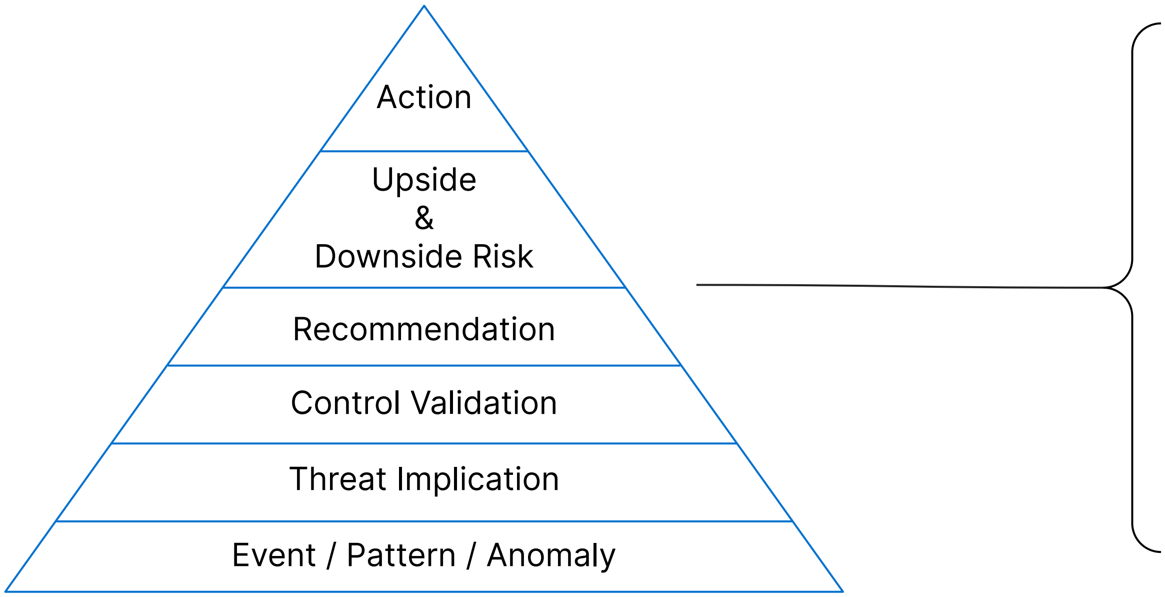
Intelligence to Risk Framework



Action

Upside
&
Downside Risk

Recommendation

Control Validation

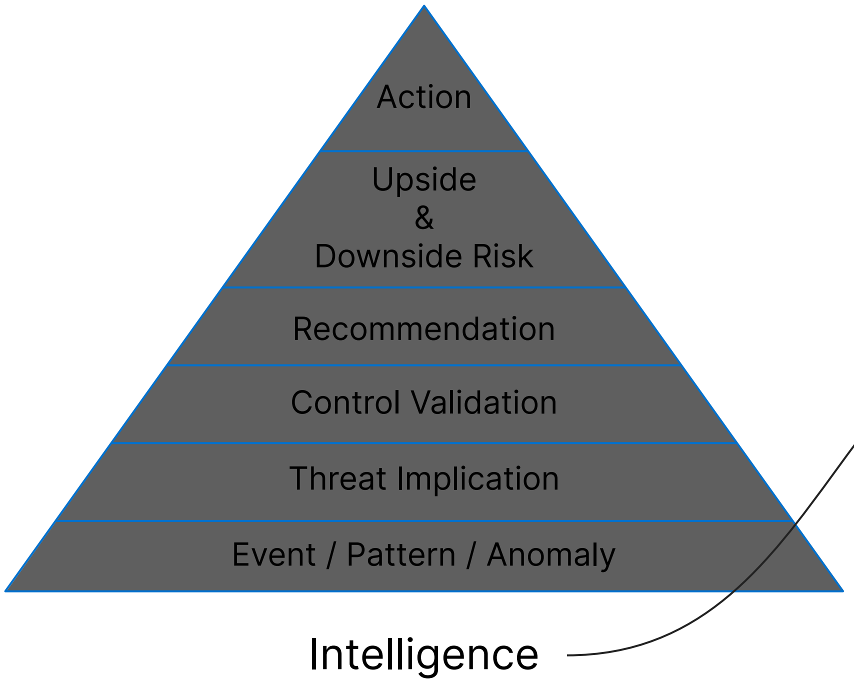
Threat Implication

Event / Pattern / Anomaly

Intelligence

The "Intelligence to Risk Framework" is a progressive process that takes you from raw intelligence to specific actions with upside/downside risk baked into your messaging.

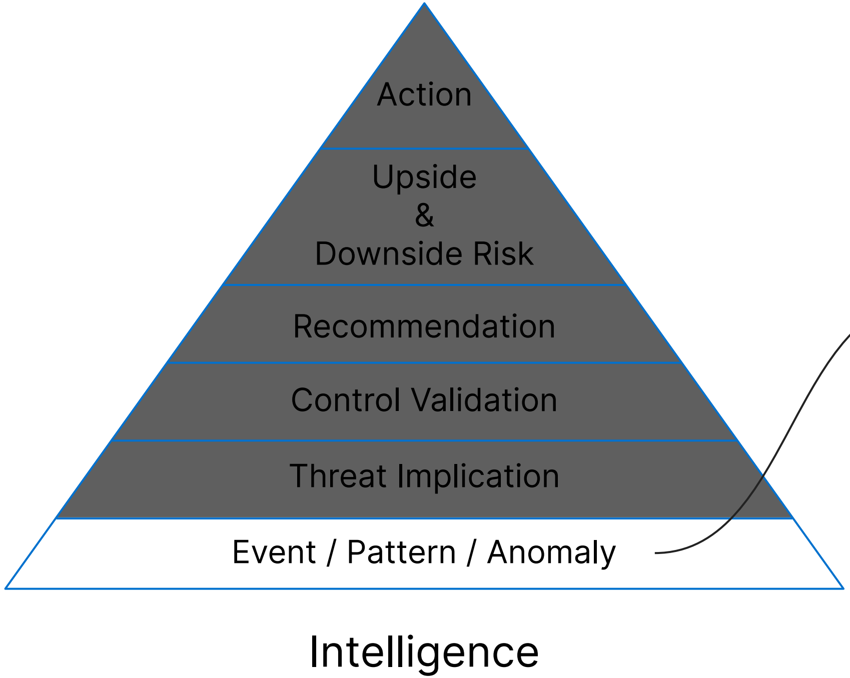
Intelligence to Risk Framework



Intelligence

Everything starts with intelligence, either internal or external

Intelligence to Risk Framework



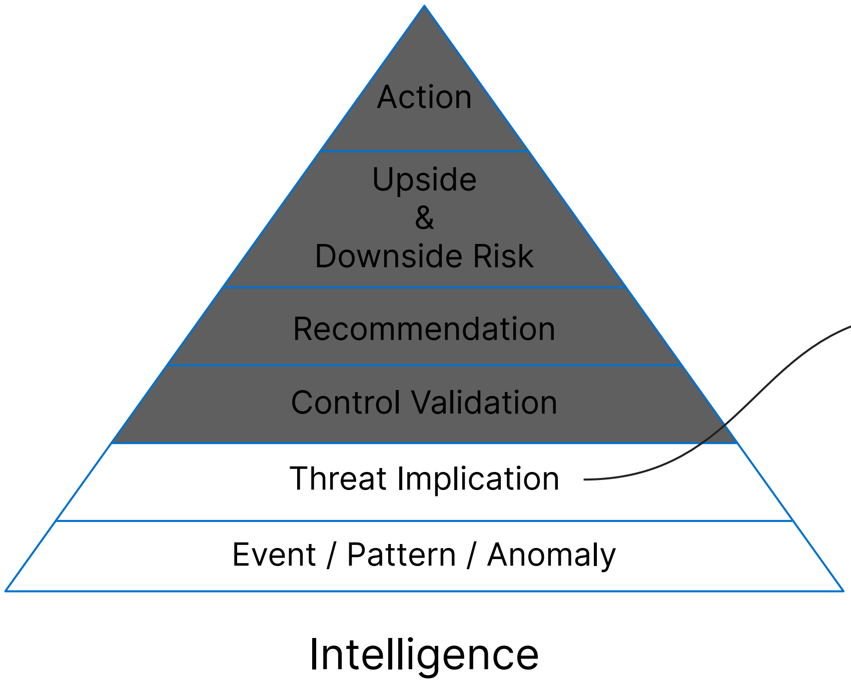
Event/Pattern/Anomaly

After consuming a single piece of intel or multiple intel reports there are three forms of insight that are derived.

- Event: A singular event that has an outsized impact on the present, such as Russia invading Ukraine or the public disclosure of Log4j
- Anomaly's: An outlier event discovered from a series of data points, usually part of a retrospective exercise looking at past events.
- Patterns: Non-obvious connections from disparate sources such as consuming a series of reports of a set theme.

Note: This is the one I've come across most in my time using this framework.

Intelligence to Risk Framework



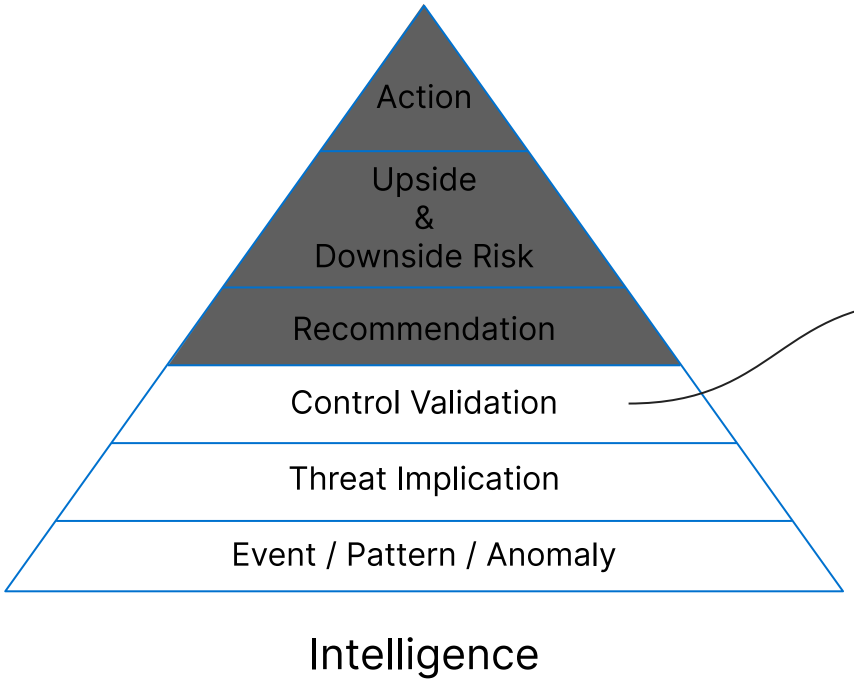
Threat Implication

The “implication” of a threat can stand alone (event) or be created through the evolution of actor behaviors (anomaly/pattern). I would label this as “general risk” because we’ve not taken the time to uncover how this risk applies to our Orgs. controls, business, etc.

- *IMPORTANT: Time to flex those mental muscles! The implication has cascading effects, either obvious or non-obvious. It’s our job to uncover these effects and convey them in a meaningful way through second-order thinking.*

Example: Our research team monitored ShadowPad malware use against India's electric grid (source). The threat implication for India is straightforward. The implication for western businesses is significant for any business that outsources helpdesk, call center, manufacturing, etc.

Intelligence to Risk Framework



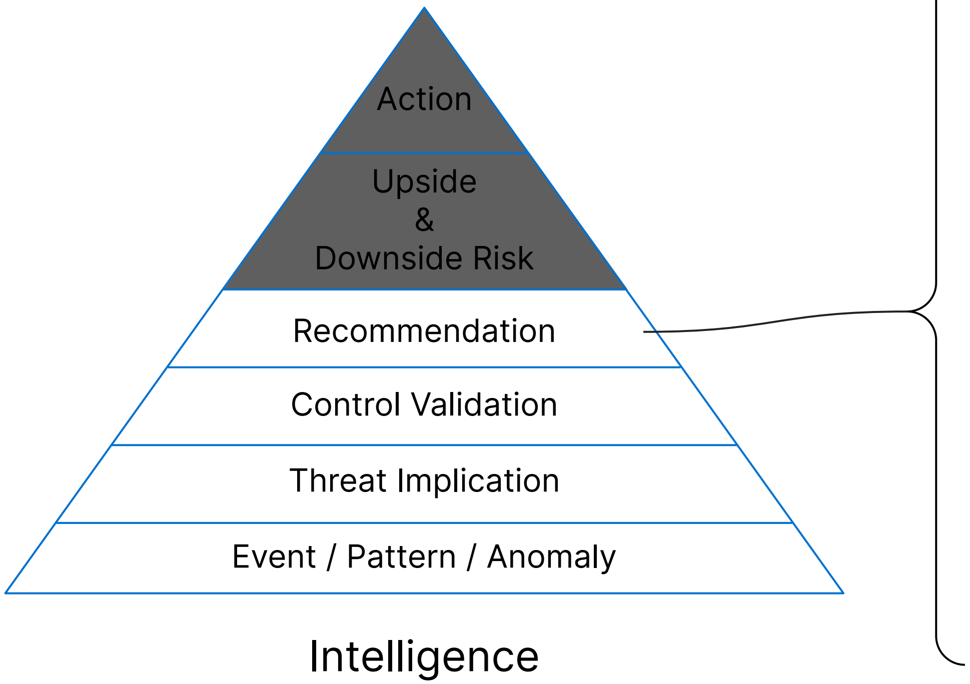
Control Validation

Once we've thoroughly understood the threat implications and bottled it up into a easily understandable format (written or presentation), it's time to think through the existing controls we have in place to defend against this threat. If there are existing controls, make sure to clarify in simple terms how and in what capacity you're defending against this threat. Equally important is to clarify where your existing defenses are not covering and the downstream implications of that.

This is where multiple stakeholders representing different perspectives with different levels of control knowledge are critical for real validation (or at least discovery that controls are missing/lacking).

Recorded Future®
Predict 22
The Intelligence Summit

Intelligence to Risk Framework



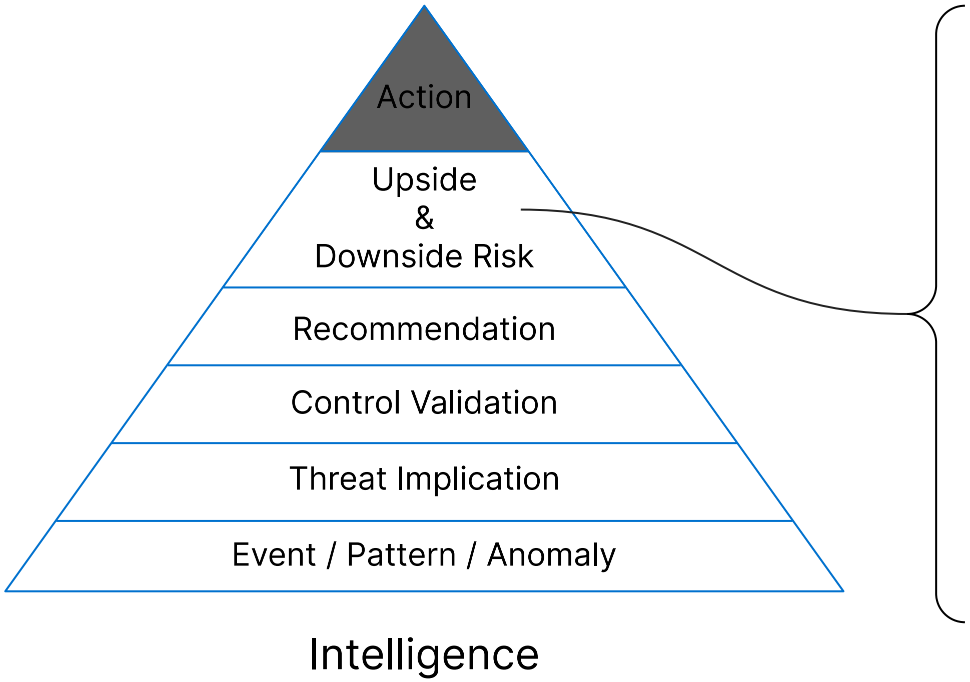
Recommendation

It’s time to think through what recommendations our leadership should consider to mitigate (sometimes accept/transfer) the implications of the threat.

- *Mitigate: With every recommendation there’s a decision to be made that comes with trade offs, both downsides and upsides. We need to anticipate that tradeoff and incorporate it into the recommendation, showing that we’ve thought through the downside and upside risks associated with decision. We may not be accurate, but we’re providing something our leadership can build on.*
- *Recommendation Types: Immediate short-term recommendations tend to have a low cost (time, money, human resources, cultural change), but are less sustainable, while longer-term recommendations cost more, but tend to be more sustainable (extended security posture)*

Example: The supply chain for different types of firmware is complex and multiple orgs are involved in creating it. Most execs would decide to accept the risk of using compromised firmware because mitigation would be too resource intensive.

Intelligence to Risk Framework

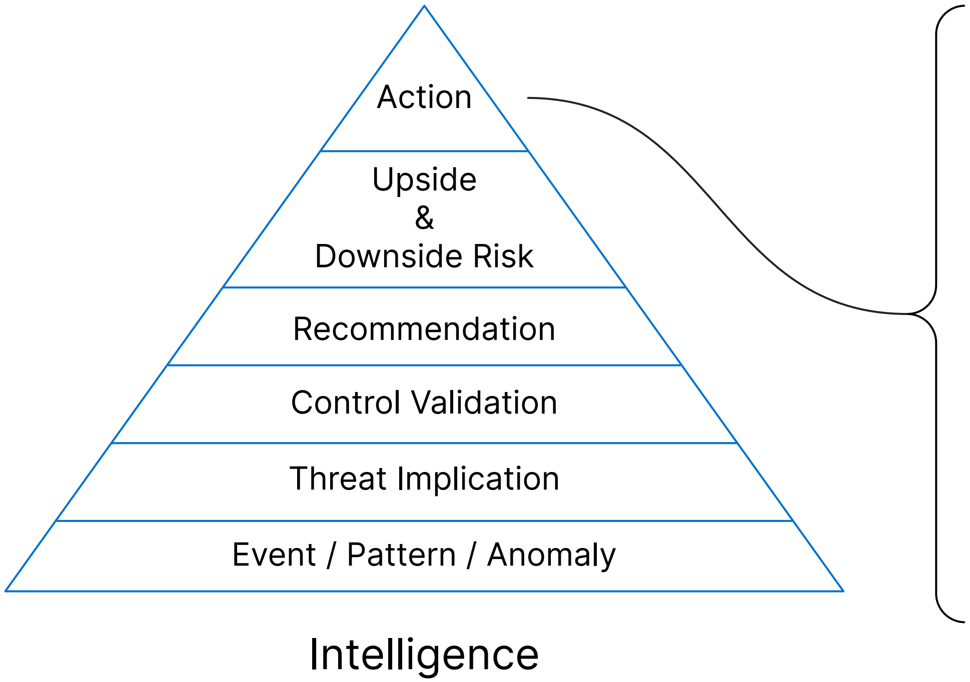


Upside/Downside

The tradeoff risks we’re contemplating can be measured quantitatively and qualitatively based on likelihood and impact (during the initial process don’t get bogged down by the quantitative piece). When sharing the tradeoff risks in our recommendation, focus on 1 downside and 1 upside risk. By focusing your audience's attention on one detailed narrative, your main points will come across without distraction. This focused approach does not mean we ignore the remaining risks, we’ll incorporate those into the appendix.

- Downside: Compliance, Social Governance (e.g. Brand reputation), and Resources.
- Upside: All upside gains for mitigating risk lead to revenue, but this can be broken down into different variables. Speed, increased market share, reduce churn, increase employee engagement, etc.

Intelligence to Risk Framework



Action

Based on our ability to convey this message within our businesses current focus/restraints, the leadership team will decide (and act) if they're willing to commit to short-term, long-term, or a combination of both recommendations. Remember, not acting is sometimes the "action" taken.

Recorded Future®
Predict 22
The Intelligence Summit