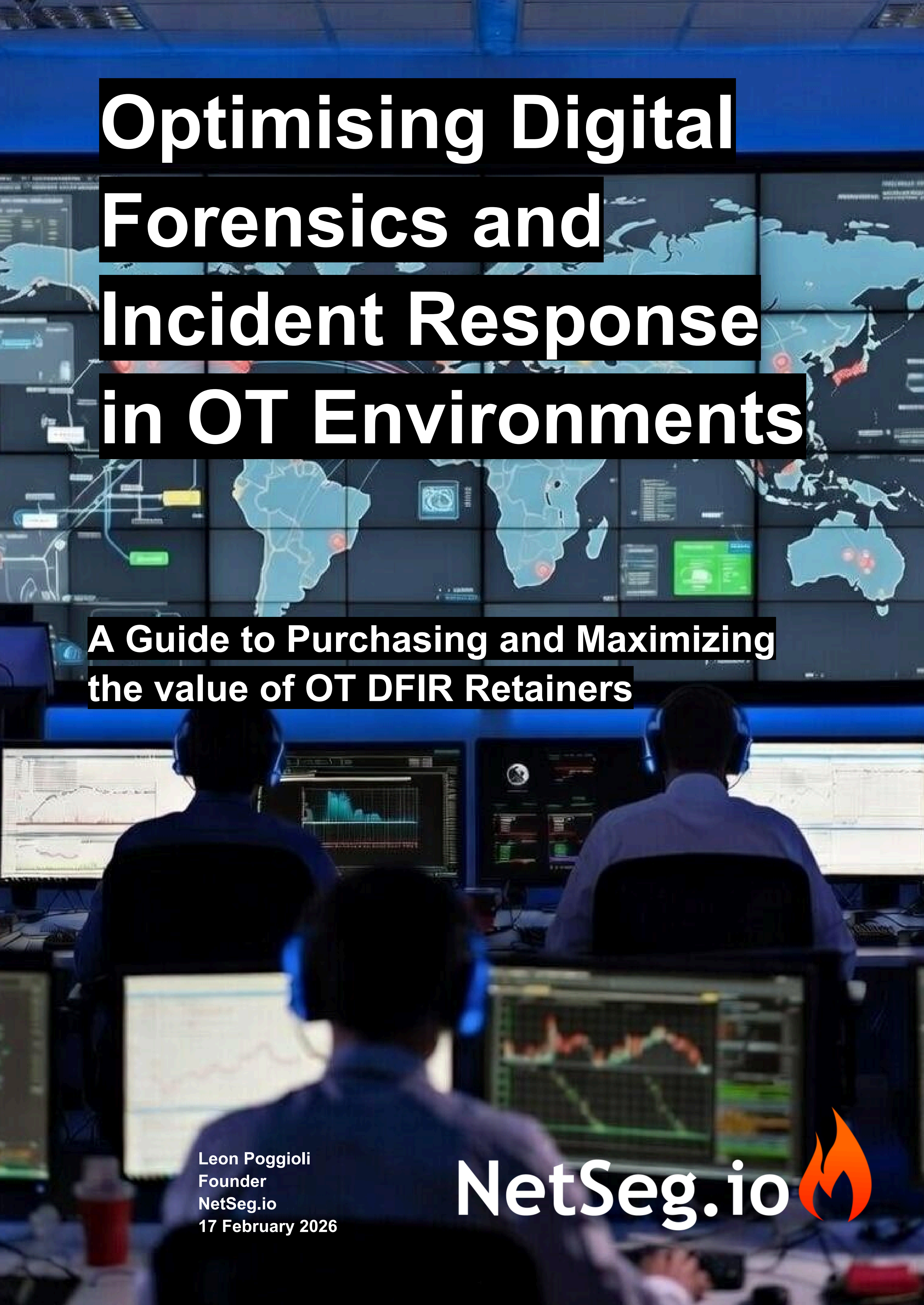
Optimising Digital Forensics and Incident Response in OT Environments

A Guide to Purchasing and Maximizing the value of OT DFIR Retainers



Leon Poggioli
Founder
NetSeg.io
17 February 2026

NetSeg.io

Optimising Digital Forensics and Incident Response in OT Environments

Executive Summary

In an era where cyber threats to operational technology (OT) systems are escalating, organizations must prioritize rapid and effective incident response. OT Digital Forensics and Incident Response (DFIR) retainers provide a proactive solution by securing expert support on standby, ensuring minimal downtime during crises.

This guide explores the fundamentals of purchasing these retainers, key considerations for selection, and strategies to extract maximum value. By focusing on flexible models like hour-based buckets and adaptive usage, businesses can enhance resilience while optimizing costs. Drawing from industry best practices, it highlights how forward-thinking approaches can transform retainers from reactive tools into strategic assets for ongoing security enhancement.

Introduction

Unlike traditional IT systems, OT environments demand specialized handling due to their real-time operations, legacy systems, and potential for physical safety impacts. Cyber incidents in OT can lead to production halts, equipment damage, or even threats to human life.

It is for these reasons that organisations operating OT networks require DFIR capabilities with deep OT domain expertise - not just to investigate an incident, but to recommend courses of action that don’t jeopardise Safety, Reliability, or Productivity of these systems.

DFIR retainers are pre-arranged agreements with cybersecurity firms that guarantee priority access to expert teams for investigating and mitigating incidents. These retainers typically involve a fixed fee for a set number of hours or services, offering peace of mind and faster response times compared to ad-hoc engagements. As threats from nation-state actors, ransomware groups, and supply chain vulnerabilities grow, investing in OT DFIR retainers has become essential.

This guide aims to demystify the purchasing process and provide actionable insights for maximizing return on investment (ROI). It is designed for security leaders, risk managers, and procurement teams seeking to build robust defenses without unnecessary expenditure.

Understanding OT DFIR Retainers

How OT DFIR differs from IT DFIR

OT DFIR retainers differ from general cybersecurity services by focusing on the unique challenges of OT, such as SCADA systems, PLCs, and ICS protocols. Due to the critical nature of OT systems, and the differing impacts to disruption - the approach to responding to OT cybersecurity incidents is very different to responding to IT cybersecurity incidents. For example, taking an IT server offline might mean losing an application, taking an OT service offline might put a person's safety at risk, or cause severe operational disruption to plant.

Core components

Incident Response Readiness: On-call experts for triage, containment, eradication, and recovery.

Digital Forensics: Analysis of logs, network traffic, and device artifacts to identify attack vectors.

Proactive Elements: Some retainers include baseline assessments or threat hunting to prevent incidents.

Retainers are often structured as annual contracts with renewable terms, ensuring continuity, providing a "bucket of hours" that can be drawn down upon to get assistance handling an incident, and topped up during the incident itself if required.

Most DFIR providers also offer emergency assistance to non-customers, but this incurs a higher cost and lacking the background and context of your environment means the service is less effective that a provider who is working with you on a retainer basis.

Benefits Over Ad-Hoc Services

Speed: Guaranteed response within hours (e.g., 2-4 hours SLA) versus days for non-retainer clients.

Cost Predictability: Fixed upfront costs avoid premium pricing during emergencies.

Expertise Alignment: Providers with OT-specific experience reduce risks associated with unfamiliarity in industrial settings.

Compliance Support: Aids in meeting standards like NIST 800-82, IEC 62443, or sector-specific regulations.

Preparedness: Your OT DFIR provider should be able to help you prepare for a potential incident by gathering necessary information about your environment and accelerating the Incident Response Velocity.

Organizations in critical infrastructure sectors report up to 50% faster recovery times with retainers, according to industry benchmarks.

How to Purchase OT DFIR Retainers

Step 1: Assess Your Needs

Begin with a risk assessment tailored to your OT landscape. Identify high-value assets, potential threat actors, and historical incident data. Key questions include:

- What is your average downtime cost per hour?
- How mature is your internal IR team for OT?
- Are there regulatory mandates requiring external support?

This evaluation helps determine retainer scope, such as remote-only versus on-site deployment.

Step 2: Evaluate Providers

Select vendors with proven OT DFIR track records.

Look for:

Certifications and Experience: Teams with GIAC, SANS, or OT-specific credentials; case studies in similar industries.

Global Reach: 24/7 availability and local presence for on-site needs.

Integration Capabilities: Compatibility with your existing tools (e.g., SIEM, EDR for OT). Transparency: Clear SLAs, pricing models, and post-incident reporting.

IT vs OT vs Both: Looking at what drives OT cybersecurity incidents, based on surveys like the SANS state of cybersecurity 2024, close to half of OT compromises began as an IT compromise. Given the specialised domain that is OT DFIR, the best solution for organisations with large OT networks is a provider who can show strong capability across both IT and OT environments, as well as the intersection between them to identify root causes involving lateral movement from IT to OT.

Step 3: Negotiate Contract Terms

Focus on flexibility to avoid lock-in:

Pricing Models: Opt for tiered options, such as basic (remote triage) to premium (full forensics and recovery).

Hour Buckets: Purchase in predefined blocks (e.g., 100-500 hours annually) for economies of scale - often at discounted rates compared to pay-as-you-go.

Rollover Provisions: Ensure unused hours can carry over or be repurposed to incident response readiness, to ensure value for money.

Scalability: Clauses for scaling up to purchase additional hours during major incidents without renegotiation.

Exit Strategies: Short notice periods and data ownership rights.

Aim for contracts that align with your fiscal cycles, with built-in reviews to adjust based on evolving threats.

Common Pitfalls to Avoid

Buying a DFIR retainer that lacks OT domain expertise: IT and OT incident response activities are very different - after all, safety and production are at stake, and your attackers are more likely to be a nation state than an organised crime gang trying to extort you with some basic ransomware. Make sure your provider has deep OT domain experience, and ideally can straddle both IT and OT environments, since many OT breaches come as the result of lateral movement from an IT breach.

Overbuying: Start conservative and scale based on usage data. It's easy to start small with, say, 50 hours, and if you are lucky enough to not need to use them, you should be able to re-purpose those hours towards things like Tabletop exercises or readiness assessments.

Ignoring Fine Print: Watch for hidden fees like travel expenses or after-hours surcharges. Ensure you

Vendor Lock-In: Favor providers offering modular services over all-or-nothing packages. It is also best to source DFIR services from an independent service provider who can cover all technology, unless you have an "all-in" strategy and want to leverage DFIR capabilities from an organisation where you have already made a significant investment in their own technology.

Rollover provisions: Ensure unused hours can be re-purposed to "Peace time" activities like tabletop exercises. It's unrealistic to buy a block of hours and expect them to be available after 3 years to draw on, but there should be avenues through which to use those hours to improve your readiness and assess any key current gaps in your OT cyber maturity.

Maximizing Value from Your OT DFIR Retainer

To transform a retainer from a cost centre into a value driver, it is important to adopt a strategic mindset. The goal is not just incident resolution but leveraging the partnership for broader security gains. Treating your DFIR provider as a partner will allow them to gain a better knowledge of your environment and business, which will be more useful when responding to an incident.

Strategy 1: Proactive Utilization

Don't wait for a crisis or let your hours expire unused. Use retainer hours for:

Tabletop Exercises (TTX): Simulate OT incidents to test response plans, stress-testing your processes and knowledge, and identifying gaps before real threats emerge.

Readiness Assessments: Regular scans and red-team exercises in OT environments. This helps identify major risks and exposures in your environment that you can address before they get exploited by an attacker.

Training Sessions: Upskill internal teams on OT forensics tools and best practices, this helps act as a force multiplier on your DFIR capabilities by building internal capabilities that can be leveraged to complement the deep domain expertise of a global DFIR provider.

This approach can reduce incident frequency by up to 30%, per the SANS report.

Strategy 2: Efficient Management of purchased hours

Bucket Purchasing: Buying hours in larger buckets should give better value for money by accessing volume discounts. This is particularly effective for organizations with variable incident rates.

Repurposing Unused Hours: Advanced providers allow converting leftover hours into consulting services, such as architecture reviews or threat intelligence briefings. For instance, reallocating to TTX or strategic consulting ensures no value is lost at contract end.

Usage Tracking: Implement dashboards to monitor consumption of hours, triggering alerts for underutilization so that investment can be re-purposed to “peace time” activities.

Strategy 3: Integration with Broader Security Ecosystem

Hybrid Models: Combine retainer with internal capabilities for cost efficiency—use experts for complex OT forensics while handling initial triage in-house.

Performance Metrics: Define KPIs like mean time to respond (MTTR) and review quarterly to refine key activities undertaken under the retainer.

Long-Term Partnerships: Providers offering flexible repurposing enable seamless transitions from reactive to proactive engagements, maximizing ROI through customized consulting or simulated exercises.

By emphasizing these tactics, organizations can achieve a 2-3x ROI on retainers, turning them into enablers of resilience rather than mere insurance.

Case Study Insights

One public case study example is a major manufacturer who suffered a security incident due to a Log4J vulnerability. They were able to respond to the incident within 8 minutes in partnership with their DFIR provider, providing recommendations to the organisation's internal threat hunting team with investigation summary provided within 30 minutes of incident detection.

I've purchased a retainer. What happens when I "hit the red button"?

Triggering your OT DFIR retainer marks the transition from preparedness to active response. This is where the value of the pre-arranged agreement becomes immediately apparent: bypassing procurement delays, legal reviews, and negotiations that can add hours or days to response times in non-retainer scenarios. With a well-structured retainer, activation is designed to be swift, structured, and focused on minimizing impact to your operational technology environment.

Activation Process

Most reputable OT DFIR retainers include a clear, client-specific activation playbook established during onboarding. When you suspect an incident (e.g., anomalous behavior in PLCs, unexpected process changes, ransomware indicators, or safety system disruptions), follow these typical steps:

Initiate Contact: Use the designated 24/7 hotline, dedicated email, or portal provided in your retainer agreement. Many providers offer a single point of contact answered by a security analyst or engineer who triages calls on a 24x7 basis.

Initial Triage (Minutes to Hours): Upon activation, expect an immediate acknowledgment—often within minutes—and a rapid triage call. The provider's team will gather essential details:

- Nature and scope of the suspected incident
- Affected OT assets (e.g., specific ICS segments, HMIs, or field devices)
- Current containment measures in place
- Safety and operational priorities (e.g., avoiding unnecessary shutdowns)

This phase typically occurs within 1-4 hours (depending on your SLA), with priority given to retainer clients over ad-hoc requests.

Confirmation and Resource Assignment: The provider confirms the incident falls within retainer scope and assigns a dedicated response lead and specialists experienced in OT environments. For critical infrastructure, this often includes experts familiar with protocols like Modbus, DNP3, or proprietary systems common in your sector.

What Happens Next: The Response Phases

Once engaged, the provider follows a structured, parallelized methodology tailored to OT constraints (e.g., minimizing disruption to real-time processes). Expect activities aligned with industry standards like NIST SP 800-61 or SANS frameworks, adapted for industrial settings:

Containment: Immediate actions to isolate the threat without halting critical operations where possible. This may include network segmentation, disabling compromised accounts, or virtual air-gapping of affected zones. OT specialists prioritize safety and production continuity.

Investigation and Forensics: Rapid collection and analysis of evidence from OT devices, network traffic, logs, and memory where feasible. In OT, this often involves non-intrusive methods, custom tooling for legacy systems, and careful handling to preserve evidence for potential legal or regulatory needs.

Eradication: Removal of the root cause - whether it be malware, backdoors, or persistence mechanisms - while validating that the adversary has been fully removed from the environment.

Recovery: Safe restoration of systems, validation of integrity (e.g., firmware checks), and monitored return to normal operations. This phase includes testing to confirm no residual threats remain.

Post-Incident Activities: Root cause analysis, lessons learned, and recommendations to strengthen defenses. Many retainers include a formal report suitable for executive, regulatory, or insurance purposes.

Throughout, communication is transparent and frequent, with regular status updates to your designated incident coordinator. The team works collaboratively with your internal OT/IT staff, respecting your operational realities and chain of command.

OT-Specific Considerations

OT incidents demand extra caution due to potential physical consequences. Expect the provider to:

- Emphasize "do no harm" principles: avoid actions that could trigger safety interlocks or equipment damage.
- Coordinate closely on change management for any remediation steps.
- Provide guidance on bridging IT/OT teams during the response.

Maximizing Effectiveness During Activation

To get the most from your retainer:

- Activate early - even on suspicion - rather than waiting for confirmation. Early intervention often prevents escalation, the DFIR team will be prepared, and your consumption of time will be quite low if the incident is a “near miss”.
- Have your internal incident response plan and key contacts ready.
- Document observations as the incident unfolds to aid the triage process.

Providers offering flexible hour buckets (as discussed earlier) ensure that complex OT investigations, which may require extended forensics or on-site presence, draw efficiently from your allocated hours without surprise costs.

In rare but severe cases, such as nation-state level attacks, multi-system ransomware, or incidents requiring prolonged on-site presence—the initial hour allocation may be fully consumed before remediation is complete. Retainer agreements typically include provisions for rapid purchase of extra hours, often at the same discounted rate as your original bucket. Preparing internal approval processes in advance (e.g., pre-authorized spend thresholds) allows your team to approve additional hours within minutes rather than hours, keeping momentum and avoiding any pause in critical response activities.

In summary, triggering the retainer delivers priority access to OT-savvy experts who hit the ground running with pre-established processes. This rapid, coordinated response significantly reduces mean time to containment and recovery, protecting both your operations and bottom line. By activating promptly and leveraging the full scope of services, including any repurposable hours for follow-up consulting or TTX, will ensure the retainer delivers its maximum protective value.

Conclusion

Investing in OT DFIR retainers is a critical step toward safeguarding operational continuity in an increasingly hostile cyber landscape. By carefully selecting providers, negotiating flexible terms, and actively managing usage, such as through hour buckets and repurposing for consulting or TTX, organizations can maximize ROI as well as their readiness to respond to incidents. This proactive stance not only ensures rapid response but also fosters a culture of continuous improvement, benchmarking their readiness against industry peers.

For those exploring options, it makes sense prioritize providers that emphasize capabilities across both IT and OT, with comprehensive preparedness and readiness offerings, as these offer the greatest potential for long-term partnership benefits. Implementing these strategies will position your organisation to be best prepared to respond to OT cybersecurity incidents, whether they originate in OT, or come as a result of lateral movement from IT into OT.

Next steps

NetSeg has a 2-way partnership with Sygnia, a specialised Digital Forensics and Incident Response service provider with specialist skills across both IT and OT DFIR. Both organisations leverage each other's capabilities to deliver OT DFIR capabilities to organisations in Australia and New Zealand. If you'd like to explore your own needs further please contact NetSeg's founder Leon Poggioli at leon@netseg.io to discuss your needs further.

References

https://www.sans.edu/cyber-research/sans-2024-state-ics-ot-cybersecurity/

https://nortal.com/insights/why-cyber-exercising-is-the-key-to-surviving-digital-threats

https://www.sygnia.co/case-study/log4j-attack-contained-in-minutes/?service_filter=75&vertical_filter=82

https://www.sygnia.co/incident-response-readiness-executive-guide/

https://hub.dragos.com/hubfs/Dragos_WP_OT-Incident-Response-0323.pdf?hsLang=en