Report on threatconnect

Threat Level framework is designed to categorize and evaluate the severity of cybersecurity threats. Although ThreatConnect itself doesn't specifically publicize a proprietary "evaluation system" with set levels, the framework for evaluating threat severity is commonly referenced in terms of threat levels used by many cybersecurity frameworks. The levels often used in threat evaluation systems are typically based on a scale that ranges from minor to critical.

Here's a generalized list of threat levels and their characteristics commonly found in threat evaluation systems:

1. Informational (Level 0)
   Characteristics:
- Indicates that no immediate threat is present.
- Information or activity that is purely for awareness.
- Typically includes routine system updates or non-malicious activity.
- Used for tracking purposes and improving situational awareness.

2. Low (Level 1)
   Characteristics:
- Minor threat with low impact on operations.
- Involves low-level malware or adware.
- Exploits that are difficult to execute or have limited impact.
- Basic security measures (e.g., antivirus, firewall) are often sufficient.
- No significant data compromise or operational disruption.

3. Medium (Level 2)
   Characteristics:
- Moderate threat that could potentially impact operations.
- Includes more sophisticated malware, phishing attacks, or social engineering attempts.
- Requires active monitoring and may need immediate attention.
- Possible data compromise or minor operational impact.
- Potential to escalate if not addressed properly.

4. High (Level 3)
   Characteristics:
- Significant threat that is likely to impact operations.

- Includes targeted attacks, advanced persistent threats (APTs), or ransomware.
- Requires immediate action to mitigate.
- High potential for data theft, operational disruption, or financial loss.
- May involve coordinated and persistent attack vectors.

5. Critical (Level 4)
   Characteristics:
- Severe threat with critical impact on operations.
- Involves highly sophisticated attacks, nation-state actors, or zero-day exploits.
- Immediate and comprehensive response required.
- High likelihood of extensive data theft, operational shutdown, or severe financial loss.
- Could result in significant reputational damage and regulatory implications.