Rating Threat Intelligence in the ThreatConnect TI Ops Platform

Reduce false positives and achieve consistent collaboration and communication about threats

Why are standardized threat ratings & confidence levels important?

In order to achieve effective threat intelligence use, sharing, and collaboration, there needs to be a common vocabulary and a standard way to rate threat intel. The ThreatConnect TI Ops Platform leverages built-in Threat and Confidence Ratings. The result is that false positives are being minimized, analysts are all operating efficiently, and collaboration is working effectively. This gives the defenders the upper hand over the adversaries.

Threat Rating

In ThreatConnect, a severity rating can be assigned to any piece of intel, taking into account:

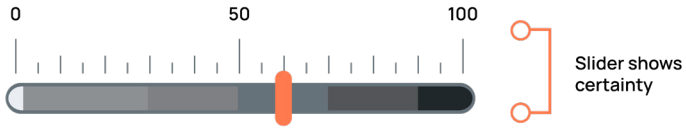
1. Capability (skills and resources) of the adversary/threat
2. Determination (focus and persistence) of the adversary/threat
3. Progression of the event/incident (phase in the Cyber Kill Chain)

Level	Label	Capability	Determination	Progression
0	Unknown	Not enough information to assess threat		
1	Suspicious	Unknown		No confirmed malicious activity (some suspicious activity has been observed)
2	Low	Unsophisticated	Purely opportunistic and short-lived	Pre-attack activity or attempt (potential to turn into a large threat)
3	Moderate	Basic skills and resources	Directed but not persistent	Active intrusion (delivery, exploitation, installation)
4	High	Advances skills and resources	Targeted and persistent	Post-compromise (C2, actions on objective)
5	Critcal	Unlimited skill and resources	Wholly focused and determined	Any phase of progression

Confidence Rating

A Confidence Rating can be assigned to threat intelligence using factors like:

1. Has it been confirmed by independent sources or first-hand analysis?
2. Is it plausible and logical? Taken by itself, does it make sense?
3. Is it corroborated by, or consistent with, other available information?



Type	Label	Capability	Determination	Progression
Unknown	0	Unknown; has not been assessed		
Discredited	1	Confirmed as inaccurate		
Improbable	2 - 29	Unconfirmed	Not logical or plausible	Contradicted by other information
Doubtful	30 - 49	Unconfirmed	Possible but not logical	No additional information on subject
Possible	50 - 69	Unconfirmed	Reasonably logical	Some consistencies with other information
Probable	70 - 89	Unconfirmed	Logical and plausible	Consistent with other information on the subject
Confirmed	90 - 100	Confirmed accurate by independent sources and analysis		