DRAGOS

An Executive's Guide to ICS/OT Incident Response

DRAGOS

OT Cyber Incidents on the Rise

Operational technology (OT) risks are on the rise, with more threat actors and incidents targeting industrial organizations by the day. Even when organizations invest in preventative OT cybersecurity controls, cybersecurity incidents are an inevitability. Coupled with emerging policy and worldwide regulations calling for increased executive responsibility and more corporate transparency in reporting cybersecurity events, an appropriate incident response has never been more crucial to industrial cyber resilience.

Unfortunately, many ICS/OT organizations struggle to prepare for and recover quickly from incidents in their environments. Recent reports show that most organizations who tested their OT incident response preparedness faced at least some challenges in five out of seven core response capabilities. What's more, 80% of organizations face a lack of visibility across OT networks, that make detections, triage, and response incredibly difficult at scale.[1]

80%
OF ORGANIZATIONS FACE A LACK OF VISIBILITY ACROSS OT NETWORKS

As industrial organizations seek to improve those numbers, one of the most important considerations they need to keep in mind is that OT cyber incident response is not a simple add-on to an existing IT incident response program. The unique nature of OT environments requires an incident response plan and program that are specifically tailored to OT risks.

It takes thoughtful and OT-specific planning, consistent testing, and significant expertise to develop an effective and rapid OT incident response capability.

How Cyber Incident Response is Different in OT

While some of the basics of incident response are universal across IT and OT environments, the truth is that OT incident response takes a whole other level of preparation and readiness compared to IT. That's because OT incident response is called to respond to different risks, with a different approach, and with different expertise and tooling.

1 Dragos "2022 ICS/OT Cybersecurity Year in Review" Report, **dragos.com/year-in-review**.

DRAGOS

Different Risks

The stakes are so exceedingly high when cyber incidents strike industrial environments because OT systems are inextricably tied with physical world.

These systems are designed to run everything from machines and robots in manufacturing facilities to pumps and valves at water stations to electrical grid equipment run by power plants.

OT = IT + Physics

This means that cyber incidents that impact these OT systems can also have very real physical consequences.

Most drastically, they can threaten human and environmental safety. OT cyber incidents can also make a material impact on operational uptime. Consequently, every minute they remain ongoing can directly affect revenue.

This means that the risk management goals of an OT incident response team are going to be vastly differentiated from those of an IT-focused team.

Different Approach

And that's just the start of the differences. On top of that, OT incident responders must be able to effectively:

- interact with systems from which forensic data must be collected differently to maintain stricter operational and uptime requirements
- triage systems without shutting them down or disconnecting them the way IT systems can be disabled during an ongoing incident
- examine activity for systems that use different protocols and technology into which typical IT forensic tools offer little to no visibility
- bring enough OT network expertise to the table to understand what abnormal activity looks like and when their actions may do more harm than good for system stability

An incident may not be limited to a single location, process, or system. Since OT environments have the additional risk element of physical, safety, and environmental concerns, it is important to prioritize a response plan before operational down time due to an incident. Given these factors, the reality is that OT response plans cannot be copied and pasted from the IT incident response playbook.

Traditionally speaking, it is unlikely that IT incident responders will be equipped to hit the ground running in an ongoing OT incident response crisis when working from an IT incident response playbook.

An IT staffer isn't usually trained to be able to walk up to an ICS historian or a PLC and know what to touch, what to examine, and what can or cannot be shut down to do a forensic collection.

There are simply too many physical consequences at play that an untrained IT team would never know about. Additionally, OT incident responders approach digital forensics differently than IT, using threat intelligence to guide a hypotheses-driven response to analyze the root cause.

It's also important not to overlook details in OT incident response like familiarity with Personal Protective Equipment (PPE) – even something as simple as wearing compliant shoes and a hardhat could be something an IT incident responder isn't accustomed to or prepared for.

Clearly, industrial organizations need to make specialized OT incident response plans, practice them, and prepare to execute on them with the right set of tools and expertise at their fingertips. Doing so is crucial for industrial organizations seeking to effectively manage cybersecurity risks in today's threat landscape.

DRAGOS

Why a Consequence-Driven Plan is the Foundation to OT Incident Response Readiness

While preparation ahead of an incident is always core in either IT or OT incident response, it is much more important in OT incident response because of the unique nature of the environments and questions to be answered.

Some considerations:

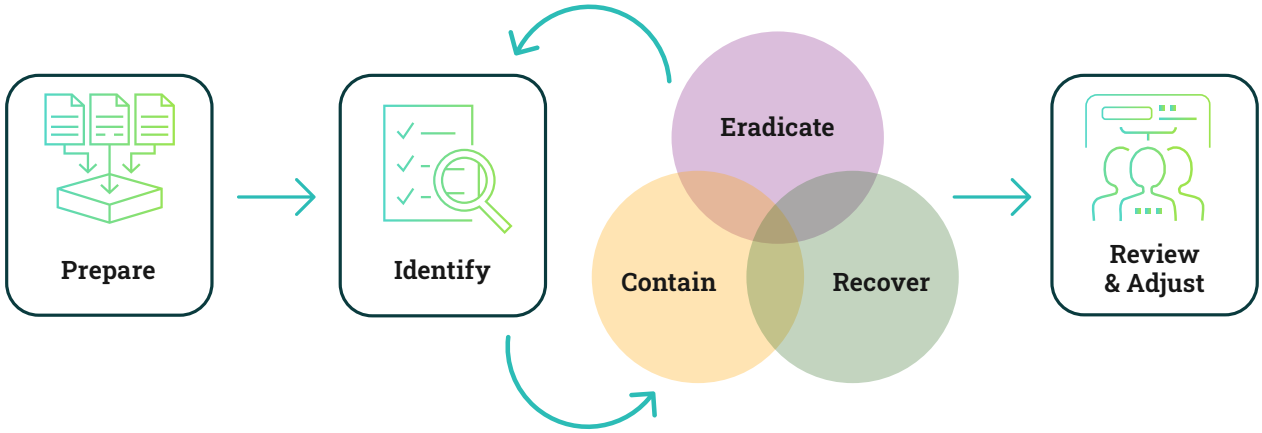
- Many of the questions that organizations want answered are best answered through OT network traffic analysis that cannot be obtained after the attack if the environment was not configured to collect that data, or the tools used to provide those insights had not been deployed prior to the incident.
- Because the safety and reliability of ICS operations is the priority, forensic data collection often has to take place over an extended period of time. As a result, some important data may be overwritten, so teams need to ensure their continuous network monitoring is tuned to keep tabs on ICS operations with this in mind.
- In most cases, the collection of forensic artifacts from hosts in ICS environments is a manual process, requiring teams to weigh the potential impact of this process against the downtime of systems that control important physical processes.
- Many organizations struggle not only with detection of incidents due to the lack of monitoring capabilities, but they also have difficulties knowing when an event qualifies as an incident or needs to be escalated for action by either OT or IT teams.
- The cultural and operational divide between OT and IT engineers means that teams will struggle to communicate and work together unless they have guidance and playbooks set out in advance, for the necessary communication pathways and decision making required during common incidents.

These are just a few reasons why a solid incident response plan (IRP) is so foundational to the success of an effective OT incident response function within an OT cybersecurity program. The development of a plan helps organizations actively think about the OT cyber incidents most risky to them and plan their course of action should these events occur.

As you can see below, the lifecycle of incident response revolves around the development of the IRP.

Writing the plan should not be a one-and-done affair. An effective IRP is a living document that is constantly adjusted based on lessons learned through these experiences. These adjustments can be made based on both incident post-mortems and tests like tabletop exercises (TTXs).

The Lifecycle of Incident Response



In the first stages of IRP development, organizations shouldn't try to boil the ocean and create a plan that covers every possible scenario that they can think of. The idea is to tailor a plan to your industry and the most common and dangerous incident risks that organizations like yours are likely to face. Identify the common incidents that are most likely to cause the biggest safety or financial consequences and start with those. Plan the contingencies for these high-impact incidents first and then iterate from there.

Some of the risks to consider when thinking through consequences that drive the IRP should include:

- Environmental and human safety risks
- Legal considerations
- Regulatory mandates
- Insurance considerations
- Supply chain and third-party risks

Every organization's OT IRP will look different, but most plans should offer guidelines, documentation, and best practices for the organization in nine important areas:

Roles and Responsibilities

Risk Management, Triage, and Escalation Decision Making

Selected IR Lifecycle (NIST, SANS, PICERL, etc.)

Categories of Incidents and Workflows

Isolation Plan

Communication Plan

Regulatory and Legal Requirements

Internal and External Resources and Contacts

Supporting Forms and Documentation

The process of writing and continuously updating a consequence-driven OT IRP should be a highly collaborative affair. Because the execution of the plan will depend on a full roster of executive, IT, OT, and cybersecurity involvement, all of these stakeholders need to be involved to lend their expertise and advice on why and how certain procedures should be followed.

Why Existing Incident Response Capabilities Won't Work

Often just the very process of trying to write an OT IRP will highlight the biggest challenge that industrial organizations face in running an OT incident response program. Namely, getting operational engineers and IT cyber incident responders on the same page—philosophically and operationally. Often getting these teams to agree on procedures and policies is hard enough—let alone regularly coordinating them to execute on these plans.

Because OT=IT+Physics, OT cyber incident response requires a blend of expertise that bridges the knowledge and cultural space of the IT and operational engineering teams. Internal cyber incident response teams can rarely bridge that gap on their own, even with the addition of a new hire or OT-focused tool. The hybrid specialization required to quickly and effectively respond to OT cyber incidents makes this a field where it is incredibly cost-prohibitive to build that bridging capability internally. These kinds of experts are incredibly rare and expensive to keep.

This means that the most cost-effective approach is to seek outside help. Now, the next logical question that many executives ask is:

"Can't my existing IT incident response retainer handle this?" Most times, the answer is 'No.'

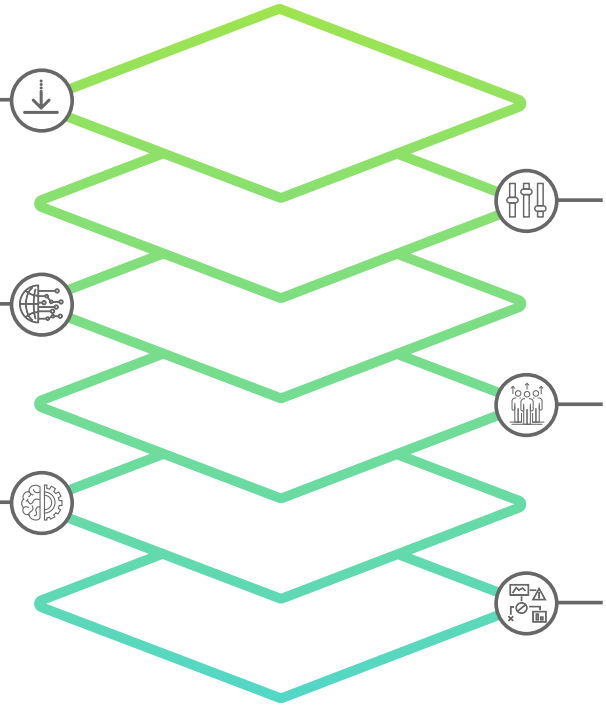
That's because IT incident response retainers are not designed for managing the risks of physical consequences. Organizations need a retainer relationship with a specialized firm that can supply OT-focused experts, armed with OT-capable tooling who are fully aware of the physical consequences of not only the incident itself but the forensic and response actions of the team. Only a team like this can help an industrial organization at every stage of OT incident response preparedness.

This includes:

Establishing the baseline and doing risk assessments and response planning

Operationalizing the IRP

Running practice incident scenarios and helping the organization learn from them (and from actual incidents) to improve the security roadmap and ongoing program



Putting controls and platforms in place that will help the team collect forensics and get good visibility into how an incident occurred/is occurring

Standing by as a team ready for when incidents strike

Optimizing controls and plan based on lessons learned

DRAGOS

The Role of an OT Incident Response Retainer in an OT Cybersecurity Program

Often executives see an OT incident response retainer as a back-up insurance policy for potential worst-case scenarios. However, a well-planned retainer can act as an important lynchpin for the design of not just the incident response program but also the broader OT cybersecurity program.

Laying the Foundation of Cyber Preparedness

An incident response retainer guides some of the most critical support actions for OT incident preparedness. First, it provides a chance to assess organizational cybersecurity maturity and evaluate the organization's preparedness, establishing a baseline. A retainer also formalizes procedures between OT, IT, and executive stakeholders – strategic and a practical level what the goals are for risk management, what the roles are during an incident, how and when calls are made to escalate incidents to the executive level These discussions will aid collaborating not only in incident response and crisis management, but also fostering longer-term relationships between the IT and OT executives that may not have been strong before. it's essential that there is a communication plan in place, with processes and procedures established so that teams aren't scrambling to figure out who's doing what and how to engage when an incident occurs.

Taking the time to evaluate and plan on the front end directly speeds up recovery during the heat of an event. It can make all the difference between an inevitable cybersecurity breach attempt, or something that costs millions of dollars and makes the cover of the Wall Street Journal for all the wrong reasons.

> After all, often the first questions executives field from the board when incidents occur are:
>
> Did you have a plan? Did you have a retainer? Did you address all the requirements from a legal and regulatory perspective?
>
> Having a retainer in place with a provider that has OT cybersecurity expertise helps risk managers answer these questions with confidence and meet expectations for appropriate due diligence.

Optimizing OT controls and procedures

Ideally, organizations should set aside some retainer hours to utilize for testing and optimizing their plans and security controls. A flexible retainer arrangement will allow an organization to burndown retainer hours on other services, such as a tabletop exercise, or an architectural review of the network to better understand your most critical systems. Additionally, when incidents do occur, the retainer partner should be providing reports on lessons learned.

All of this can directly be fed back into the incident response program and the OT cybersecurity program to optimize OT protection, visibility, and processes to prepare for future incidents.

Practice Makes Preparation for the Imperfect

Tabletop exercises (TTXs) are an excellent use of incident response retainer resources. TTXs demonstrate how a realistic attack might occur in your industrial environment, so participants can practice how they would respond, gaining a better understanding of strengths and weaknesses in incident response capabilities.

Here's an example of what a TTX scenario might look like:

Operations staff report one of the operation stations is running very slowly, and some popups display and then disappear. They also mention that a vendor stopped by last week to show off a new feature on the system. To demonstrate the new feature, the vendor plugged in their laptop to access a page, but didn't make any changes to the systems. The operation station is still running, however seeing the popup windows displayed, the operators no longer have control abilities. While communicating with their IT support about the unexpected system behaviors, the stations around the plant begin rebooting into safe mode. After a few minutes, the computers display a screen saying the computer files are locked.

Stakeholders would be called to practice their knowledge with this example. They'd be asked questions like:

- At what point would this be considered an incident?
- Can the site be safely run without these stations (manual mode)?
- Is there a procedure, playbook, or guide for this type of issue?
- Are the systems backed up? At what point would senior leadership be notified, and do they know their responsibilities if your company is ransomed?

The answers would be used to put together a report on how the team answered, what strengths and weaknesses were uncovered, and how the IRP could be adjusted accordingly.

DRAGOS

What to Look for in an OT Incident Response Retainer

As industrial organizations seek out a partner to help them fill the gaps in their OT incident response capabilities, they should try to seek out a trusted advisor that can offer:

An industry-based approach to risk

Experienced responders with good judgement under extreme pressure

Operational environment safety and forensic cybersecurity expertise

Cross-functional understanding of OT incident stakeholders

The ability to leverage technology that makes sense in an OT environment

Dragos Rapid Response Retainer

The Dragos Rapid Response Retainer services provides 24x7 access to an industry-leading team of OT cybersecurity experts who provide customers around the globe with the response and cyber resilience support they need to get back to business quickly.

We specialize in helping organizations with industrial environments navigate intrusions and incidents, providing responders who not only understand your OT technology, but also have situational awareness and crisis management experience.

DRAGOS

How it Works

Dragos Rapid Response Retainer provides a 24x7 team of responders experienced in OT crisis management. Retainer engagements include the following:

Readiness Assessment

Every retainer engagement begins with a Readiness Assessment as part of an onboarding workshop, to assess current incident response preparedness. With a baseline established, the Response team at Dragos can make strategic and tactical recommendations tailored exactly to an organization's progress in their OT cybersecurity journey. This includes improvement suggestions for the IRP, controls, and forensic processes.

Rapid Response with the Dragos Platform

A subscription to the Dragos Platform is not required to purchase a retainer, but it is highly recommended. The Dragos Platform provides the continuous visibility to OT devices, profiles, traffic patterns, vulnerabilities and threats that equips responders to better analyze, investigate, and perform root cause analysis when an event occurs. Sites with Platform installed benefit from a guaranteed response time that varies depending on the number of retainer hours purchased.

Flexible Retainer Hours

Dragos provides a range of Rapid Response Retainer tiers, pricing, and burndown options. Every tier offers the flexibility to burndown unused hours through Dragos Global Services that include:

Tabletop Exercises

Architecture Reviews

Capability Maturity Assessments

Network Vulnerability Assessments

To learn more about the Dragos Rapid Response Retainer, contact sales@dragos.com.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.