MAPPING INDUSTRIAL CYBERSECURITY THREATS TO MITRE ATT&CK FOR ICS

AUTHOR

Dragos, Inc.

APRIL, 2020

EXECUTIVE SUMMARY

MITRE ATT&CK FOR ICS IS A COMMUNITY SOURCED FRAMEWORK FOR IDENTIFYING MALICIOUS THREAT BEHAVIORS, SPECIFICALLY THE TACTICS AND TECHNIQUES OF THE ADVERSARIES, IN INDUSTRIAL CONTROL SYSTEMS (ICS).

When industrial cybersecurity defenders and tools map their detection mechanisms to MITRE ATT&CK for ICS, they are able to more efficiently and consistently anticipate and counter ICS threats.

Dragos significantly contributed to this community-supported knowledge base with findings from our technology customers and insights from our services and intelligence efforts. Dragos maps its technology and services to MITRE ATT&CK for ICS and is the first ICS vendor to fully integrate MITRE ATT&CK for ICS into its platform.

This paper offers information on why and how MITRE ATT&CK for ICS was developed and what ICS/OT (operational technology) cybersecurity practitioners can do to get the most out of this framework.

CONTENTS

EXECUTIVE SUMMARY 2

EVOLUTION IN CYBERSECURITY DETECTION TRIGGERS 4

- NETWORK ANOMALIES CHANGE DAILY 5
- IOCS CHANGE WEEKLY 5
- TTPS CHANGE ANNUALLY 5

WHAT IS MITRE ATT&CK FOR ICS 7

- WHAT IS INCLUDED 8

TAILORING KNOWLEDGE TO ICS/OT ENVIRONMENTS 9

- WHERE DATA COMES FROM 11
- HOW ICS/OT STAKEHOLDERS CAN GET THE MOST OUT OF MITRE ATT&CK FOR ICS 12
- HOW DRAGOS MAPS TO MITRE ATT&CK FOR ICS 13

CONCLUSION 15

EVOLUTION

IN CYBERSECURITY DETECTION TRIGGERS

Regardless of environment, achieving consistent detection of malicious behaviors is one of the perennial challenges in cybersecurity.

Whether targeting information technology (IT) or OT systems, adversaries have long been prevalent. They are adept at changing attack characteristics to stay in front of cybersecurity detection mechanisms.

This continual cycle of evasion has created a need for security researchers and analysts to research and define malicious activity beyond technical elements or anomalies and instead focus on threat behaviors such as tactics and techniques.

As a result, resilient cybersecurity defense teams choose to put less weight in detection based on network anomalies and indicators of compromise (IoCs) and more on threat behaviors.[1]

1 All four types of detection serve important use-cases but indicators and anomalies do not serve the primary use case of threat detection and instead can enrich and amplify detection. Read more in the Four Types of Threat Detection paper: https://dragos.com/resource/the-four-types-of-threat-detection-with-case-studies-in-industrial-control-systems-ics/

NETWORK ANOMALIES CHANGE DAILY

Network anomalies such as protocol behaviors have been used for a long time as a basic way to identify abnormalities to investigate IT and ICS/OT networks. These anomalies are changes in traffic patterns and communications that differ from the "normal" communications but do not provide context as to whether the behavior is malicious or benign. The challenge though is that there are significant volumes of anomalies daily that occur in environments forcing analysts to sift through a lot of alerts without the appropriate context of what they are looking for which leads to alarm and analyst fatigue. Network anomalies can be very useful as a data source for hunting in and for amplifying other forms of threat detection but serve as a weak form of threat detection in and of itself.

IOCS CHANGE WEEKLY

Many IT and ICS/OT cybersecurity vendors have acknowledged the limitations of network anomalies and layered on detection based on slightly more stable IoCs implemented through a variety of methods such as YARA rules. These include signs attackers are using certain malicious IP addresses, hash values, domain names, file paths, and more. IoCs contain a lot of context for an analyst but their effectiveness is entirely up to the adversary; threats routinely leverage victim specific infrastructure and malware and routinely change the technical elements of their intrusions. The exact timeline of changing IoCs are up to the adversary but conceptually it is easy to think of these as weekly changes vs. the daily changes of anomalies. In reality, indicators serve as a valuable data source for forensic investigations and scoping but should not be relied upon as the main strategy for threat detection.

TTPS CHANGE ANNUALLY

The trend in the information security community is that analysts and researchers have moved toward identifying and seeking more persistent and transposable forms of threat detection. This has led to a focus on threat behaviors as a reliable means of detecting threats and their capabilities. These fundamental tactics, techniques, and procedures (TTPs) used by adversaries remain the same even as they switch their tooling, malicious code, and infrastructure to evade detection. Whereas IoCs may change weekly, threat behaviors may persist over months and years. Additionally, threat behaviors are not unique to a specific threat group or malware family but instead describe a style and method of an attack. This allows for a much wider aperture which can detect novel capabilities but provides significant context for an analyst to investigate without being specific to a single adversary or malware sample like IoCs.

Focusing on TTPs can dramatically improve a cyber defender's ability to protect against adversaries. However, it is much more difficult for security analysts and vendors to operationalize their defense around these threat behaviors. Analysts need access to thorough intelligence on threat behaviors, and they need technology that use threat behavior-based detection to tap into this more resilient means of finding adversaries in their networks.

The brain trust at MITRE Corporation recognized the broad need for consolidated information about adversary TTPs to fuel improved analyst operations and better tools across the enterprise. In 2013, MITRE researchers spearheaded a community effort to develop a globally accessible knowledge base of adversary TTPs that were based on real-world observations called the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) for Enterprise. This framework helps many defenders take their threat detection, adversary emulation, protection strategy, and incident response capabilities to the next level.

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

WHAT IS

MITRE ATT&CK FOR ICS

MITRE ATT&CK for ICS is the first ever consolidated encyclopedia of publicly observed industrial adversary threat behavior.

THE MITRE ATT&CK FOR ICS MATRIX

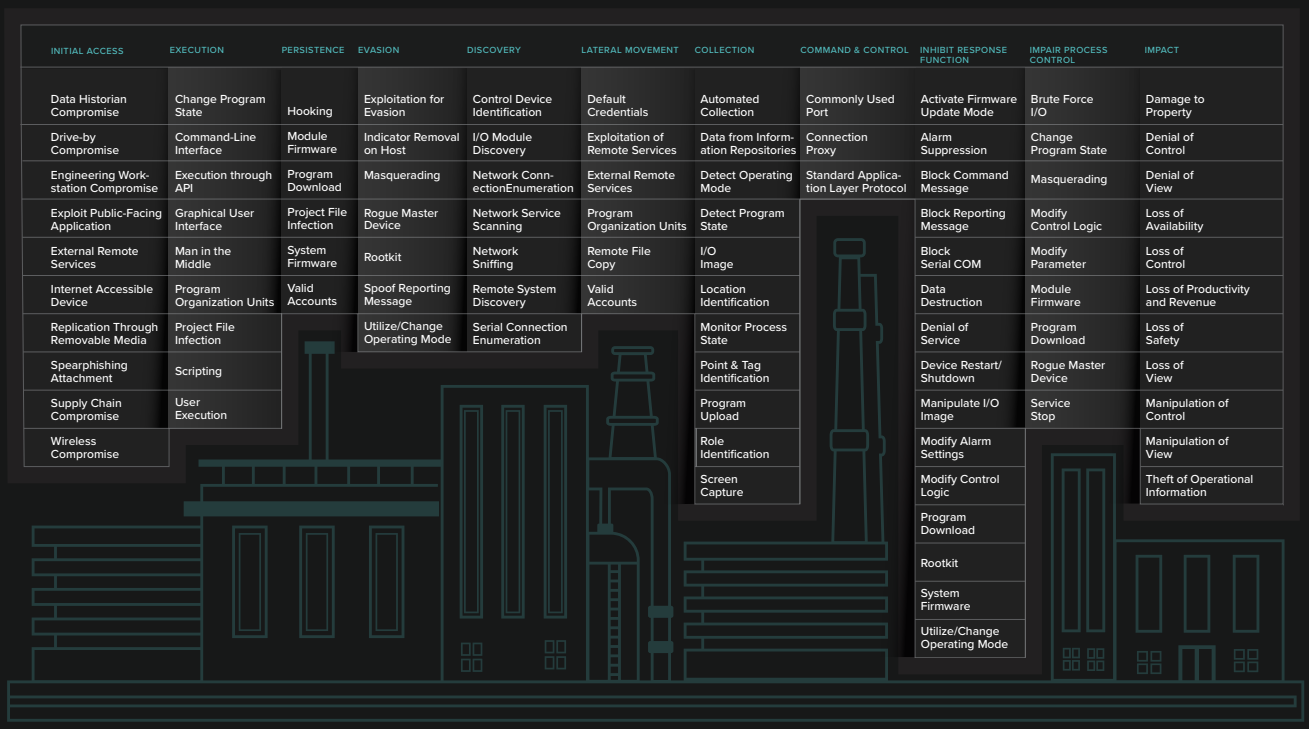


Figure 1: The MITRE ATT&CK for ICS Matrix

Before this framework, ICS/OT network defenders, incident responders, threat hunters, and penetration testers had to painstakingly collect public and non-public reports from a range of different sources and attempt to communicate across various lexicons. They had to sift through that data, clean it, and merge it into their own unique data sets to understand current threat behaviors 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.

MITRE ATT&CK for ICS completely changes the game by consolidating and standardizing the format of ICS/OT adversary knowledge from dozens of sources. Dragos contributes greatly to the effort, but Dragos is just one of 33 others that participates in the framework's development and it is worth acknowledging the significant value in a community-sourced effort and the contributions of many. Together they feed the framework with the intelligence necessary to establish the fullest picture available of today's industrial adversary landscape.

The comprehensive and well-organized knowledge base offered by MITRE ATT&CK for ICS helps defenders uncover the unique threat behaviors used by adversaries targeting ICS environments and does so without requiring defenders to put extra work into organizing this data.

WHAT IS INCLUDED

One of the biggest challenges for ICS/OT network analysts is understanding detection coverage. MITRE ATT&CK for ICS serves as a single resource that covers all the publicly known ICS threat behaviors recorded today. ATT&CK contains hundreds of ICS adversary tradecraft citations that cover not only commonly used ICS software malware tools but also tactics and techniques.

TACTICS

This is the most common operational goal of industrial attackers, including data collection, command and control, inhibiting response function, and impairing process controls

TECHNIQUES

These encompass the most common methods used to achieve those goals, such as automating data collection, commonly used ports to establish C&C, alarm suppression, and modifying control logic.

The framework sets these up as a matrix of broad tactics that provide buckets that are filled with more specific attendant techniques.

The tradecraft citations included within the framework are meant to complete the story of adversary behavior for ICS/OT defenders, from initial reconnaissance and intrusion to causing physical damage and disruption of industrial control processes. This story 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.

TAILORING KNOWLEDGE

TO ICS/OT ENVIRONMENTS

In developing MITRE ATT&CK for ICS, MITRE, community contributors, and Dragos acknowledged that conceptually ICS security is one-quarter IT security and three-quarters engineering and operations discipline.

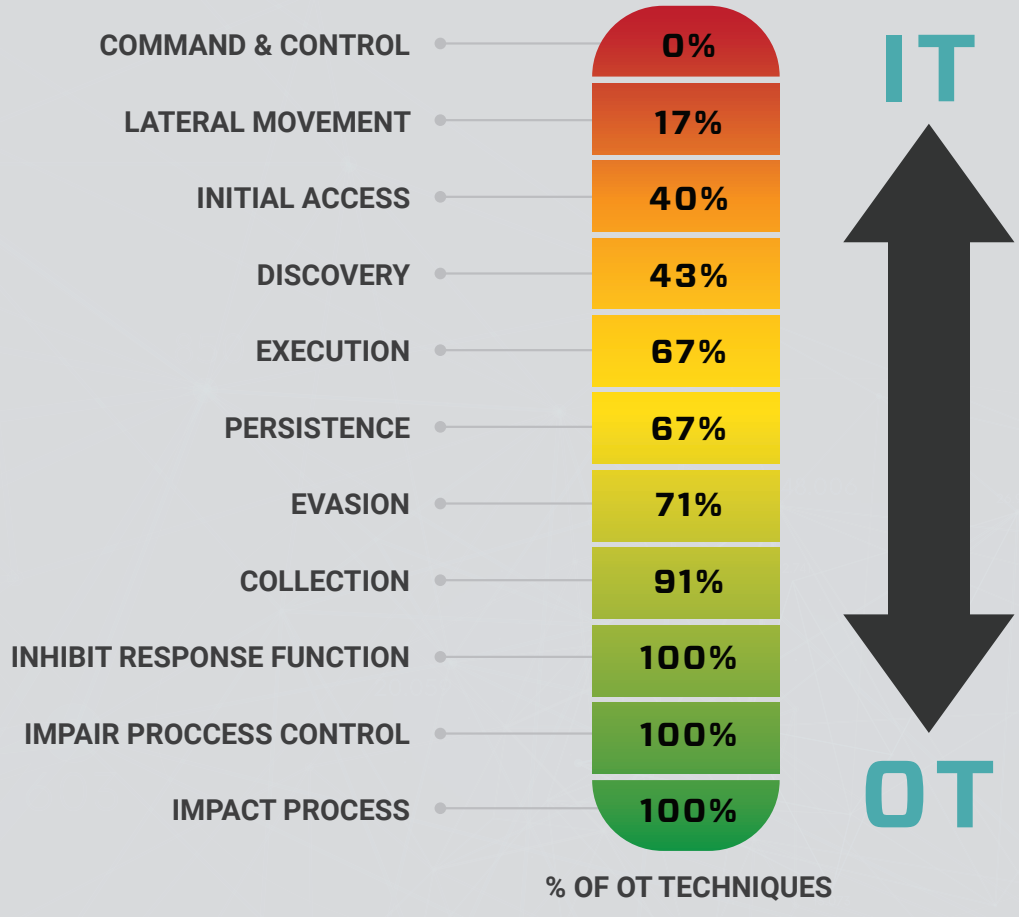
The reality of ICS and its interaction with the physical world require both adversaries and defenders to take different approaches than they would in the attack or defense of enterprise IT networks.

Dragos' experts saw in an initial analysis of the framework that 73% of the techniques detailed within were applicable only to ICS/OT environments. MITRE is working to strike a balance and reduce overlap between MITRE ATT&CK for ICS and ATT&CK for Enterprise. Defenders should be mindful of the overlaps and use this opportunity for increased coverage. Not all efforts in IT are useless to ICS and vice versa, but by leveraging the right approaches and tools for the right problems, defenders will achieve more reliable and repeatable successes.

MITRE ATT&CK for ICS will remain primarily focused on techniques that are only applicable to ICS/OT environments, although it is still essential to understand how the adversary entered the network and maintained communications. It is essential to understand how the adversary entered the network and maintained communications. At Dragos, the behavior witnessed suggests that specialized ICS attackers are often supported by generalist adversaries who sometimes use similar TTPs for initial intrusion into both IT and ICS/OT networks. Once adversaries gain a foothold in ICS/OT systems, they then turn it over to ICS specialists. This is not always the case though, and there are unique intrusion access methods such as those that take advantage of specialized communication links, networks, and interconnections with vendors and integrators of the asset owner and operators supply chain.

There will always be some overlap between the two frameworks. However, the only general IT TTPs also included in MITRE ATT&CK for ICS are the ones leveraged by the ICS adversary groups that target these environments. This leads to a prioritization of those efforts for defenders.

Figure 2: Percentage of OT Techniques



WHERE DATA COMES FROM

The data collated into the MITRE ATT&CK for ICS framework comes from data presented in public incident response and threat intelligence reports about real-life attacks that have unfolded in ICS environments. MITRE dedicates a team of full-time analysts to parse through reports, newsletters, and other updated intelligence feeds to integrate new tactics and techniques that comprise the most common parts of the ICS Cyber Kill Chain. They work to extract technical details from each data source and integrate those into the framework on a daily basis. By keeping specifically to what has actually happened in the world instead of focusing on the art of the possible the framework centers defenders on practical and prioritized threat behaviors.

One note to remember is that the data set used to build MITRE ATT&CK for ICS is understandably smaller than ATT&CK for Enterprise. First of all, most ICS defenders still do not have a lot of visibility into those environments and do not have the same level of forensic data that can be leveraged by the organization or its security vendors to understand exactly how the ICS Cyber Kill Chain unfolded. Additionally, these are very sensitive environments and organizations are still not likely to share public information. ICS security incidents are largely dealt with quietly and threat intelligence still remains private to protect the organization and not to alert adversaries in the environment that researchers are now aware of a new TTP.

It is necessary to remember that the data within ATT&CK still has its limitations. Nevertheless, it is the best resource the ICS security community has ever had and is getting better as it grows.

HOW ICS/OT STAKEHOLDERS CAN GET THE MOST OUT OF MITRE ATT&CK FOR ICS

MITRE ATT&CK FOR ICS CAN OFFER TREMENDOUS BENEFITS TO A RANGE OF CYBERSECURITY STAKEHOLDERS TASKED WITH PROTECTING ICS/OT ENVIRONMENTS.

SECURITY ANALYSTS

MITRE ATT&CK for ICS offers valuable insights to security analysts within the ICS/OT security operations center (SOC). It offers a centralized resource to gain a solid understanding of ICS/OT adversary tradecraft. It also provides standardization in lexicon about attacks for consistent reporting and analysis across organizations and across the security industry. It is a valuable resource for analysts challenged to test and understand their coverage of detection. If analysts see techniques for which they have no mechanism to detect, they will know they need to push for targeted improvements.

INCIDENT RESPONDERS

The framework's library of enumerated threat behaviors can help tremendously with incident response (IR) triage efforts. IR can lean on MITRE ATT&CK for ICS to track specific ICS tradecraft across the cyber kill chain and to develop IR playbooks based on automated detection of particular ICS adversary TTPs.

THREAT HUNTERS

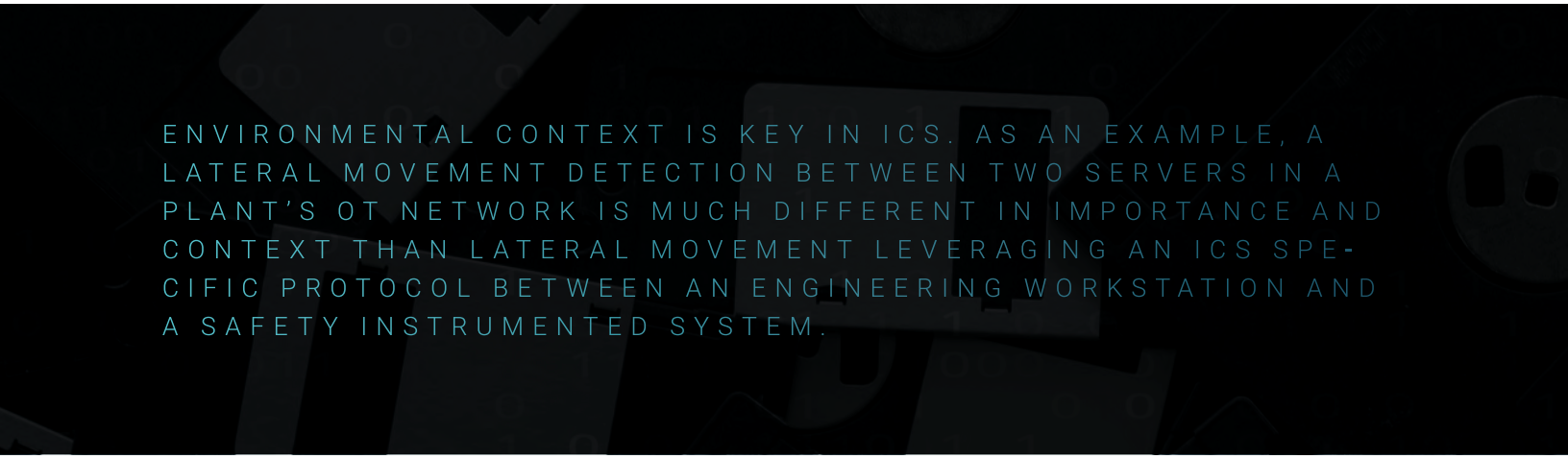
Proactive threat hunters can use MITRE ATT&CK for ICS to drive hunts in ICS/OT environments by using threat behaviors listed in the framework that will not necessarily be unearthed through automated detection. It provides more places for adversary hunters to look for behavioral patterns or other signs that could be contributed to further investigation and to find evidence of stealthy attacks.

PENETRATION TESTERS

Penetration testers can use MITRE ATT&CK for ICS to emulate threat behaviors of known ICS adversaries to help them test defenses and validate detection coverage. Similarly, red teams can lean on the framework to more realistically simulate attacks that help their blue team defenders improve their response capabilities.

C-SUITE

The C-suite can reap big benefits from the framework. Security executives can use MITRE ATT&CK for ICS to help prioritize which security initiatives to invest in next, which security efforts they should develop, and ultimately be able to understand the coverage against threats their investments translate to so that they may communicate it outside of security jargon.



ENVIRONMENTAL CONTEXT IS KEY IN ICS. AS AN EXAMPLE, A LATERAL MOVEMENT DETECTION BETWEEN TWO SERVERS IN A PLANT'S OT NETWORK IS MUCH DIFFERENT IN IMPORTANCE AND CONTEXT THAN LATERAL MOVEMENT LEVERAGING AN ICS SPECIFIC PROTOCOL BETWEEN AN ENGINEERING WORKSTATION AND A SAFETY INSTRUMENTED SYSTEM.

Asset identification and threat detection in this way are best combined together especially for the purposes of ICS security.

Network traffic analysis will give organizations the biggest benefit when using MITRE ATT&CK for ICS. Currently, approximately 62% of the techniques described in the framework can be covered just through network traffic. Network based visibility and monitoring is critical as well to understanding and detecting abuse of native functionality in systems which are techniques leveraged by the most disruptive attacks, such as CRASHOVERRIDE and TRISIS, seen to date. To maximize coverage, organizations should also be looking to their event logs through host-based collection mechanisms. There is overlap between host-based collection and network traffic analysis, but 17% of the techniques detailed in MITRE ATT&CK for ICS can only be reliably seen through host-based collection.

HOW DRAGOS MAPS TO MITRE ATT&CK FOR ICS

BY FOCUSING ON THREAT BEHAVIORS, NETWORK DEFENDERS ARE ABLE TO CREATE DETECTIONS WITH HIGH DURABILITY AND CONTEXT THAT ALSO INCREASES THE LONGEVITY AND THUS RETURN ON INVESTMENT OF THE EFFORTS.

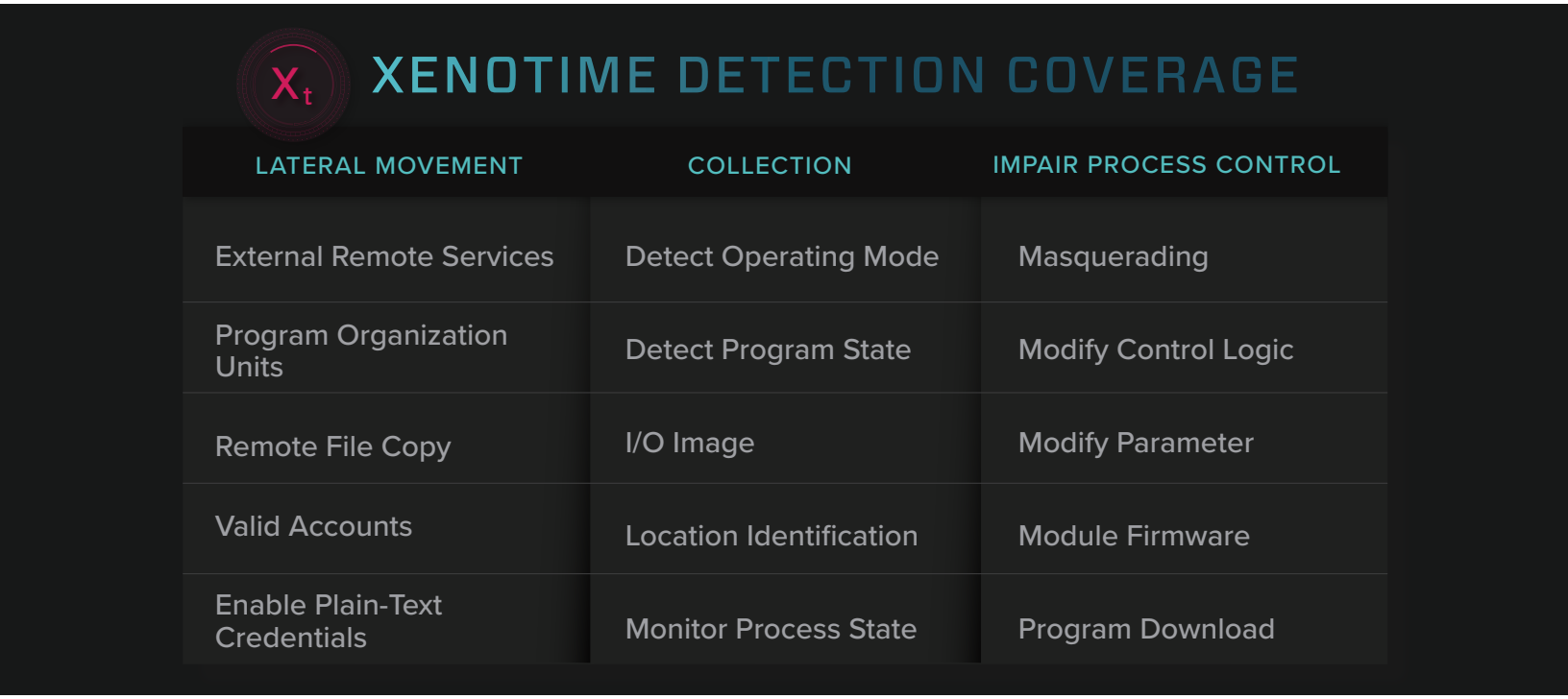
As an organization, Dragos is firmly committed to the philosophy of improving ICS/OT threat detection by shifting toward threat behavior-based detection mechanisms. Dragos believes the future of industrial security depends on more effective operationalization of TTP-based detection.

Internally at Dragos, teams leverage the MITRE ATT&CK for ICS framework. For example, the Professional Services team leverages this as part of adversary simulation exercises to ensure the simulations mirror real-world TTPs. The Dragos Intelligence team is actively involved in the development of the framework's tactics and techniques matrix itself, and provides feedback on the tactics and techniques as they align with the ICS activity groups tracked by Dragos.

Most importantly, the Dragos Platform has utilized this matrix to map detection coverage breadth and detection depth. Dragos is the first ICS vendor to fully integrate ATT&CK for ICS into its platform and the only ICS specific technology on the market that leverages threat behaviors as the core detection mechanism. Sometimes Dragos cannot contribute non-public tactics and techniques that it found for the sake of customer privacy and to avoid widespread proliferation of newer TTPs. However, Dragos is able use TTPs to enhance its own internal ICS ATT&CK framework and create detections for TTPs not yet publicly identified to give our customers increased coverage. Together with the coverage provided by ICS ATT&CK coverage, this proves a potent tool in the approach to securing ICS.

What does that platform-based detection look like in action? One of the classic public cases includes the activity group XENOTIME, which was responsible for the TRISIS malware that targeted ICS safety systems. All of the TTPs used by XENOTIME can be traced to individual tactics and techniques within the MITRE ATT&CK for ICS matrix:

Figure 3: XENOTIME Detection Coverage



With the framework's matrix powering the Dragos Platform, any time a customer witnesses multiple individual detections from the XENOTIME TTP profile, they will be alerted to start investigations into other XENOTIME-like behaviors. This means that a defender would not only have detections, but understand their priority and have enough context to piece together other alerts and information to fully detect the intrusion and respond to it correctly. This also means that defenders are protected not only against the XENOTIME group but all other groups that leverage XENOTIME-like behaviors. Every time an attack is observed and documented into a new threat analytic in the Dragos Platform customers gain increased coverage against all future similar attacks. Removing entire styles of attacks from an adversary's toolkit is a powerful way to give defenders the upper hand.

CONCLUSION

Adversaries evolve threat behaviors slowly over time. Prioritizing behavioral threat detection provides longer lasting and more comprehensive detection than simply relying on anomalies or indicators. By leveraging the MITRE ATT&CK for ICS Framework, Dragos measures and maps threat detections in the Dragos Platform to visualize coverage and gaps and provide ICS/OT cyber defenders a comprehensive ICS detective map to identify malicious behavior and understand adversaries more in-depth than ever before.

TO LEARN MORE ABOUT HOW THE DRAGOS PLATFORM UTILIZES THE MITRE ATT&CK ICS FRAMEWORK, CONTACT US AT INFO@DRAGOS.COM.