DRAGOS

Whitepaper

STRENGTHENING INDUSTRIAL CYBER DEFENSE WITH MITRE ATT&CK FOR ICS AND THREAT INTELLIGENCE

September 2022

Dragos, Inc.

info@dragos.com

@DragosInc

OVERVIEW

This whitepaper is a distillation of thoughts from three webinars conducted by Berto Sanchez, Senior Director of Threat and Sharing Analysis from Anomali; and Sergio Caltagirone, Vice President of Threat Intelligence for Dragos. These webinars were a part of the Anomali Detect LIVE Virtual Event series. We've included soundbites from the presentations throughout. *For more information about these webinars, see "View Detect LIVE Webinars to Learn More" on page 9.*

Building a strong cyber defense against all the possible industrial threats that could theoretically disrupt an organization's operational technology (OT) infrastructure or assets, is increasingly becoming more challenging for critical infrastructure around the world. There are simply too many threats and never enough money or time to neutralize every risk.

Organizations with industrial control systems (ICS) and OT environments grapple with this increasingly complex task. Three major problems exist that are thwarting their ability to build a solid OT security program:

Increasing Threat Landscape

Dragos analysts are tracking a continuously increasing number of attack groups focused on ICS / OT without any falling off the map. These are not hypothetical boogeymen, these are real attacks that are unfolding worldwide.

- Dragos 2021 Year in Review analysis showed three new ICS-targeting activity groups, bringing the total to 18 focused on OT systems and assets. *(dragos.com/year-in-review)*

Lack of OT Cybersecurity Resources

The growth of attacks and the expanding number of OT systems remotely accessible makes it difficult to ever really have enough resources to bring cyber risk to industrial systems down to zero. It takes prioritization.

- In 2021, external connections to OT spiked upwards, more than doubling to 70%. This increase is likely due to the high demand for remote access in the wake of the COVID-19 pandemic. *(dragos.com/year-in-review)*

ICS Cyber Defense Practices Are Often Immature

Many industrial organizations are still unprepared to detect and respond to the kinds of attacks targeting their OT and ICS assets.

- During 2021, Dragos uncovered that 86% of its services customers had limited to no visibility into their ICS environment. *(dragos.com/year-in-review)*

Modern ICS cyber defense requires focused investment. Luckily, there are resources to do it efficiently. By effectively utilizing threat intelligence and the MITRE ATT&CK for ICS framework, organizations can focus on the threats that matter.

> **We always want to make sure that every dollar we spend is towards the most effective decision we can make. What we can do is we can then basically try to reduce the threat landscape down to a set of behaviors. With sufficient intelligence, we can actually much better manage and understand what adversaries do.**
>
> — Sergio Caltagirone, Vice President of Threat Intelligence for Dragos

THREAT INTEL MAKES INDUSTRIAL CYBERSECURITY MORE EFFECTIVE AND EFFICIENT

Threat intelligence holds the key for not boiling the ocean with industrial cybersecurity investment and activities.

Organizations have to get down to what matters most to them — prioritizing the most important crown jewel assets and protecting against the attacks most likely to target those. This is how organizations ensure they maximize the efficiency and effectiveness of what they spend on cybersecurity monitoring, controls, and response.

Threat intelligence makes it possible for organizations to focus on what matters most by helping them find and protect against the attack patterns that actually impact assets and infrastructure that looks like theirs.

The Importance of Asset Visibility

Visibility into one's own environment lays the foundation for an effective threat intelligence program — whether for IT or OT assets. Intelligence is simply information about how threat actors behave and operate within the environments they target. Threat intelligence programs use that information as a multi-dimensional yardstick to compare what's happening in the outside world against what's occurring within their organization's assets. If there's nothing to compare the intelligence to, then there's no way to effectively use that intelligence.

This is why asset management and monitoring are the first steps to building out an effective OT threat intelligence program. Organizations need to map their OT assets and build monitoring mechanisms that are instrumented to a prioritized set of those assets.

HOW MUCH VISIBILITY IS ENOUGH?

There isn't a cybersecurity analyst in the world who won't ask for more data if they can get it. Ask them how much data they want and they'll say they want it all. Of course, this is not logistically feasible, especially in ICS environments. As organizations decide how much cyber detection visibility they can instrument into their OT systems, they must find a middle ground.

One of the best ways to start understanding whether there's enough visibility in an environment is to answer a simple question. If the board of directors were to ask your team if you can bring the plant online safely and securely after an incident, can you confidently answer them? Would your team be able to have enough data to explain what happened or what didn't happen, or if it was a cyber incident at all? If the answers are no, then there is definitely a need for more visibility.

> **Gaining visibility is not just understanding all the assets that you have. It's also understanding the data sources that are coming in and understanding what those data sources actually mean so you can actually work toward achieving your security outcomes. Because the last thing you want to do is collect all the data and then start missing things because you are unaware of the possibilities that that data source can have for you.**
>
> — Berto Sanchez
> Senior Director of Threat Intelligence of Anomali

Measuring Quality of Industrial Threat Intelligence

As for the intelligence itself, organizations should be seeking industrial threat intel with four traits that can be summed up with the acronym, CART: Completeness, Accuracy, Relevance, Timeliness.

COMPLETENESS:

Complete threat intelligence provides contextual information about how the threat operates within particular attack chains, environments, industries, and technological setups. It also contextualizes the operational impact and risk measurement of the threat to support appropriate prioritization by defenders.

RELEVANCE:

Relevance can be judged not only by the germaneness of the threat to a recipient's technology environment or industry, but also by the appropriateness of the delivery mechanism for their role or mode of working.

ACCURACY:

Consistently inaccurate threat intelligence is worse than no threat intelligence at all. At the same time, perfectly accurate threat intelligence is not going to provide much value either. The best intel operates somewhere in the middle between the extreme of being always right with little new information provided and being cutting-edge but constantly riddled with inaccuracy.

TIMELINESS:

Timeliness is crucial but is the one quality that most needs to be judged in context of the other three. The consequences of action in OT environments are often orders of magnitude more impactful than in the realm of IT. ICS threat intelligence may have a different scale of timeliness in order to ensure higher accuracy and fully reasoned recommendations.

In addition to building out visibility and sourcing threat intelligence with strong CART traits, organizations also need a way to fold the intel into the security program. This is where the MITRE ATT&CK for ICS comes in — industrial organizations use it as a decisioning framework to drive the most effective prevention and response actions across their ICS/OT assets.

THE PYRAMID OF PAIN, CYBER KILL CHAIN, AND MITRE ATT&CK FOR ICS

Before digging into what MITRE ATT&CK for ICS is and how it works, it's important to understand why it was created.

The Shift from IoCs to Threat Behaviors

> **Get away from the malware, get away from the infrastructure, focus on the long-term behaviors. You're going to burn yourself out, you're going to burn your organization out if you're just constantly focused on what IP addresses should I block today? It is not a tenable approach. You could block the entire Internet and you would still get compromised.**
>
> — Sergio Caltagirone
> Vice President of Threat Intelligence for Dragos

There was a time when almost all threat intelligence was primarily focused on indicators of compromise (IoCs). These are usually simplistic technical markers such as IP addresses related to malicious activities which could be used to feed detection and blocking mechanisms. The thing about IoCs is that they're tied to attack elements that are trivial for the threat actors to change — and not even manually. Dynamic infrastructure and polymorphic malware have long made it easy for the bad guys to automate the process of sidestepping detection from IoCs.

As a result, the ultimate objective for good threat intelligence is to move away from IoCs and focus on behaviors. Whereas IoCs are ephemeral, behaviors — the tactics, techniques, and procedures (TTPs) of the threat actors —tend to be longer-lasting because they're harder for the attackers to change.

Defining Attack Stages with the Cyber Kill Chain

This dynamic is best illustrated by David Bianco's Pyramid of Pain, which very elegantly describes the difficulty with which attackers can evade different detection markers:

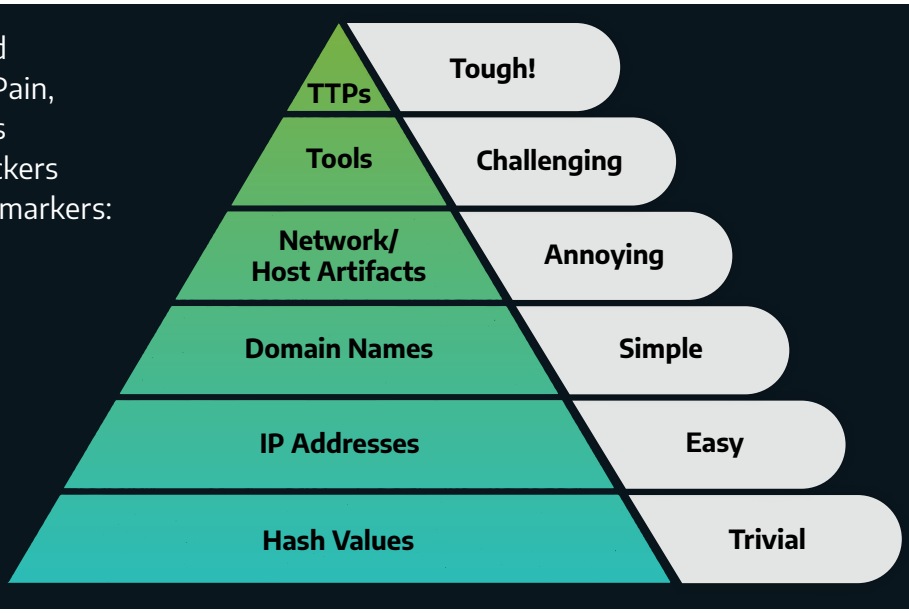

Figure 1: David Bianco's Pyramid of Pain

Behavioral-based detection and defense hones in on the very top of that pyramid. Behavioral-based threat intelligence is more effective because it:

- focuses on real threats
- drives change through real case-studies
- ignores specifics of malware or infrastructure and emphasizes longer term behavior

Behavioral-based intelligence is made even more effective when it is contextualized by where in the Cyber Kill Chain specific behaviors tend to fall. First developed by cyber experts at Lockheed Martin and now co-opted by the broader cybersecurity community, the cyber kill chain describes the stages most attacks go through in order to achieve threat actor's objectives. The idea is that the earlier in the kill chain an organization can detect an attack, the faster it can be neutralized and the least amount of damage that attack can inflict.

Threat intelligence that focuses on behaviors in the cyber kill chain make it easier to find attacks earlier. MITRE ATT&CK for ICS was developed with these principles in mind to start compiling and mapping the behaviors of attackers in the context of the cyber kill chain.

The Role of MITRE ATT&CK for ICS

Developed nearly a decade ago by MITRE researchers seeking to improve detection of post-compromise cyber adversary behavior, MITRE ATT&CK is a high-level knowledge base of publicly observed cyber attacker TTPs. ATT&CK catalogs behaviors — ones that last rather than more ephemeral IoCs. It classifies them and maps them against the stages of the kill chain.

ATT&CK provides a visual framework of attack patterns that can be translated to security tools and actions to detect and respond more quickly to attacks, and even

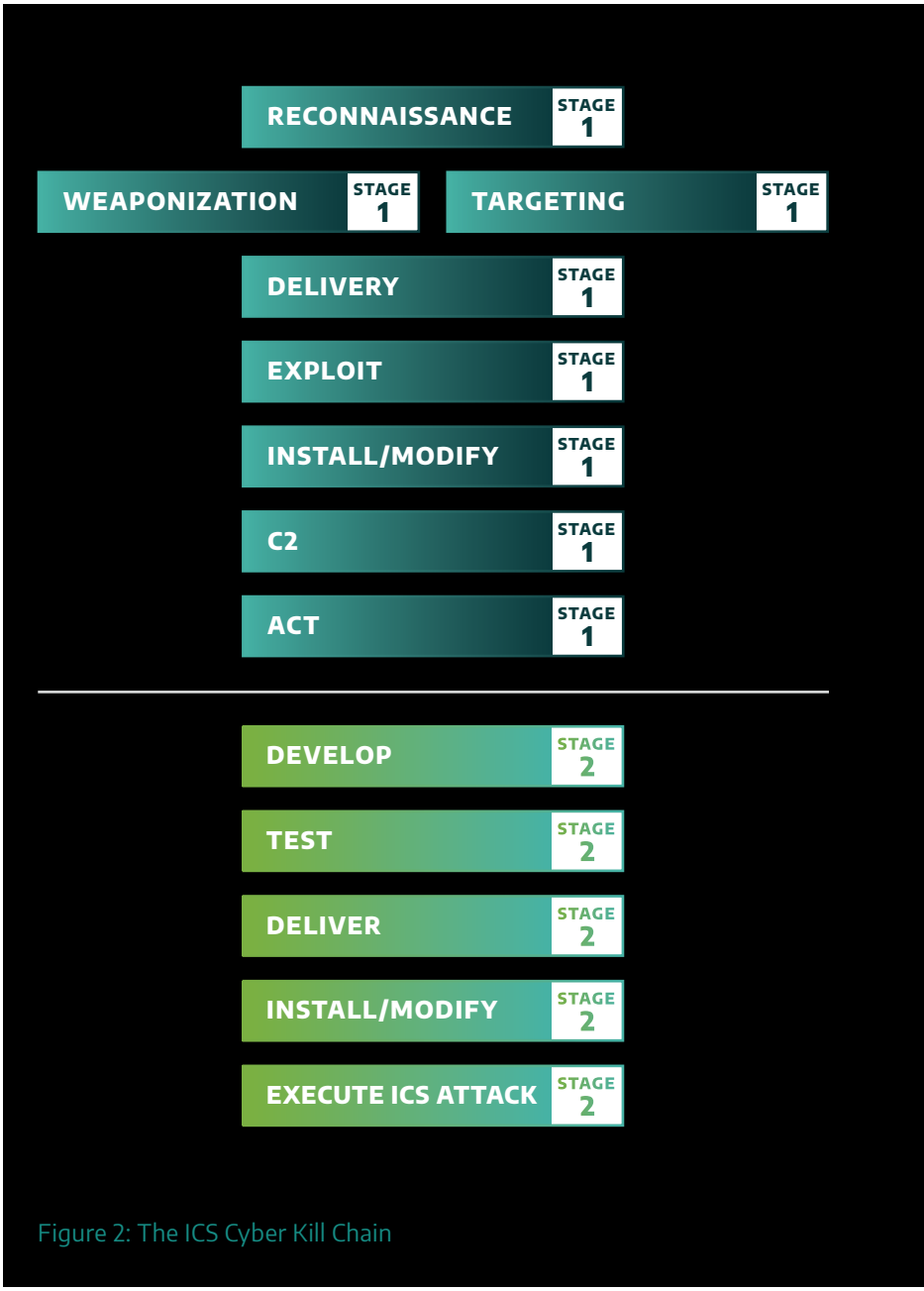

Figure 2: The ICS Cyber Kill Chain

to potentially to build better prevention mechanisms. It also standardizes the way we talk about attackers. Everybody has a name for attackers and their behaviors. ATT&CK provides a common lexicon so everyone knows they're talking about the same thing.

However, ATT&CK was initially written for enterprise IT. As the framework progressed, it became increasingly clear to OT defenders that the TTPs described within simply did not translate well to OT environments. This realization led to a parallel effort by MITRE to build up ATT&CK for ICS. Its mission is exactly the same as for the main framework, but it is purpose-built for incident responders who operate in the unique environments of the industrial world and respond to threats that specifically target these OT systems.

Before this framework, OT network defenders, incident responders, threat hunters, and penetration testers all had to painstakingly collect public and non-public reports from a range of different sources. They had to sift through that data, clean it up, and merge it into their own unique data sets to understand current threat behaviors enough to use TTPs to drive their investigations and defense. Each of these homespun data sets take tremendous amounts of work to develop and maintain, and they are all inconsistent in their coverage. ATT&CK for ICS consolidates and standardizes the format of OT adversary knowledge from dozens of sources.

Attack behavior witnessed by OT analysts suggests that specialized ICS attackers are supported by generalist adversaries who use the similar TTP for initial intrusion into both IT and OT networks. Once they gain a foothold in OT systems, they then turn it over to ICS specialists. As a result, there will always be some overlap between MITRE ATT&CK and MITRE ATT&CK for ICS. The tradecraft citations included within the latter are meant to complete the story of adversary behavior for OT defenders, from initial reconnaissance and intrusion to causing physical damage and disruption of industrial control processes. That includes intelligence on what the view looks like from the asset owner's perspective, including impact on protocols unique to embedded systems, and specialized apps that operators use.

5 Ways to Operationalize MITRE ATT&CK for ICS

MITRE ATT&CK for ICS can be operationalized by OT and ICS cyber defenders in a number of compelling ways. These use cases include:

- informing speedier and risk-prioritized response to attacks against an industrial environment
- improving detection coverage by offering better clues on what the organization should be monitoring for
- using hypothesis-driven threat hunting to find hidden or new threats with similar patterns as those mapped to the framework
- future-proofing ICS security roadmaps by watching changes in attack models tracked by ATT&CK

We recommend five common-sense steps for industrial cyber defenders to start using ATT&CK for ICS.

1 Get Relevant Threat Intelligence

Receiving relevant threat intelligence about ICS/OT environments is the first step. As outlined earlier in the paper, all of the CART characteristics—completeness, accuracy, relevance, and timeliness—are all important traits of the threat intelligence used for detecting and hunting threats today. But for ICS defenders, relevance is perhaps the very most important to them. Using irrelevant data or intelligence for detecting and prioritizing threats in OT environments

not only wastes time, but could actually do more harm than good.

2 Extract Behaviors from Threat Intel

Next, to get real value out of ATT&CK for ICS an organization needs to extract behaviors from that threat intelligence. Ideally you can have a vendor do that for you — it can greatly streamline the process to look for one that can map those behaviors directly to the ATT&CK framework. If this isn't possible, then your analysts should be doing this work.

3 Conduct Regular Threat Hunting

There's been a big drive in the last several years for security analysts to engage in what's called hypothesis-driven threat hunting. The idea is to hypothesize what you think happened or could potentially happen within your environment and do searching throughout to either prove or disprove that hypothesis. ATT&CK for ICS can help teams avoid wasting time with these hunts by providing relevant, targeted ideas for these hunts. They can do this by taking particularly worrying attack patterns that are impacting organizations or assets like theirs, picking a piece of the attack kill chain and looking at the behaviors that happened before or after it. From that point the team can look in both directions for signs that these activities have impacted their assets in similar ways.

4 Test Detection Capabilities Across ATT&CK for ICS Framework

While the bare minimum amount of monitoring data can at least provide enough information to deliver an answer to fiduciaries about the basics of when, where, and how attacks happen, that's just the start. Organizations should consider ongoing work to evaluate whether they can detect the behaviors at every step of the attack kill chain as mapped by ATT&CK for ICS. Doing so is an excellent route for determining if an organization has effective detection coverage in place.

5 Reduce Your Threat Universe

Use threat groups and their associated behavior groupings to reduce your 'threat universe.' Look at the ATT&CK for ICS frameworks and understand what behaviors belong together and which ones are most relevant to your sector, to your asset types, and to your most critical processes. Focus on those behavior groupings to hunt on them, detect them, and build out controls that protect against them in order to most efficiently spend your industrial cybersecurity investments.

Finally, as you work through these steps be vigilant for sea changes in attack modeling. One of the most important things cyber defenders should be paying attention to is changes in the ATT&CK for ICS framework, because when that occurs there are new behaviors or previously unknown behaviors. While IoCs change quickly, TTPs change more slowly and when they do then teams must think of long-term ways to adjust to these major shifts. The good news is that whereas everyone was on their own to look for these shifts in times past, now with ATT&CK for ICS a lot of that work is shouldered by the community.

VIEW DETECT LIVE WEBINARS TO LEARN MORE

You can view the following Anomali Detect LIVE webinars to learn more about strengthening your industrial cyber defense leveraging threat intelligence and MITRE ATT&CK for ICS:

- **ICS/OT and Frameworks Discussion**
- **The Power of Cyber Threat Intelligence Together with MITRE ATT&CK**
- **Prioritize and Strengthen Your Cyber Defense with MITRE ATT&CK and Threat Intel**

ABOUT ANOMALI

Anomali delivers intelligence-driven cybersecurity solutions, including ThreatStream®, Match™, and Lens™. Companies use Anomali to enhance threat visibility, automate threat processing and detection, and accelerate threat investigation, response, and remediation.

To learn more about Anomali, visit **www.anomali.com**.

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries including electric, oil and gas, manufacturing, and mining, and protect mission critical networks including ICS/OT and emerging applications such as the Industrial Internet of Things (IIOT).

Dragos is privately held and headquartered in the Washington, DC area with a regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT WWW.DRAGOS.COM.