ThreatConnect™

Applying Thermodynamic Principles to Threat Intelligence

Kinetic and potential are different states of energy that describe the capability of an object to do work. Kinetic energy results from an object in motion, such as a moving car. Potential energy comes from an object's position and may be converted into kinetic energy, such as holding a ball above the ground, a compressed spring, or a drawn bow and arrow. In countless applications scientists measure these forms of energy to better understand how an object will interact with its environment. We posit that these concepts can be applied to the cybersecurity world to apply and assess intelligence on indicators.

An indicator in the cybersecurity world has several different characteristics that will dictate if or how an organization defends against it.

We posit that these equations can be used to assess the kinetic and potential energy of indicators:

$$E_K = U\left[\frac{S + O + D + A}{4}\right]\left[1 - \frac{T}{P}\right]$$

- E_K Kinetic Energy of an indicator
- U Whether the indicator has been used in an attack (1 for yes, 0 for no)
- S Whether your Organization's Sector was targeted in the attack (1 or 0)
- O Whether your Organization has been targeted (1 or 0)
- D Whether your Organization's specific data types have been targeted (1 or 0)
- A Whether the attack carried out by the pertinent Adversary (1 or 0)
- T Age of the indicator in days since it was first identified
- P Number of days over which you deprecate malicious indicators

$$E_P = C\left[1 - \frac{T}{F}\right]$$

- E_P Potential Energy of an indicator
- C Whether tactics associated with that indicator are consistent with your adversaries' (1 or 0)
- T Age of the indicator in days since it was first identified
- F Number of days over which you deprecate suspicious indicators

By evaluating indicators, irrespective of their source, for their kinetic and potential energy, **organizations can incorporate basic intelligence requirements and their defensive decisions.**

In doing so, organizations can incorporate intelligence requirements and more efficiently assess and defend their organization and avoid wasting defensive resources on unnecessary indicators. Organizations can also use this evaluation to identify intelligence or collection gaps. Conversely, intelligence providers similarly can use this framework to identify shortcomings in their product that, if addressed, would facilitate its consumption and integration. If intelligence providers also included the calculated energies for various industries for the indicators in their reports, they could facilitate their customers' consumption and triage efforts.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

Worksheet

	Indicator										
1	Has this indicator been used in an attack? (1 or 0) If 0, skip to row 11.										
2	Was your organization's sector targeted in the attack related to this indicator? (1 or 0)										
3	Was your organization targeted in the attack related to this indicator? (1 or 0)										
4	Was your organization's specific and unique data type targeted in the attack related to this indicator? (1 or 0)										
5	Was the attack related to this indicator carried out by an adversary that is pertinent to your organization? (1 or 0)										
6	Add the previous four rows and divide by 4.										
7	How long has it been in days since this indicator was first identified?										
8	Divide the previous row by the number of days over which you deprecate malicious indicators.										
9	Take 1 minus the previous row.										
10	Kinetic Energy of the indicator is row six multiplied by row nine.										
11	Are the tactics associated with the indicator consistent with your adversaries' tactics? (1 or 0)										
12	Divide previous row by the number of days over which you deprecate suspicious indicators.										
13	Take 1 minus the previous row.										
14	Potential Energy of the indicator is row eleven times row thirteen.										

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708