Cyber Threat Framework

Frequently Asked Questions (FAQ)

Why did you create this?

In discussing cyber threat activity with senior leadership and policy makers within the US Government's Executive Branch, it became apparent that *perspective matters* and that we had no common conceptual backdrop or language by which to communicate. Cyber experts couldn't easily and consistently convey what was happening on the networks to non-cyber audiences, and senior leaders couldn't readily understand the essence of what they were being told or how to put it to use in decision making. The problem was compounded when passing threat information between departments/agencies, where each characterized activity to meet their internal needs using their own terms, many of which had different meanings even when they used the same words. The Cyber Threat Framework was created to address all of these issues – to describe and present cyber threat information in a manner that allowed traceability from the most specific information to a broad executive summary regardless of where it was collected or by whom, using terms that were independent of any particular mission or expertise. The Framework is also meant to enhance information sharing amongst the widest possible audience, whether in government, industry, or academia, domestic or internationally. We found it preferable to create this 'independent' framework to which all others could be mapped rather than try to create a Rosetta Stone translator for the myriad of alternative models in use.

Is the material 'public' unencumbered information?

Yes. The Cyber Threat Framework and the accompanying Lexicon are publicly available on the Director of National Intelligence Website (https://www.dni.gov/index.php, search for 'Cyber Threat Framework'). Copies of both and briefings on what the Framework is and how to use it are posted on this website.

Doesn't making this unclassified and widely available help our adversaries?

No. The building blocks of the Cyber Threat Framework are publicly available knowledge and many are contained in a myriad of existing frameworks or cybersecurity literature proffered by industry or within the US Government. The principles that make the Framework unique are the use of standardized language drawn from a variety of sources and the hierarchical approach to its presentation, both of which are built on common and open knowledge.

Why are you sharing this rather than keeping it for US Government advantage?

While the Cyber Threat Framework is valuable to a single user because of the compilation of data described in common, publicly available terms, and its presentation in a consistent, structured and repeatable manner, its power is multiplied when it serves as a platform facilitating communication and information exchange between multiple parties. "Cyber" is a complex and intrinsically difficult mix of issues such as technology, threat, and target. We make the problem even more difficult when we choose to describe and discuss it in different 'tongues'. By serving as a form of 'cyber Esperanto' for threat, the structured hierarchical approach serves as a form of syntax and grammar for such a dialogue, while the use of a shared or common lexicon constitutes its dictionary.

Given that individuals, government, industry, or academia, are dependent on the availability and reliability of automated systems and all face the same cyber problems, it's in everyone's interest to have a common language and an ability to share information to the greatest extent possible – attributes which are goals and characteristics of the Framework. Since malicious cyber activity frequently crosses national borders, this structured and hierarchical methodology can also provide a common approach to facilitate the exchange of cyber threat data between countries or other types of organizational boundaries. Note that the efficient exchange of threat data does not require that each party implement an identical model. Even when the participants have customized this model – or created their own – as long as they consistently adhere to their model and share the structure and accompanying documentation, effective information sharing can still occur.

Who participated in its creation?

The Cyber Threat Framework has its origins in an Office of the Director of National Intelligence/National Intelligence Manager for Cyber-led working group whose members represented departments/agencies from across the Federal Executive Branch. Its current form and content have been further shaped by an ongoing dialogue with industry, academia, and foreign partners.

Who is expected to be the primary user?

Within the US Government, the Cyber Threat Framework is the preferred means for providing cyber threat information to and describing threat activity for senior leadership and policy makers. The Department of Homeland Security, Federal Bureau of Investigation, and the Office of the Director of National Intelligence's Cyber Threat Intelligence Integration Center were early adopters, using the Framework as a means for describing and sharing cyber threat information with consumers both in and outside of government. In non-US Governmental settings, it has received a positive reception from Allied nations and from corporate executives looking for a means to better understand individual threat activities and put them into a business context, and to provide a common context for cyber security and cyber threat intelligence professionals to track and describe malicious activity. This Framework adds value in all those settings, providing a means to communicate the details of cyber threat activity between the technical staff and corporate leadership that is of value to both.

Does this portend a change in cyber threat activity reporting?

At present, cyber threat reporting within the US Federal Government follows standards established by each of the reporting agencies in both content and format – the Cyber Threat Framework does not replace these existing standards or reports, but can be added by these organization as metadata or can be applied manually or in an automated fashion after the fact to normalize the data. However, since the Framework is the preferred approach for providing a consolidated threat picture to senior US Government leaders and policy makers, we expect reporting agencies will increasingly include cross-references and linkage to the Framework in their activity reporting. Over time, the transparency and simplicity of the Framework, the commonality it provides, and its ability to enhance information sharing and facilitate understanding will promote further adoption and use.

What cyber threat activity is captured in the Framework?

The Cyber Threat Framework is meant to be broad enough to describe all reported cyber threat activity, whether attributed to a foreign actor, a cyber criminal, or an insider threat. All of the available detail about the threat activity can be captured in the Framework – aggregations of activity are decomposed into the individual details of each activity and then included separately. The Framework is meant to record any observed and reported cyber threat activity; implied activity (X was observed to occur which implies Y must have happened) and analytic judgements are not included, but can be correlated and associated with Framework records.

Where would I get all this data?

Collecting data for the Cyber Threat Framework is much like crowd sourcing. No individual or entity is expected be omniscient. Collectively, each contributes (reports) what they observe or generate from cybersecurity activity (e.g., network audit logs) or other records (such as open source research) which can then be captured within the appropriate part(s) of the Framework. While the ability of a single organization to generate a picture of threat activity through this approach is useful – especially if it can be applied to different threat actors or incidents – the Framework gains power as a means for normalizing and facilitating exchange or pooling of data between organizations. Such data aggregation can be done within a single large organization, a consortium, or a larger group that has agreed to share data.

Does every 'block' need to be completed?

No. The value of the Cyber Threat Framework is that it's a representation of what was observed and reported, a form of 'ground truth' or objective data that can support but does not replace analysis. Implied activities (to do X implies the perpetrator must have done Y) are not included since they are not objectively or directly measured data, though one could implement the Framework to allow inferences or implied activity to be 'tagged' or associated with specific data. By illuminating both knowns and unknowns the Framework enables the consumer to draw logical conclusions about threat activity, and through subsequent analysis, to make informed judgments about malicious actor behavior or internal cyber defenses – e.g., were our prior judgments about the threat valid, why didn't we see something expected or necessary, are we looking for the right things or in the right places, are our sensors capable or optimally positioned?

I own a small business – you expect me to collect and report all this data?

No. If you have or collect cyber threat information and have the means to provide it to others, we would encourage you to do so to an appropriate forum (e.g., a commercial cybersecurity provider, Information Sharing Analysis Center, etc.), however limited your data might be. Every data point contributes to a greater understanding, and because not everyone sees everything, every contribution adds value.

Can 'insider threat' and supply chain activities be captured?

Yes. All reported cyber threat activity can be included in the Cyber Threat Framework, whether it's conducted by a national-state actor, cyber criminal, or a malicious insider, and whether it's digital in nature (sensor derived) or identified through other means such as user or security reports.

Why aren't cyber analytic products included?

A fundamental principle of the Cyber Threat Framework is that it represents observed, and measurable, and measured facts concerning cyber threat activity. As such, the Framework serves as a common foundation of knowledge from which to make analytic judgments. It supports but does not replace analysis.

Is the collected data useful standing alone, or do I need additional information for it to make sense?

Yes. The fact of cyber threat activity, the type of reported activity, and its placement within the Cyber Threat Framework can inform a variety of consumers and uses. That said, systematically capturing data such as *when* the activity occurred, *who* it targeted and *how*, *who* reported it, and *how long* after the activity was it reported may improve confidence in the data, can facilitate more timely and informed cybersecurity decision making, can an support analytic efforts such as trend and vulnerability analysis.

Who is the intended audience?

The Cyber Threat Framework has value to a variety of consumers, from senior executives to cyber security and cyber intelligence professionals in government, industry, and academia. Originally the Framework was built to more consistently capture disparate threat data and to better inform senior leadership and policy makers in the US Government by placing cyber threat activity in a consistent context and avoiding technical and non-technical audiences 'talking past each other' due to arcane jargon—or the use of common terms that mean different things to each community. As the Framework evolved it became apparent that other decision makers could also benefit from the same insights and would accrue the same benefits from a shared or common platform. Further, because the Framework provides traceability from the executive summary at the top of the Framework to the most finite details known about the threat activity in the lowest levels, it has value to cyber analysts and network defenders as well. From our initial outreach we have also discovered the Framework has utility in communicating cyber threat activity between and with our international partners as well.

Who is currently using the Framework?

Since 2013 the Cyber Threat Framework has been the foundation of the US Government's Cyber Incident Response Schema. Early adopters of the Framework include the US Department of Homeland Security, the Federal Bureau of Investigation, the Office of the Director of National Intelligence's Cyber Threat Intelligence Integration Center, as well as several NATO members. Within NATO it is the methodology for describing cyber threat activity in their evolving Cyber Defense Strategy. Various research organizations and private sector firms have examined the Framework and incorporated it or mapped it to their own cyber ontologies. A number of universities have expressed interest in incorporating it into their business, information systems, and management curricula.

Where would I expect to see the framework?

The Cyber Threat Framework will be used to characterize cyber threat activity in Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) products, and in discussions involving policy and decision making in the Federal Executive Branch of the US Government. It is also under consideration for inclusion in the conceptual context and language used for notification by the US Government to victims of malicious cyber activity.

How would it be presented?

The Cyber Threat Framework currently appears within specific threat reporting or as an accompanying graphic depiction of cyber threat activity. Several partners are exploring how to operationalize it as a tool for knowledge discovery or visualization. As an open standard and transparent model, the Framework lends itself to automation of the tagging and exchange of data, and to subsequent analysis or decision making.

We have a similar framework – how is this different?

The Cyber Threat Framework was drawn from a myriad of existing frameworks each developed to support a specific mission or unique user community. This Framework serves as a universal translator drawing on the best of breed from all. It is independent of any cylinder of excellence or specialty. The Framework provides a common language (a 'Cyber Esperanto') that enhances communication and information sharing across communities and throughout individual organizations, from the network operational center or server room to the board room.

I've been 'hacked' and I just need to get back on line – how does the Framework help?

The Cyber Threat Framework can provide a better understanding of the cyber problem you face and suggest what actions you might need to take to recover, but it does not identify or specify preventative measures or recovery actions should prevention fail. We are working to build linkages to the NIST Cybersecurity Framework to facilitate those mitigation actions and to help entities preemptively enhance their cybersecurity posture. This Framework was designed to add clarity and consistency by adherence to a structured hierarchical approach to describing cyber threat activity plus shared and explicitly-defined terminology to bridge the gap between the technical experts and the layperson in terms that are 'actionable' and relevant to both.

Presuming I've collected all this data or see it in reporting, what can I do with it?

The Cyber Threat Framework is meant to help establish 'ground truth' about the existing cyber threat environment and the activities being encountered therein. As a collection of 'known' objectively measured data, it forms the basis for subsequent analysis of a given activity and over time, can provide the basis for identifying trends and vulnerabilities. It also provides the foundation for effective communication between the technical experts and management within an organization, which supports informed decision making and for sharing cyber threat information with other organizations.

I don't understand – who can help me?

Visiting the Office of the Director of National Intelligence's web site is a first step. Please use the "contact us" link on this site to submit your questions, comments, or information requests. Engaging with the Department of Homeland Security, the Federal Bureau of Investigation, or the Office of the Director of National Intelligence's National Intelligence Manager for Cyber provides additional avenues for answers to specific questions.