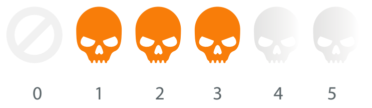
ThreatConnect™

Evilness Rating

Skulls Scale for Cyber Threats

Threat Rating



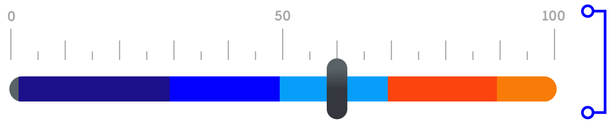
SKULLS SHOW SEVERITY

When assigning a threat rating, consider the following factors:

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	Advanced skills and resources	Targeted and persistent	Post-compromise (C2, actions on objective)
5	Critical	Unlimited skill and resources	Wholly focused and determined	Any phase of progression

Confidence Rating



SLIDER SHOWS CERTAINTY

When assigning a confidence rating, consider the following factors:

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	Percentage	Confirmation	Plausibility	Consistency
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		

Why are standardized threat ratings & confidence levels important?

In order for threat intelligence sharing and community collaboration to work, we all need to be speaking the same language. We, the analysts at the front lines, need a standard vocabulary and a standardized rating system so that we are all evaluating threats in the same manner. The ThreatConnect platform does this by providing the universal threat and confidence rating system described here and applying it across all ThreatConnect intelligence sharing communities. The end result is that we are all on the same page, speaking the same language, and ultimately are collaborating more effectively.
We are winning the battle of wits against the threat actors, together.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708