   - Threat Probability • Impact Score

2. **Asset Criticality (ACR)**
   - Exposure • Device • Capabilities

3. **Asset Exposure Score (AES)**

**Cyber Exposure Score Calculation Process**

- Average of all Asset Exposure Scores (AESs)
- Cyber Exposure Score

**Figure 1. Scoring Calculation Processes**

**Cyber Exposure Scores and Asset Exposure Scores:**
5 Things to Know

1. The Cyber Exposure Score is the average of all Asset Exposure Scores.
2. Scores are calculated every 24 hours.
3. Scores will change over time.
4. Use the scores to prioritize vulnerability remediation.
5. Use the scores to help non-technical stakeholders understand the business implications of cyber risk.
Surveying the Elements and Processes

Derived through data science–based measurement of vulnerability data, threat intelligence and asset criticality, the Cyber Exposure Score is automatically generated every day. Data science algorithms combine **Tenable Vulnerability Priority Rating (VPR)**, which predicts the likelihood of exploitability, with **Tenable Asset Criticality Rating (ACR)**, which infers the business impact if the asset is successfully attacked.

Vulnerability Priority Rating (VPR)

Derived via a machine-learning algorithm, the VPR is the output of **a process called Predictive Prioritization**, which is incorporated into both **Tenable.io** and **Tenable.sc**.

VPR is a number that indicates the remediation priority (0–10, with 10 being the highest severity) of a single vulnerability. For example, a vulnerability currently being exploited in the wild would have a significantly higher VPR than a vulnerability where no working exploit has been observed.

VPR is a dynamic number that changes with the evolving threat landscape. It enables organizations to focus on remediating the vulnerabilities with the highest likelihood of being leveraged in a cyberattack.

For more information about VPR and Predictive Prioritization, read the technical whitepaper, **Predictive Prioritization: Data Science Lets You Focus on the 3% of Vulnerabilities Likely to Be Exploited**.

An AES quantifies the asset’s vulnerability landscape. It’s calculated using the asset’s vulnerability threat, criticality and scanning behavior information. Two component models are used to calculate the AES (see Figure 2):

- **Vulnerability Priority Rating (VPR)**
- **Asset Criticality Rating (ACR)**

VPR: 3 THINGS TO KNOW

1. The scores can change over time.
2. Scores are derived from machine-learning algorithms and are automatically calculated every 24 hours.
3. Use the scores to prioritize vulnerability remediation – and reduce the number of vulnerabilities requiring immediate remediation by 97%.
**Asset Criticality Rating (ACR)**

The Asset Criticality Rating (ACR) is a dynamic rating that represents the criticality of an asset on a network. Unlike VPR, which is an absolute value produced by the Predictive Prioritization process, the ACR is a subjective measurement, modifiable by the user.

ACR automates asset criticality assessment by using data from scan results and applying a rules-based approach that relies on three key pillars (see Figure 3): internet exposure, device type and device functionality.

1. **INTERNET EXPOSURE**
   - **Is the asset internet-facing or internal?**
     - **EXTERNAL**
       - Target of Cloud Scanner
       - Routable IP
     - **INTERNAL**
       - Non-routable IP
       - Same Subnet as an Internal Scanner
       - DMZ

2. **DEVICE TYPE**
   - **What type of device is the asset?**
     - **GENERAL COMPUTER**
       - Workstation
       - General Server
     - **COMPUTER APPLIANCE**
       - Networking Device
       - Networking Security
       - IoT Device
       - Data/Computing Center

3. **DEVICE FUNCTIONALITY**
   - **What is the asset’s purpose based on its capabilities?**
     - **BUSINESS PURPOSE**
       - Finance/Accounting
       - Industrial Control and Monitor
       - IT Management
       - R&D
     - **SOFTWARE SERVICE**
       - Database Server
       - Application Server
       - File Server
       - Mail Server
     - **DEPLOYMENT**
       - Production
       - Stage
       - Development

*Figure 3. ACR Feature Groups*
These three factors are then combined using various rules to assign an ACR (see Figure 4).

ACR Calculation Process

EXPOSURE + DEVICE TYPE + CAPABILITIES → ASSET CRITICALITY RATING (ACR)

Each pillar consists of rules for attribute detection and criticality scoring. One key criterion for determining criticality is the scale of business impact if the asset were to be compromised. When a critical asset is compromised, it can majorly impact an organization’s confidentiality, integrity and/or availability.

ACRs range from 0 to 10:

- A low ACR means the asset is not deemed to be business-critical.
- A high ACR means the asset is extremely business-critical.

A lower-criticality asset usually has less impact under threat. For example, IT management, proxy servers and mail servers tend to have high criticality. Meanwhile, IP telephones and printers typically have medium or low criticality.

PRO TIP

Use authenticated scans to improve ACR quality. Authenticated scans provide higher attribute confidence and variety.
**Algorithm**
Here's an overview of the ACR algorithm:

**Step 1**
Extract ACR attributes from scans.

**Step 2**
Aggregate ACR attributes per assets.

**Step 3**
Calculate the ACR per asset via:
- An expert system maps criticality to ACR attributes.
- Mapped ACR attributes are aggregated to produce an ACR per asset.

**Figure 5. ACR Algorithm**

**REMEDIATION GUIDANCE WORKFLOW**

Within Tenable Lumin, security teams receive a list of the top recommended remediation actions to reduce the organization's Cyber Exposure Score.

For additional information, you can drill-down into specific vulnerabilities or assets for business and technical context to enable more effective remediation.
ACR in Action

BEFORE ACR:
Network’s asset criticality coverage is LOW

Security analyst runs host discovery scan and finds 16 unique assets on the network.

3 of the assets are known and have criticality attributed via CMDB/manual tagging.

There are 13 assets with unknown criticality (represented by ?s).

AFTER ACR:
Network’s asset criticality coverage is HIGH

Security analyst scans same network with credentialed advanced network scan (skipping asset #3, which is on an exclusion list, so scans never include it and asset features can’t be collected).

ACR complements analyst’s prior work (asset #1, 2) and helps fill in the unknowns.

Before 13 assets had unknown criticality.
Now, only 2 assets have unknown criticality.

Notes:
• Although ACRs are automatically generated, you can override this value to align with the actual criticality of the asset to your organization.
• ACR isn’t perfect; it didn’t calculate the criticality for assets #10 and #16 because they generated no known asset features.
# Bringing It All Together: Putting the Cyber Exposure Score to Work

Let’s take a look at a few use cases to help visualize how Tenable Lumin and the Cyber Exposure Score can be incorporated into your daily security practice.

## EXECUTIVE USE CASES

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Product Feature</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>I want to understand my overall security posture and quantify risk level across my organization.</td>
<td>Cyber Exposure Score</td>
<td>Cyber Exposure Score</td>
</tr>
<tr>
<td>I want to see how my risk level is trending over time.</td>
<td>Cyber Exposure Score Trend</td>
<td>Cyber Exposure Score</td>
</tr>
<tr>
<td>I want to measure my success benchmarked to peers.</td>
<td>External Benchmarking</td>
<td>Benchmarking against Industry and Population</td>
</tr>
<tr>
<td>I want to measure risk per business entity.</td>
<td>Internal Benchmarking (using Tags)</td>
<td>Benchmarking against Asset Tags</td>
</tr>
</tbody>
</table>

## DIRECTOR/MANAGER USE CASES

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Product Feature</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>I want to understand the security posture and quantify risk level across my area of responsibility (e.g., geography, BU, asset type).</td>
<td>Cyber Exposure Score</td>
<td>Cyber Exposure Score</td>
</tr>
<tr>
<td>I want to see how my risk level is trending over time for my area of responsibility.</td>
<td>Cyber Exposure Score Trend</td>
<td>Cyber Exposure Score</td>
</tr>
<tr>
<td>I want to measure my success benchmarked to other parts of the organization.</td>
<td>Internal Benchmarking</td>
<td>Benchmarking against internal groups</td>
</tr>
<tr>
<td>I want to measure risk per my area of responsibility.</td>
<td>Internal Benchmarking (using Tags)</td>
<td>Benchmarking against Asset Tags</td>
</tr>
<tr>
<td>I want to know the top actions to take to reduce my risk.</td>
<td>Recommended Solutions</td>
<td>Recommended Solutions</td>
</tr>
<tr>
<td>ANALYST/TECHNICIAN USE CASES</td>
<td>PRODUCT FEATURE</td>
<td>METRICS</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>I want to understand the security posture and quantify risk level across my area of responsibility (e.g., geography, BU, asset type).</td>
<td>Cyber Exposure Score</td>
<td>Cyber Exposure Score</td>
</tr>
<tr>
<td>I want to measure progress against my SLAs.</td>
<td>Cyber Exposure Score Trend</td>
<td>Cyber Exposure Score</td>
</tr>
<tr>
<td>I want to measure my success benchmarked to other parts of the organization.</td>
<td>Internal Benchmarking</td>
<td>Benchmarking against internal groups</td>
</tr>
<tr>
<td>I want to measure the status of my assigned work.</td>
<td>Cyber Exposure Score Trend</td>
<td>Cyber Exposure Score</td>
</tr>
<tr>
<td>I want to know which vulnerabilities and vulnerable assets pose the biggest risk.</td>
<td>Cyber Exposure Score</td>
<td>Cyber Exposure Score</td>
</tr>
<tr>
<td>I want to know the top actions to take to minimize risk.</td>
<td>Recommended Solutions</td>
<td>Recommended Solutions</td>
</tr>
</tbody>
</table>

You can determine your Cyber Exposure Score by business context or asset groups using tags. This not only illuminates pockets of high risk, but it also allows you to benchmark cyber risk internally across different business units, geographic locations, computing environments and more.
What’s Your Cyber Exposure Score? Find Out Now.

Curious to see your Cyber Exposure Score? Learn more about Tenable Lumin now.