Risk scores

Published: 2024-09-04

Detections are assigned a numeric risk score that is associated with a severity level. Risk scores enable you to quickly triage detections by their potential risk to your network.

Here are some considerations about working with risk scores:

- Certain detections are eligible for dynamic risk scores, which are adjusted based on machine learning observations.
- Detections can be filtered or sorted by risk score on the Detections page.
- Notification rules can be created based on a minimum risk score criteria.
- Risk scores accompany detection markers for devices in activity maps and on device overview pages.

The following sections provide information about how the ExtraHop system calculates risk scores.

Risk factors

The ExtraHop system assigns each detection a risk score based on a combination of three factors that assess the threat identified in the detection: likelihood, complexity, and business impact. Each of these factors is given a level of low, medium, or high.

These factors are combined to derive a numeric risk score for each detection type. You can view the level of each factor on the detection detail page.

Likelihood

Likelihood measures the probability of an attack occurring. Attacks that require significant planning or resources, such as acquiring elevated privileges, are assigned a likelihood of low. Attacks that target large and exposed attack surfaces, or routinely exploited vulnerabilities, are assigned a likelihood of high. A high likelihood risk factor indicates a common and reliable threat, which results in a higher risk score.

Complexity

Complexity measures the skill level required to perform an attack. Attacks that require minimal skill, unsophisticated techniques, or that can be performed with publicly available tools are assigned a complexity of low. Attacks that require an experienced attacker, specialized tools, and advanced techniques are assigned a complexity of high. A high complexity risk factor indicates a sophisticated offender who is capable of achieving objectives stealthily, which results in a higher risk score.

Business impact

Business Impact measures the adverse effects an attack can have on business operations. Attacks that do not affect business operations, such as reconnaissance scans and enumerations, are assigned a business impact of low. Attacks that can result in the loss of significant data or systems, such as ransomware encryption, are assigned a business impact of high. A high business impact risk factor indicates an attack that can jeopardize business operations, which results in a higher risk score.

Although risk scores can provide the estimated severity of security risks, risk scores do not replace decision-making or expertise about your network. Always review security ⧉ detections to determine the root cause of unusual behavior and when to take action.

Risk score severity

Risk scores are grouped into one of the following color-coded severity levels:

Red (80-99)

Red risk scores are assigned to detections that pose a severe threat to your environment and should be researched immediately. For example, ransomware, data exfiltration, and vulnerability exploits that can significantly affect your business.

Orange (31-79)

Orange risk scores are assigned to threats or security issues that should be assessed to mitigate potential damage. For example, reconnaissance detections such as scans and enumerations, detections based on threat intelligence, or maintenance reminders about weak TLS cipher suites and expired TLS server certificates.
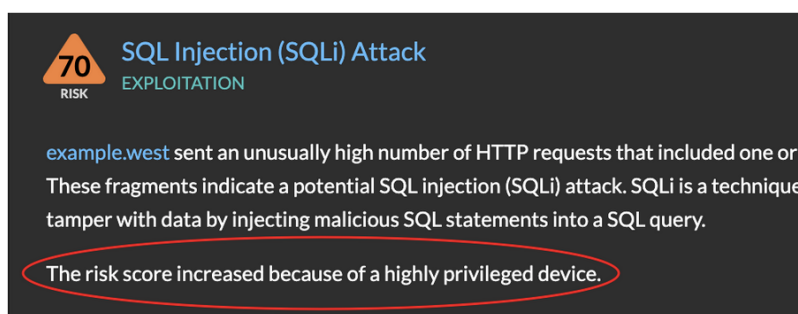
Yellow (1-30)

Yellow risk scores are assigned to detections that have an extremely low potential for impact on your network.

Dynamic risk scores

If a detection is eligible for a dynamic risk score, the Machine Learning Service can raise or lower the risk score to reflect the presence of specific participants or patterns in your environment.

When a risk score is adjusted, the detection card displays an explanation for the change:

The risk score can be adjusted for any of the following reasons.

High value devices

Risk scores are raised when one of the participants is a high value device. A device is determined to be high value if the ExtraHop system observes the device providing authentication or other essential

services. Users can also manually specify a device as high value ⤴, which can also affect the risk score.

Privilege level

Risk scores are raised when one of the participants has a high privilege level. Privilege is a measure of access that a user has to services and devices. For example, a high privilege level would be assigned to a device associated with an administrator account that accesses high value or remote devices over administrative protocols such as SSH. If an attacker compromises a device associated with a high privilege level, the potential impact on the network is higher.

Vulnerability scanners

Risk scores are lowered when one or more of the offenders is a vulnerability scanner.

Transfer size

Risk scores related to detections about data transfer, such as exfiltration or data staging, are raised or lowered when the relative volume of data is significantly different than other detections of the same type.