Risk Score Calculation Documentation

1 Overview

The risk score calculation is designed to assess security risks across multiple users within an organization or within specific departments. Each user is evaluated based on security threats and event severity levels. The calculation can be adjusted dynamically based on organizational needs and observed user behavior over time.

1.1 Risk Score Formula

The risk score for each user is computed as:

$$\text{Risk Score} = \sum(\text{Event Count} \times \text{Thread Weight} \times \text{Event Weight})$$

Where:

- **Event Count**: The number of security incidents recorded for a specific event across an organization/department.
- **Event Weight**: The impact level of an event based on severity classification (e.g., Critical, High, Medium, Low).
- **Thread Weight**: The significance of the security thread (e.g., IAM, Phishing) in the overall risk model.

2 Configurable Weights

The calculation relies on predefined weights for both security threads and event severities. However, these values can be dynamically adjusted based on an organization's risk tolerance, security priorities, and how users react to threats over time.

2.1 Thread Weights

Each security thread is assigned a weight representing its importance in the risk model. The following table shows example values:

These weights can be modified to reflect evolving security policies or department-specific risk assessments.

Thread	Weight
Identity and Access Management (IAM)	0.2
Data Loss Prevention (DLP)	0.2
Endpoint Detection and Response (EDR)	0.2
Phishing	0.4

Table 1: Example Thread Weights

2.2 Event Weights

Each event severity level is assigned a weight based on its impact:

Event Severity	Weight
Critical	0.50
High	0.25
Medium	0.15
Low	0.10

Table 2: Example Event Weights

These values can be adjusted based on security policies and organizational risk tolerance.

3 Risk Score Calculation Per Event

For each user, the risk score is determined by summing the contributions from all security events across different threads:

$$\text{Event Contribution} = \text{Event Count} \times \text{Thread Weight} \times \text{Event Weight}$$

For example, consider a user with the following security event:

- **Thread**: IAM
- **Event**: Critical
- **Event Count**: 8 incidents

Using the formula:

$$8 \times 0.2 \times 0.5 = 0.8$$

This value (0.8) is added to the total risk score for that user.

4 Total Risk Score Calculation

The final risk score for a user is calculated by summing all event contributions across all security threads:

$$\text{Risk Score} = \sum_{\text{threads}} \sum_{\text{events}} (\text{Event Count} \times \text{Thread Weight} \times \text{Event Weight})$$

4.1 Example Calculation

Assume a user has the following recorded security events:

Thread	**Event**	**Event Count**	**Thread Weight**	**Event Weight**	**Contribution**
IAM	Critical	8	0.2	0.5	0.8
DLP	High	5	0.2	0.25	0.25
EDR	Medium	7	0.2	0.15	0.21
Phishing	Low	9	0.4	0.10	0.36

Table 3: Example Risk Score Calculation

4.2 Total Risk Score for the User

$$0.8 + 0.25 + 0.21 + 0.36 = 1.62$$

5 Risk Contribution Per Thread

Each thread's contribution is calculated as a percentage of the total risk score:

$$\text{Thread Contribution \%} = \frac{\sum(\text{Event Contributions in Thread})}{\text{Total Risk Score}} \times 100$$

For the example user, the contributions per thread are:

Thread	**Contribution to Risk**	**Percentage**
IAM	0.8	49.38%
DLP	0.25	15.43%
EDR	0.21	12.96%
Phishing	0.36	22.22%

Table 4: Thread Contribution Percentages

This breakdown can be used to generate risk distribution visualizations for better analysis.

6 Risk Score Trends Over Time

The risk model allows tracking of risk scores over time for each user. This helps in identifying patterns of increasing or decreasing risk based on security incidents.

6.1 Risk Score Change Indicators

After each risk assessment, the change in risk score compared to the previous evaluation is recorded. This can be used to monitor security improvements or emerging threats.

- A positive change indicates an increase in risk.
- A negative change indicates a reduction in risk.
- The numerical difference is recorded to track trends over time.

6.2 Example Risk Score Change Output

```
User1: 63.52 (+13.52)
User2: 44.05 (-5.95)
```

7 Dynamic Risk Weight Adjustments

One of the key features of this model is the ability to dynamically adjust thread and event weights based on:

- Organization-wide risk strategy.
- Department-specific security focus areas.
- How users respond to security policies over time.

By analyzing trends in user behavior, security teams can modify the importance of specific threads or event severities, ensuring that risk scores accurately reflect the evolving security landscape.

8 Summary

- Risk score = Sum of (Event Count × Thread Weight × Event Weight).
- Security threads and event severities have configurable weights.
- Risk can be tracked across users within an organization or within specific departments.
- Risk score trends help in identifying changes in security posture over time.
- Organizations can dynamically adjust risk factors based on evolving needs.