INTELLIGENCE · CONCEPTS AND HISTORY

Cyber Threat Intelligence: Generating Predictive Knowledge in InfoSec

Cyber threat intelligence turns information about attackers into knowledge defenders can act on before an attack succeeds. This short article explains its levels, the main analytic models and what makes it useful rather than noisy.

ModQu research article · 680 words · 6 references (APA 7th edition)

Most information security work is reactive: patching vulnerabilities, blocking malicious traffic and investigating incidents after they happen. Cyber threat intelligence (CTI) aims to change this by learning who is likely to attack, how they operate and what they want, so that defenders can anticipate attacks and prioritise their efforts. Because no organisation can defend everything equally, knowing which threats are most likely is what allows limited security budgets to be spent where they matter. It applies the ideas of traditional intelligence, requirements, collection, analysis and dissemination, to the digital threats facing organisations.

Three levels

Like other intelligence, CTI is produced at different levels. **Strategic** threat intelligence informs executives about the threat landscape, such as which groups target their industry and why. **Operational** intelligence describes specific campaigns and the tactics, techniques and procedures attackers use. **Tactical** or technical intelligence consists of indicators of compromise: malicious IP addresses, domain names and file signatures that can be fed directly into security tools. Tounsi and Rais (2018) note that technical indicators are the most widely shared form but also the shortest-lived, because attackers can change them cheaply.

Thinking like the attacker

Two analytic models shaped the field. Hutchins et al. (2011) adapted the military "kill chain" to computer intrusions, describing seven stages from reconnaissance through weaponisation, delivery, exploitation, installation and command and control to actions on objectives. Their key insight was that defenders need to break only one link to stop an intrusion, and that studying how attackers progress lets defenders build layered defences and detect campaigns early.

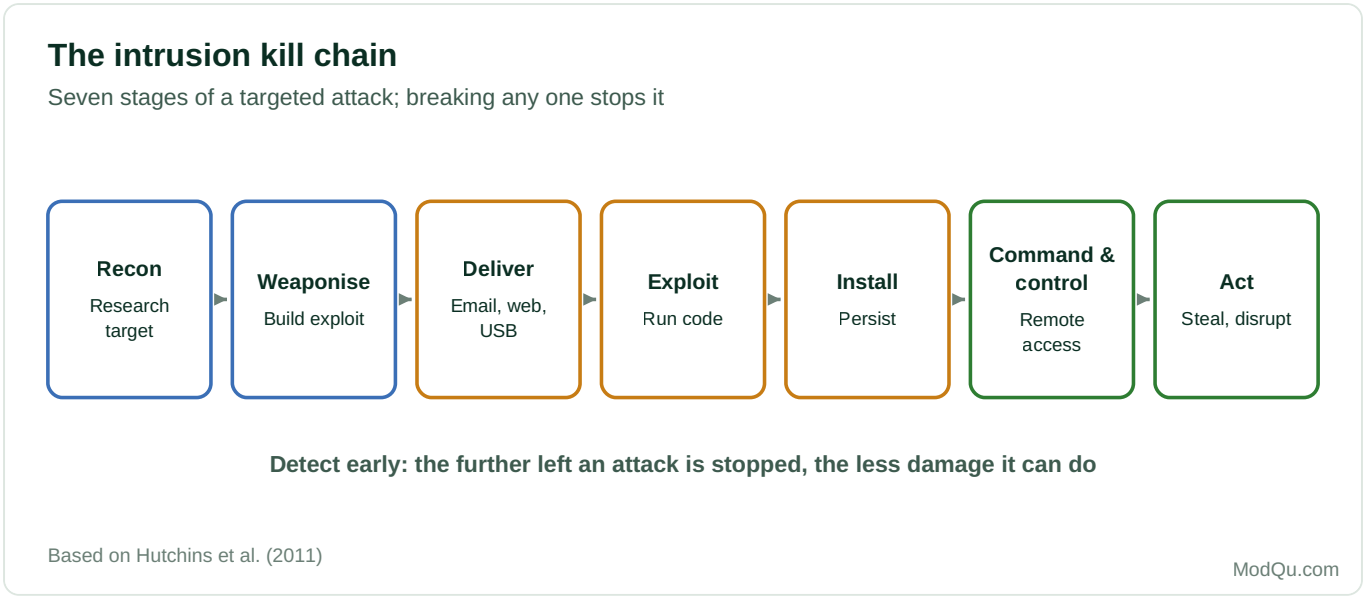


Figure 1. The intrusion kill chain. Mapping where an attack was detected or stopped shows defenders where their defences are strongest and weakest. Based on Hutchins et al. (2011); diagram by ModQu.

Caltagirone et al. (2013) proposed the **diamond model**, which describes every intrusion event through four linked features: the adversary, its capability, the infrastructure it uses and the victim. Pivoting between these features, for example from a known piece of infrastructure to other victims who were attacked through it, helps analysts connect separate incidents into campaigns. Strom et al. (2018) describe MITRE ATT&CK, a public knowledge base that catalogues attacker techniques observed in real intrusions, now widely used as a common vocabulary for detection and reporting. Mapping an organisation's defences against such a catalogue shows which known techniques it could detect and which would pass unnoticed, turning threat knowledge into a concrete list of improvements.

Where the information comes from

Threat intelligence draws on many sources. Inside the organisation, firewall, email and endpoint logs record attempted and successful intrusions, and incident investigations reveal how attackers behaved. Outside it, security vendors publish reports on threat groups, governments issue advisories, industry groups circulate warnings among members, and researchers monitor underground forums where stolen data and attack tools are traded. Each source has strengths and biases. Vendor reports tend to focus on the groups their own customers encounter; internal logs show only attacks that were noticed. Good analysts record where each piece of information came from and how much it can be trusted, exactly as in other intelligence disciplines.

Sharing and its limits

Because attackers reuse tools and infrastructure against many targets, sharing intelligence among organisations multiplies its value. Wagner et al. (2019) review sharing platforms and standards and identify persistent obstacles: concerns about trust, legal liability and reputation, and the low quality of much shared data. Lemay et al. (2018), surveying public reports on advanced persistent threat groups, show how much can be learned from open reporting but also how inconsistent naming and attribution across vendors make it hard to combine.

What makes CTI useful

Useful threat intelligence is driven by the organisation's own requirements: which assets matter most, and which adversaries are likely to target them. It favours knowledge of attacker behaviour, which changes slowly, over lists of indicators, which change quickly. And it reaches the people who can act, from the security operations team to the board. A short monthly briefing for executives on which threats matter to the business, and why, is often worth more than thousands of automated indicators that no one reviews.

References

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis* (Technical Report ADA586960). Center for Cyber Intelligence Analysis and Threat Research.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80–106.

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security, 72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). *MITRE ATT&CK: Design and philosophy* (Technical Report MP180360). The MITRE Corporation.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security, 72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security, 87*, Article 101589. https://doi.org/10.1016/j.cose.2019.101589