Cyber Threat Insight Reporting

Sample Key Threat Indicators (KTIs) Definition

Severity:
Indicates the criticality of the issue.

..

Impact Score:
Represents the potential damage if the threat is realized.

..

Risk Level:
A general indicator of risk associated with each issue.

..

Issue Response Time Days:
The longer it takes to respond, the higher the threat level could be.

..

Category:
Certain categories (e.g., unauthorized access) carry a higher base threat level.

..

Activity Type:
Suspicious activity types (e.g., high login attempts, data modification) indicate a greater threat.

..

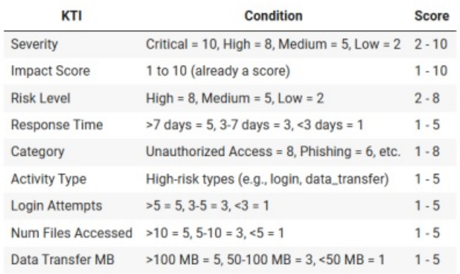
Login Attempts:
Unusually high login attempts signal a brute force attack.

..

Num Files Accessed and Data Transfer MB:
Large data transfers or access to many files in a session could indicate data exfiltration or suspicious activity.

..

KTIs based Scoring Example



KTI	Condition	Score
Severity	Critical = 10, High = 8, Medium = 5, Low = 2	2 - 10
Impact Score	1 to 10 (already a score)	1 - 10
Risk Level	High = 8, Medium = 5, Low = 2	2 - 8
Response Time	>7 days = 5, 3-7 days = 3, <3 days = 1	1 - 5
Category	Unauthorized Access = 8, Phishing = 6, etc.	1 - 8
Activity Type	High-risk types (e.g., login, data_transfer)	1 - 5
Login Attempts	>5 = 5, 3-5 = 3, <3 = 1	1 - 5
Num Files Accessed	>10 = 5, 5-10 = 3, <5 = 1	1 - 5
Data Transfer MB	>100 MB = 5, 50-100 MB = 3, <50 MB = 1	1 - 5

Threat Level Thresholds Definition:
Low Threat: 0–3
Medium Threat: 4–6
High Threat: 7–9
Critical Threat: 10+

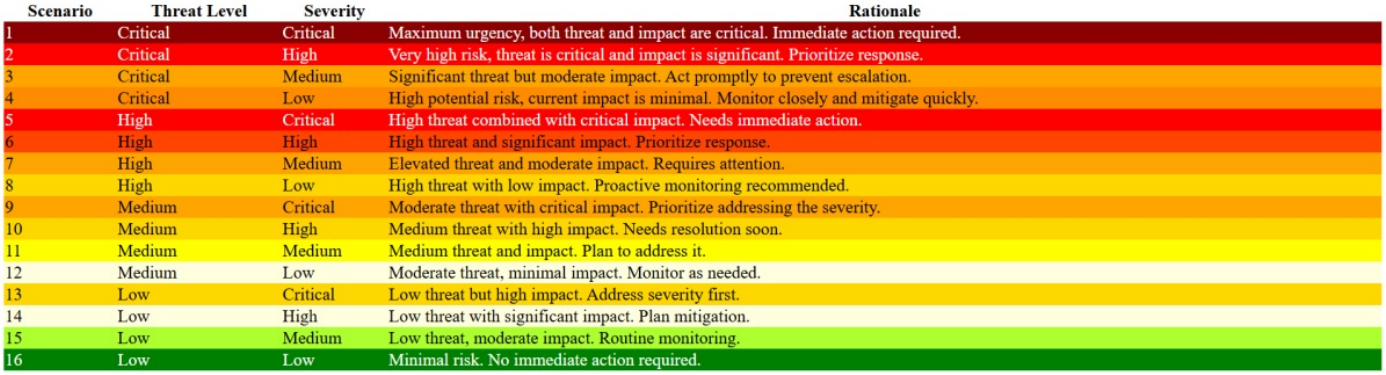
..

Threat Level:
it can be calculated as a weighted sum of these scores.
Example:
Threat Score = 0.3 × Severity + 0.2 × Impact Score + 0.2 × Risk Level + 0.1 × Response Time + 0.1 × Login Attempts + 0.05 × Num Files Accessed + 0.05 × Data Transfer MB

..

Suggestion for Adaptative Defense Mechanisms Colors Scheme

The color scheme is aligned with the mechanism's goals, emphasizing clarity and urgency for visual communication. The intensity of red, orange, yellow, and green represent the risk.



Scenario	Threat Level	Severity	Rationale
1	Critical	Critical	Maximum urgency, both threat and impact are critical. Immediate action required.
2	Critical	High	Very high risk, threat is critical and impact is significant. Prioritize response.
3	Critical	Medium	Significant threat but moderate impact. Act promptly to prevent escalation.
4	Critical	Low	High potential risk, current impact is minimal. Monitor closely and mitigate quickly.
5	High	Critical	High threat combined with critical impact. Needs immediate action.
6	High	High	High threat and significant impact. Prioritize response.
7	High	Medium	Elevated threat and moderate impact. Requires attention.
8	High	Low	High threat with low impact. Proactive monitoring recommended.
9	Medium	Critical	Moderate threat with critical impact. Prioritize addressing the severity.
10	Medium	High	Medium threat with high impact. Needs resolution soon.
11	Medium	Medium	Medium threat and impact. Plan to address it.
12	Medium	Low	Moderate threat, minimal impact. Monitor as needed.
13	Low	Critical	Low threat but high impact. Address severity first.
14	Low	High	Low threat with significant impact. Plan mitigation.
15	Low	Medium	Low threat, moderate impact. Routine monitoring.
16	Low	Low	Minimal risk. No immediate action required.

This color based scenarios approach aligns urgency with the dual factors of threat level and severity, ensuring quick comprehension and appropriate prioritization.

Autor: Atsu Vovor |Consultant Data Analytics Specialist | Machine Learning | ..