# Scoring Methodology and Data Structure

**Overview:**

This page provides detailed documentation on the scoring definitions, column structure, formulas, and conditional formatting used in the Heatmap Insights workbook. It outlines the methodology for scoring Logging, Prevention, Detection, and Response, along with the implementation of risk calculation and external TTP identification. The content covers how data is structured, formulas applied for risk scoring and weighting, and the process for sorting and visualizing key data points.

Here are the proposed definitions for each of the scores moving forward, to help guide the scoring process:

**Logging**

1. **Score 1 (No/Low Logging)**
   * No logs captured for the relevant TTPs or attack vectors.
   * Minimal or no logging capabilities present.
   * Inconsistent or incomplete log records, with no active log review.
2. **Score 2 (Basic Logging, Low Confidence)**
   * Logging is enabled for some events but lacks coverage for critical threat areas.
   * Logs exist but are not consistently reviewed or acted upon.
   * Gaps in visibility may exist in key systems or endpoints.
3. **Score 3 (Improved Logging, Higher Confidence)**
   * Logging is comprehensive and covers most critical areas.
   * Logs are regularly reviewed, and retention policies are in place, but some gaps in analysis or coverage may remain.
   * Confidence in logging as a control is moderate, but improvements could be made.
4. **Score 4 (Comprehensive Logging, High Confidence)**
   * Full logging across all critical systems and events, with automated review and alerting.
   * High confidence in logs being useful for threat detection and analysis.
   * Logs are retained and accessible for sufficient time frames, with robust analysis capabilities.

**Prevention**

1. **Score 1 (No/Low Prevention)**
   * No controls exist to prevent the threat or attack vector.
   * Minimal reliance on preventive measures, leading to high risk.
   * No documented prevention strategies.
2. **Score 2 (Basic Prevention, Low Confidence)**
   * Some preventive controls are in place, but they are either insufficient or inconsistently applied.
   * Limited confidence in their ability to prevent the threat.
   * Some manual interventions are needed to supplement preventive measures.
3. **Score 3 (Moderate Prevention, Higher Confidence)**
   * More comprehensive preventive measures in place, addressing the majority of threats.
   * Automated prevention is active, with regular updates and testing.
   * Gaps may still exist, but overall, risks are well managed.
4. **Score 4 (Strong Prevention, High Confidence)**
   * Full prevention mechanisms are deployed and regularly tested.
   * High confidence in the system's ability to block or mitigate threats before they occur.
   * Preventive controls are automated, fine-tuned, and require minimal manual intervention.

**Detection**

1. **Score 1 (No/Low Detection)**
   * No detection mechanisms for relevant TTPs.
   * Minimal or no monitoring capabilities.
   * Threats are rarely detected in real-time, and response is mostly reactive.
2. **Score 2 (Basic Detection, Low Confidence)**
   * Some detection capabilities in place, but coverage is inconsistent or lacks depth.
   * Detection is limited to certain areas, with slow alerting or response times.
   * Low confidence in detection accuracy and effectiveness.
3. **Score 3 (Moderate Detection, Higher Confidence)**
   * Detection mechanisms are in place across most critical areas, providing timely alerts.
   * Moderate confidence that threats will be identified in real-time.
   * Regular updates to detection rules, though some areas may still be under-covered.
4. **Score 4 (Strong Detection, High Confidence)**
   * Comprehensive detection systems cover all critical threats and attack vectors, providing real-time alerting.
   * High confidence in early detection of threats, with minimal false positives.
   * Threat intelligence and detection mechanisms are updated continuously.

**Response**

1. **Score 1 (No/Low Response Capability)**
   * No response plans or processes in place for the threat.
   * Response is mostly ad-hoc and uncoordinated when incidents occur.
   * Lack of training or preparation for response actions.
2. **Score 2 (Basic Response, Low Confidence)**
   * A response plan exists but is either incomplete or rarely practiced.
   * Response actions are slow, uncoordinated, or ineffective.
   * Confidence in the team's ability to respond is low.
3. **Score 3 (Moderate Response, Higher Confidence)**
   * Documented response processes are in place and regularly tested.
   * Moderate confidence in the team’s ability to respond effectively, but improvements are needed in speed or coordination.
   * Response times are adequate, though not optimal.
4. **Score 4 (Strong Response, High Confidence)**
   * A fully documented and tested incident response plan is in place, with regular drills and training.
   * High confidence in the speed and effectiveness of the response team.
   * Well-coordinated and fast responses, with lessons learned from past incidents integrated into the process.

#### ****Columns and Formulas****

1. **Initial Score (Column A)**  
   This column reflects the initial risk score of each TTP based on its likelihood of being used by multiple threat actors. The higher the score, the more likely the TTP is to be used across different threat actor profiles.
   * **Purpose**: To represent the likelihood of the TTP being exploited by multiple threat actors.
2. **Overall Score (Column H)**  
   The overall score is the average of the four control categories (Logging, Prevention, Detection, Response). This score indicates how well the TTP is currently being controlled within the organization.
   * **Formula**: =AVERAGE(<Logging>, <Prevention>, <Detection>, <Response>)
   * **Purpose**: To provide an aggregate score for how well the organization is managing this specific TTP across all four control categories.
3. **Risk Score (Column I)**  
   The risk score is a product of the initial score (Column A) divided by the overall score (Column H). This formula adjusts the overall score based on the likelihood of the TTP being used. A lower overall score (indicating weaker control) will increase the risk, while a higher overall score will reduce it.
   * **Formula**: =A2 / H2
   * **Purpose**: To factor both the likelihood of the TTP’s exploitation and the strength of your organization’s controls, giving a more accurate reflection of risk.
4. **External TTP (Column J)**  
   This column identifies whether the TTP belongs to a category that is external to the organization's control, such as Reconnaissance or Resource Development tactics. These external TTPs typically cannot be easily mitigated due to their nature.
   * **Formula**: =IFERROR(IF(OR(VLOOKUP(B2,Helper!A:D,4,FALSE)="Reconnaissance", VLOOKUP(B2,Helper!A:D,4,FALSE)="Resource Development"), "Yes", "No"), "Not Found")
   * **Purpose**: To flag TTPs where mitigation is inherently more difficult, due to the fact that they occur outside the organization’s control.
5. **Weighted Score (Column K)**  
   The weighted score combines the risk score (Column I) with an adjustment based on whether the TTP is external or internal (Column J). If the TTP is external, a multiplier of 0.75 is applied to reduce the weight of the risk score, acknowledging the limited control over it. For internal TTPs, the full risk score is retained.
   * **Formula**: =I2 \* IF(J2="Yes", 0.75, 1)
   * **Purpose**: To prioritize TTPs that the organization can more directly control, while reducing the risk of TTPs that are harder to mitigate due to external factors.

#### ****Conditional Formatting****

1. **Risk Score (Column I) - Gradient Color Scale**  
   The risk score is visually represented by a gradient color scale, allowing for quick identification of high and low risk TTPs.
   * **Green**: Low risk scores (<= 6.0).
   * **Yellow**: Moderate-low risk (6.1 to 9.0).
   * **Orange**: Moderate-high risk (9.1 to 12.5).
   * **Red**: High risk (> 12.5).
   * **Purpose**: To quickly visualize which TTPs pose the highest risk to the organization based on the likelihood and overall score.
2. **External TTP (Column J) - "Yes/No" Highlighting**  
   The External TTP column is formatted to distinguish between "Yes" and "No" values, with different background colors applied to each.
   * **Purpose**: To easily differentiate between external TTPs (where the organization has limited control) and internal TTPs (where controls can be more effective).

#### ****Sorting****

To prioritize the most critical TTPs, the data can be sorted by the **Weighted Score (Column K)** from highest to lowest. This sorting process ensures that TTPs with the greatest risk, adjusted for external or internal mitigation difficulty, are addressed first.

1. **Steps to Sort**:
   * Highlight the entire range of data.
   * Go to **Data > Sort**.
   * Select **Column K (Weighted Score)**.
   * Sort **Largest to Smallest** to prioritize high-risk TTPs.