SYGNIA

ENSURING CONTINUITY IN INDUSTRIAL OPERATIONS

Yoav Melamed, OT Tech Lead at Sygnia

Ensuring Continuity in Industrial Operations: A Guide to OT Backup Strategies

Tailoring backup strategies to ensure operational resilience, safeguard critical configurations, and mitigate risks in Operational Technology environments.

Author: Yoav Melamed, OT Tech Lead at Sygnia

Executive Summary

> In today's rapidly evolving threat landscape, robust backup strategies are essential for preserving operational continuity in Operational Technology (OT) environments.

> Tailored for the unique characteristics of OT systems, this guide highlights essential considerations for key components, effective features of backup solutions, and best practices to ensure backup readiness.

> The guide also explores the broader context of disaster recovery and incident response, emphasizing the integration of backup strategies into comprehensive plans for operational resilience and rapid recovery during crises.

> By adopting these strategies, organizations can reinforce their resilience, minimize downtime, and secure uninterrupted operations against emerging threats.

INTRODUCTION

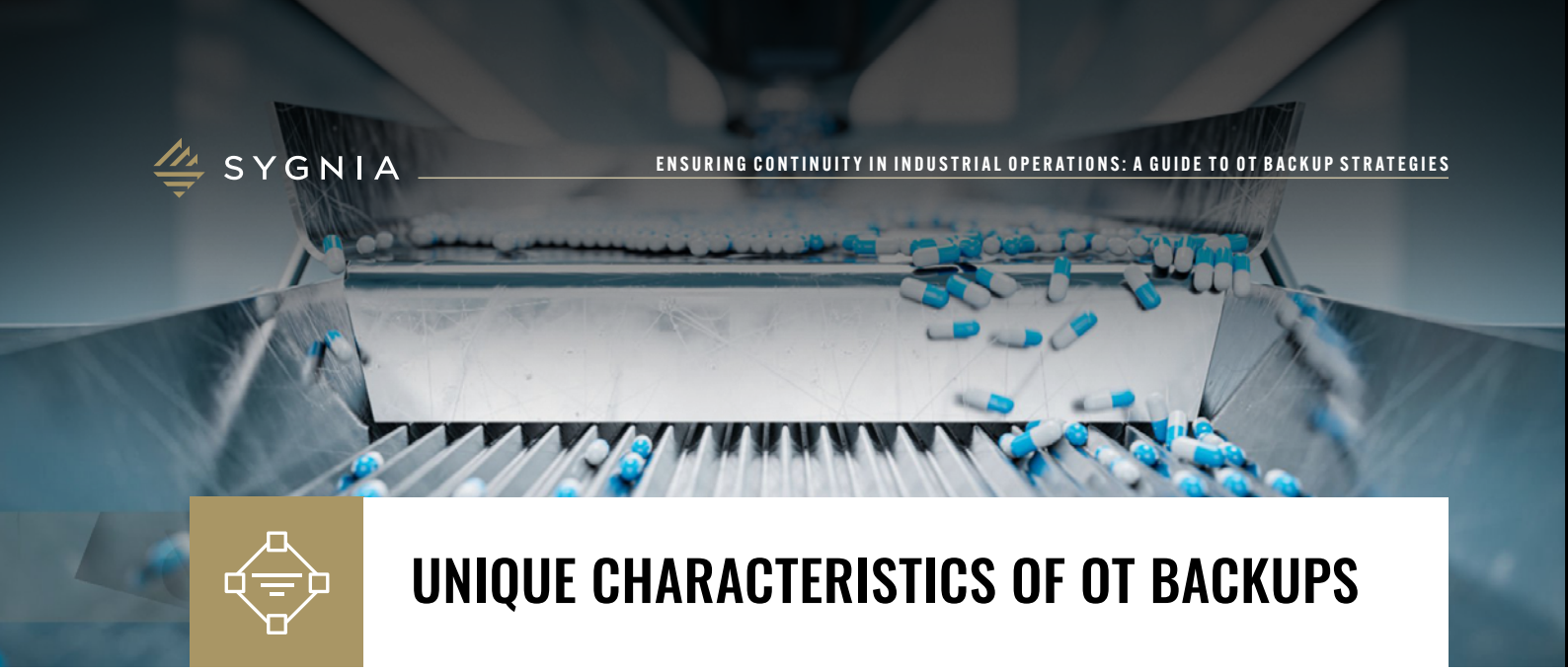
At Sygnia, we often encounter organizations grappling with the aftermath of devastating cyber incidents. For CISOs, having reliable backups is not just a technical safeguard—it is a crucial factor in crisis decision-making. The certainty of backup availability directly influences response strategies, including the choice between restoring operations independently or considering alternative measures, such as paying a ransom in ransomware attacks. Time and again, we've seen how uncertainty about backups complicates response efforts, while well-designed and maintained backup strategies empower organizations to make informed, decisive choices that safeguard operational continuity and resilience in OT networks.

WHY OT BACKUP STRATEGIES MATTER

Backups serve as an operational lifeline during crises. In ransomware incidents, for example, they enable organizations to quickly restore systems, avoiding costly payouts.

Backup strategies are not one-size-fits-all. Your approach should align with the unique ecosystem and operational needs of your organization. In some cases, a simple offline backup might be more effective and efficient than a fully centralized or cloud-hosted solution.

Additionally, robust backup strategies ensure the preservation of critical operational data, such as historical performance metrics, billing information, and configuration files. By safeguarding this essential data, organizations can meet compliance requirements, support forensic investigations, and ensure accurate, efficient recovery of processes after an incident.



UNIQUE CHARACTERISTICS OF OT BACKUPS

OT environments present distinct challenges and opportunities for backup strategies. A defining characteristic is the relatively static nature of OT system configurations. Unlike the dynamic changes often seen in IT environments, OT systems experience infrequent updates, simplifying the management and maintenance of backups. This stability allows organizations to focus on safeguarding critical system configurations and operational data. For example, while data historians generate large volumes of data essential for monitoring, optimization, and compliance, they are not always critical for the immediate operation of core OT systems. This distinction enables prioritization, ensuring that essential operations are protected while historian data backups are managed based on business requirements.

OT backup management introduces complexities not typically encountered in IT. Unlike centralized IT backups managed under unified policies, OT environments often rely on diverse systems supported by multiple vendors, each with its own tools and methodologies. This fragmented approach can hinder consistency and create gaps in availability during incidents. Moreover, maintaining real-time system availability and managing specialized industrial software, such as version control tools, adds further complexity.

To address these challenges, OT backup strategies must be robust, vendor-agnostic, and aligned with the criticality of specific systems. A tailored approach ensures operational resilience while meeting the unique demands of the OT environment.

ESSENTIAL BACKUP CONSIDERATIONS FOR OT COMPONENTS

To effectively implement OT backup strategies, it's crucial to address the specific challenges and requirements of individual components. Backup strategies should be informed by the evolving threat landscape. For instance, an organization that develops redundancy through a disaster recovery site to mitigate hardware malfunctions or natural disasters, such as fires and floods, may still find itself vulnerable to ransomware attacks if its strategy does not account for such threats. This section provides actionable guidance to ensure backup plans align with the specific needs of OT environments, enhancing operational continuity, minimizing downtime, and bolstering resilience.

Network Devices

- **Configuration Backups:** Configuration backups for switches and firewalls should be readily available to ensure rapid restoration of network functionality in case of failure or compromise. These backups should be stored securely in offline or offsite locations to prevent unauthorized access or tampering.
- **Readiness for Recovery:** Regularly update backups to reflect network changes to ensure rapid restoration during critical incidents.

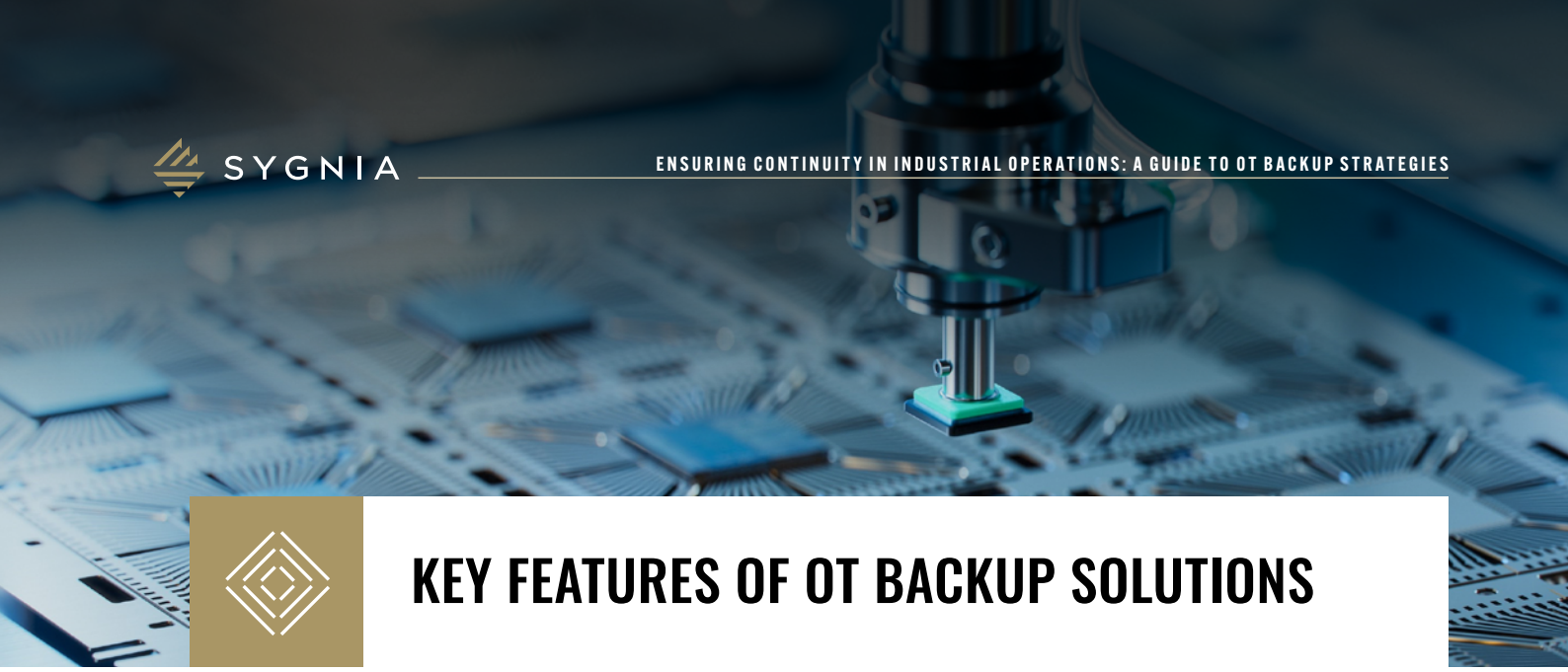
PLCs (Programmable Logic Controllers)

- **Offline Backups:** Enable efficient recovery by securely storing configuration and project files on offline devices such as a field laptop with the vendor software pre-installed. These offline backups should complement main backup storage to provide comprehensive redundancy and resilience.
- **Deployment Ready:** Maintain spare PLCs for seamless recovery during operational disruptions. These devices can be quickly connected and configured using tools like a Field PG (a rugged Siemens field laptop) to minimize downtime.

HMIs, Engineering Stations, and Servers

- **Bare Metal Recovery:** Ensure the backup solution supports full system state restore, eliminating the need to reinstall the operating system.
- **Spare Hardware:** If only a few servers are required for basic operations, having additional hardware ready to use can facilitate quick restoration. Moreover, preserving infected systems for further investigation and analysis becomes possible, aiding in forensic efforts and improving overall security posture.
- **Maintain Licenses:** Some vendors use hardware-bound licenses (HBL) that link software activation to specific hardware components. Possible solutions include license backup and restore utilities, license transfer mechanisms, or the use of license dongles.

Backup strategies for critical components should be customized to meet an organization's unique operational needs. Some OT environments may rely on virtualization platforms, Active Directory infrastructure, or SAP systems, while others might have entirely different requirements. This section emphasizes key considerations but acknowledges that it does not cover every possible component. Organizations should design backup plans that reflect their specific infrastructure, enabling rapid recovery for essential systems while retaining the flexibility to address diverse operational demands.



KEY FEATURES OF OT BACKUP SOLUTIONS

Building on the specific considerations for OT components, effective backup solutions must possess features that address both the operational and security needs of OT environments. These features ensure backups are not only reliable but also resilient against evolving cyber threats.

Agent-Free Solutions: If a backup agent cannot be installed due to vendor restrictions or legacy operating systems, ensure the backup solution is capable of functioning without agent installation. Such solutions operate by using bootable disks, interacting with the kernel level for live snapshots, or using Volume Shadow Copy Service (VSS) to perform system-level backups without agents.

Universal Restore: Opt for solutions capable of restoring systems to different hardware, avoiding costly upgrades tied to vendor dependencies.

Tamper Protection: Attackers often target backup data to increase their leverage by deleting or tampering with it. To counter this, organizations can use immutable storage solutions or maintain offline backups to ensure the integrity of their backup data. Immutable backups prevent any unauthorized changes, while offline backups, disconnected from the network, offer additional protection against cyberattacks and ransomware. Together, these approaches strengthen the reliability and security of backup data.

Encryption: Encrypting backups at rest helps prevent attackers who gain access to raw backup data from retrieving sensitive organizational information. This is particularly important if backup data contains uniform data across environments, as the unencrypted backup data could assist attackers in compromising other locations, intellectual property (such as recipe management) or when backups are stored on portable devices that may be lost or stolen. Ensure secure storage of the encryption key to facilitate restoration even if the backup software itself is compromised.

BEST PRACTICES FOR BACKUP READINESS

Once key features are implemented, maintaining backup readiness requires ongoing assessments and adherence to best practices. This section provides actionable steps to ensure backups remain reliable and aligned with organizational needs.

Conduct Comprehensive Assessments: Identify critical systems and data for prioritized backups.

Define Recovery Objectives: Establish Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) aligned with operational needs.

Use Compatible Tools: Select solutions designed for the unique characteristics and devices in your OT environment.

Separate Between IT and OT Backup Solutions: OT backup solutions must be isolated from IT backups and operate under stricter controls to mitigate cross-domain risks. This separation ensures OT systems remain secure, with backup operations adhering to the unique requirements and sensitivities of operational environments.

Enforce Access Control: Allow administrative access to backups only from trusted locations such as secure jump servers or a Privileged Access Management (PAM) solution.

Implement Identity Management: Assign permissions following the principle of least privilege, and enforce strong authentication, including Multi-Factor Authentication (MFA).

Conduct Real-Time Monitoring: Monitor backup operations for policy changes or deletion attempts.

Perform Regular Testing: Perform periodic restoration drills to ensure the reliability and effectiveness of backups. These drills should include testing various scenarios, such as restoring backups to different hardware and verifying that there are no license compatibility issues.

Document Procedures: Maintain up-to-date backup protocols, ensuring clarity and alignment with evolving environments.

Provide Staff Training: Provide ongoing education on recovery procedures to enhance preparedness.

THE LARGER PICTURE: DISASTER RECOVERY AND INCIDENT RESPONSE

With robust backup solutions and incident response readiness practices in place, the next step is to understand how these strategies integrate into broader organizational frameworks. This section connects backup strategies to disaster recovery and incident response, illustrating their role in ensuring operational resilience and rapid recovery during crises.

Disaster Recovery Planning

Backup strategies are a critical component of a comprehensive disaster recovery plan (DRP). By integrating backups into a structured DR framework, organizations ensure that recovery efforts are fast, efficient and aligned with business continuity objectives. Key considerations for DR planning in OT networks include:

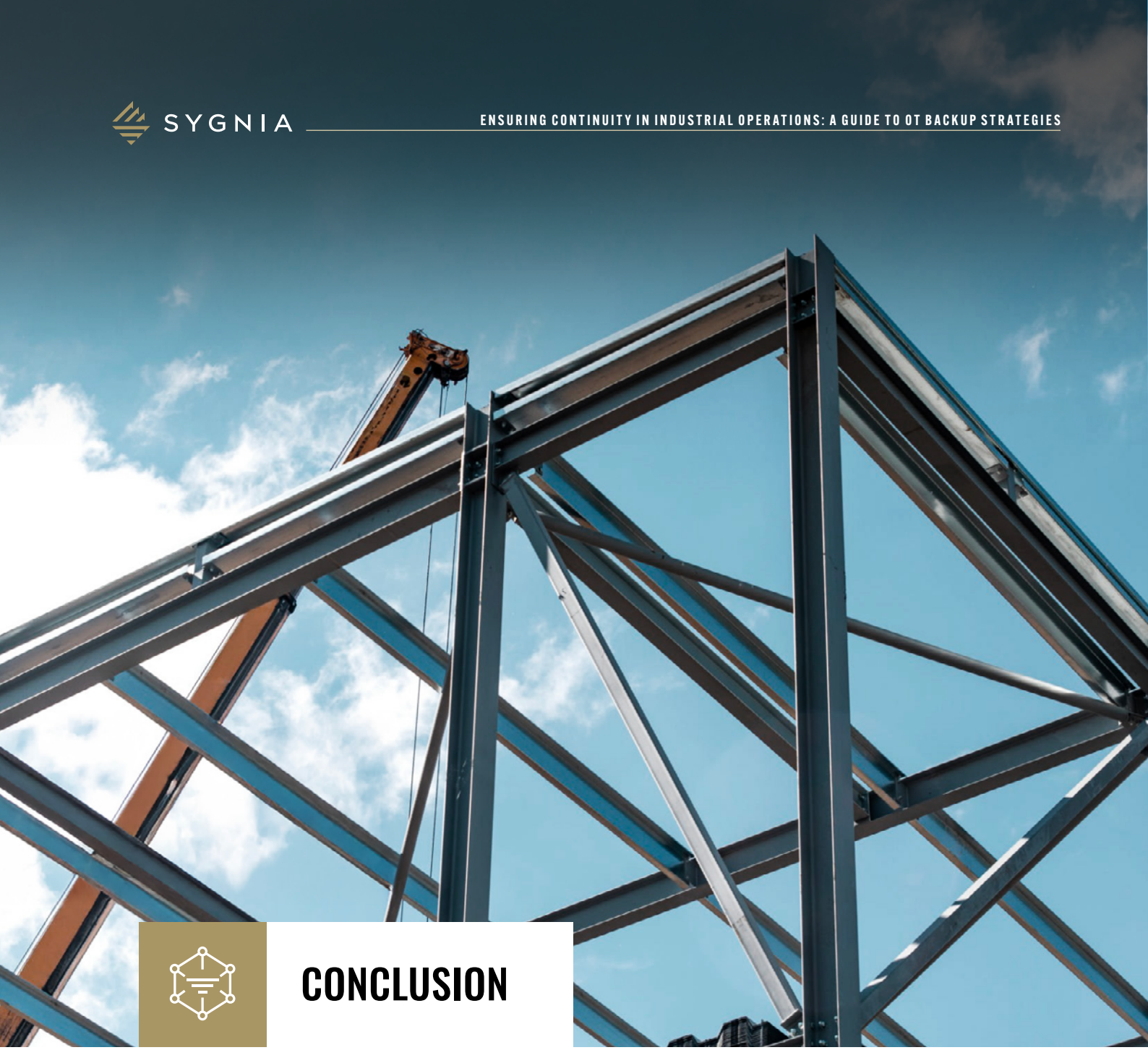
- **Prioritizing Critical Systems:** Identifying the most vital systems for operational continuity and ensuring their backups are prioritized for recovery.
- **Coordinating Across Teams, Vendors, and Service Providers:** Establishing clear roles and responsibilities for IT, OT, and recovery teams to ensure a unified response during disruptions.
- **Periodic Simulation Drills:** Conducting regular disaster recovery exercises to test the viability of backup and restoration processes and to uncover any weaknesses.

Incident Response Integration

Backups play a pivotal role in incident response (IR) strategies. Whether addressing ransomware, data breaches, or operational disruptions, reliable backups help mitigate the impact of incidents. Important aspects include:

- **Rapid Recovery:** Backups allow organizations to quickly resume operations, minimizing downtime and reducing financial losses during incidents.
- **Supporting Forensic Investigations:** Using backups to restore operations while preserving affected systems and their logs enables deeper analysis of the root cause without compromising evidence.
- **Communication Plans:** Ensuring that the availability of backups is integrated into IR communication protocols provides stakeholders with accurate information about recovery timelines.

By combining robust backup strategies with DR and IR frameworks, organizations can build a resilient operational environment capable of withstanding and recovering from unexpected disruptions.



CONCLUSION

Backup strategies are a cornerstone of resilience in OT networks and form an integral part of an organization's disaster recovery plan. Regularly reviewing and enhancing these strategies ensures they remain effective against evolving threats. A well-designed backup plan safeguards operational continuity, strengthens organizational resilience, and minimizes the impact of incidents, ultimately bolstering the overall security posture.

SYGNIA

DISCLAIMER

For full disclosure, Sygnia is collaborating with NVIDIA in a joint research and development effort to develop a novel approach for detection and response at the edge of ICS/OT networks. The MDR technology under development should facilitate hardware-based host-level detection in the upper layers of the OT network (levels 2-3.5), using a combination of hardware, software and AI technologies from NVIDIA and Sygnia, to allow performing sophisticated detection and response operations while adhering to Purdue-based network separation principles. Such technology-based solutions, once available, will have implications on several concepts outlined in this paper, specifically those in the Optimize section, allowing further enhancements in elevating network monitoring, enhancing endpoint detection and elevating infrastructure monitoring.

A TEMASEK COMPANY AND MEMBER OF THE ISTARI COLLECTIVE

TEMASEK ISTARI

24/7 INCIDENT RESPONSE COVERAGE

Suspicious of an incident? Call +1-877-686-8680 now. Learn more at www.sygnia.co