CyFIR Tool and the Shipping Industry

CyFIR Addresses Shipping-Specific Challenges

As the shipping industry undergoes a digital transformation by converging operational technology (OT) with information technology (IT), it faces new threats while enjoying growth and benefits from automation. With further technological advances, the shipping industry—and individual vessels themselves—must update cybersecurity measures regularly. Internet connected vessels are no less vulnerable to attack than other lines of business, and they face unique challenges that few other businesses do.

The shipping industry is no stranger to cybersecurity attacks. In June 2017, shipping giant Maersk suffered a $300 million loss due to the NotPetya ransomware attack *without* suffering a data breach or data loss which would have increased financial damages tremendously. Also, in 2017, UK-based shipping firm Clarkson suffered a severe data breach resulting in the loss of tremendous amounts of privacy-related information. The complexity of the shipping supply chain increases business risk, as cyberattacks on vessels or ports can spiral and delay distribution of the goods which the vessels carry.

In addition to cybersecurity risks shared by all businesses, vessels are potentially subject to very specific attacks that can cause grave results upon life or property. By spoofing GPS data, attackers can cause onboard systems to believe that they are potentially tens or hundreds of miles away from their actual locations, potentially directing vessels into unsafe waters, pirate-controlled areas, or directly into the path of other vessels. The maritime industry magazine *Safety at Sea* described an attack in which a cargo vessel traveling from Cyprus to Djibouti lost control of its own navigation system for over ten hours, preventing a captain from maneuvering with the intention of steering it into territory where it could be boarded by pirates and robbed. Even something as simple as the installation of a Wi-Fi enabled lightbulb may have led to the compromise of a vessel's Wi-Fi credentials, as numerous brands of "smart" lightbulbs store Wi-Fi SSID and encryption key information in plain text. Viruses and other malicious code can spread rapidly through USB flash drives, brought in either by vendors to patch systems or by a vessel's own crew. A flash drive used to trade movies might also be used to update a chart, thereby potentially allowing malicious code to enter a vessel's IT or OT systems.

Losses due to cybersecurity breaches can be catastrophic for any business, and the shipping business is no exception. Besides suffering a potential loss of reputation and shareholder value, shipping companies could lose future cargo bookings, be pulled through extensive litigation, suffer loss of cargo up to and including the complete contents of a vessel, and have extensive costs to repair damage to IT systems or OT systems. In critical cases—especially due to collision—an entire vessel, its crew, and its cargo could be lost.

CyFIR Mitigates Many of These Challenges

Shipboard cybersecurity protocols and measures should include efforts common to any business, such as investment in cybersecurity awareness training, the use of strong passwords and password managers, regular patching and updating of IT systems and antivirus applications, and using two-factor authentication whenever possible. Organizational cybersecurity platforms must be able to address a potentially large number of different computing platforms homogeneously and simultaneously—from a single source without impacting business needs. Additionally, due to the nature of vessels at sea, they may or may not have consistent Internet connectivity, so a deployed cybersecurity solution may not be able to rely upon a full-time connection to the "cloud." Many antivirus programs and other security solutions work well with a high-bandwidth, always-available Internet connection but fail quickly when that connection is slow or unavailable.

To address these issues, it's crucial that shipping businesses have cybersecurity measures in place that are equal to or better than their onshore counterparts.

CyFIR is uniquely qualified to mitigate these challenges.

The CyFIR Enterprise Platform

CyFIR Enterprise, a powerful forensic investigation and incident response platform, allows cybersecurity personnel to forensically examine any CyFIR-enhanced computing endpoint *immediately,* without disrupting the work being done on that computer by its normal user. From a remote CyFIR Investigator terminal—across the hall or across the world—a security analyst can immediately respond to an attack, an insider threat, or a legal/regulatory data request.

Unlike competing forensic analysis "enterprise" platforms, CyFIR can search thousands of computing endpoints at the same time, regardless if the endpoints are located on traveling vessels or are stationed at Headquarters. The operator receives responsive information as it is located on each endpoint—even over low-bandwidth connections such as FleetBroadband (FBB), as CyFIR's command-and-control architecture is designed to exchange only minimal amounts of information to and from remote endpoints. CyFIR's Smart Agents carry forensic processing capabilities within themselves, so all forensic processing is done upon request at the computing endpoints, allowing a security operator to receive near real-time feedback to quickly address an issue. Furthermore, CyFIR's monitoring capabilities are always on, even if there is no Internet connectivity for periods of time.

By providing fully remote access to computing endpoints, coupled with the ability to access and search those endpoints simultaneously, **CyFIR acts as a force multiplier, allowing one cybersecurity professional to address what would take the work of an entire team under traditional incident response and forensic investigation**

methodologies. CyFIR supports Windows, Mac, and Linux based systems with one application, combining results into a single view. *In doing this, CyFIR addresses challenges related to* ***time and budget****—by reducing the need for both—and the* ***lack of qualified human capital****, by allowing one person to perform the work of a team.*

Within the CyFIR Enterprise platform, security operators can:

- monitor the entire fleet and Headquarters at the same time through a unified graphical view,
- quickly receive alerts of potential threats on CyFIR-enhanced endpoints through a centralized dashboard
- immediately begin incident response upon determining the existence of a threat,
- investigate a computer at a forensic level to determine potential insider threat, data exfiltration, data corruption, or compromised control, without disturbing the business use of the computer as performed by the employee, quickly and quietly,
- actively hunt threats, optionally aided by CyFIR's automated malcode detection capabilities from the CyFIR Intelligence Network, maintaining forensic traceability,
- review computing devices to ensure legal or regulatory requirements,
- monitor and respond to CyFIR-enhanced endpoints at sea while minimizing additional bandwidth usage by transferring only required metadata from vessels to Headquarters,
- provide near-real time monitoring and response capabilities without additional investments in hardware or complex systems to maintain and support,
- increase the capabilities, reach, and depth of a company's cybersecurity stack, as CyFIR is complementary to EDR and other cyber platforms,
- provide reporting via the optional CyFIR Intelligence and Analytics dashboard for high-level stakeholders to quickly understand their cybersecurity effectiveness and posture, and
- arrange for cyber insurance through the Lloyds of London market via Ridge Global.

CyFIR Managed Services

CyFIR Managed Services—provided by trained personnel using the power of the CyFIR Enterprise platform—provides several benefits to vessels and ports that are having challenges addressing:

- an overall lack of digital culture,
- lack of awareness and training in cybersecurity,
- complexity of IT and OT diversity,
- difficulty in staying up to date with the latest threats, and
- supply chain challenges.

CyFIR's ability to provide a "single pane of glass" into an organization of different computing platforms, paired with its ability to see running processes on endpoints from Windows, Mac, and Linux based operating systems, makes it the ideal platform for handling large ports with different levels of IT awareness and security. Qualified and experienced cybersecurity professionals using CyFIR will be able to monitor networks for signs of malicious activity, grouping processes automatically into categories of those known to be *good*, those known to be *malicious*, and those that have *not been previously analyzed* by the digital intelligence community. Often these unknown processes are simply corporate, or business line specific software used in daily operations, but this category also harbors unknown threats such as “zero-day” attacks—those yet unseen or stopped by antivirus vendors. After identifying these processes, CyFIR Managed Services automatically sends these processes for deep automated inspection, and the results are reviewed and validated by trained personnel, and only those suggesting malicious activity are alerted to the port authorities for action. Through the CyFIR Managed Service, CyFIR Enterprise provides a port with a critical “last line of defense” to a cyber breach or attack.

Because CyFIR’s platform is flexible and can search thousands of computers simultaneously, CyFIR Managed Services personnel can act quickly when a threat is located and can identify that threat throughout a network rapidly. Additionally, with the power of CyFIR Enterprise beneath the CyFIR Managed Service, incident response can begin *immediately* instead of letting attackers gain ground in a victim network while the port authorities arrange for an incident response provider and wait for that provider to address a situation. When most incident response firms advertise a “72-hour response window” after the contract has been negotiated, CyFIR Managed Services personnel can often have an incident response, or an investigation *completed* before competitors can have their first person on site.

Conclusion

CyFIR Enterprise, and CyFIR Managed Services, address many cybersecurity challenges currently facing ports and vessels involved in transport and commerce. Through its expansive, investigative platform, CyFIR operators and CyFIR Managed Services can surveil large networks for malicious code, evidence of breaches, and more. Because of CyFIR’s concurrent nature, entire networks can be searched in the time competitors can search four or five computers. Without requiring antiquated “image and analyze” computer forensics and incident response practices, ports can respond to incidents instantly, thereby minimizing the cost and exposure of a cybersecurity event or breach. In this way, CyFIR answer’s the European Union Agency for Cybersecurity’s (ENISA) recommendation to enforce detection and response capabilities at the port level to react as fast as possible to *any* cyberattack before it impacts port operation, safety, or security. CyFIR’s capabilities also support a number of points of guidance outlined in BIMCO’s **“The Guidelines on Cyber Security Onboard Ships,”** giving organizations the abilities to identify threats, assess risk exposure, develop wider and more responsive protection and detection measures, enhance their “defense in depth” capabilities, and to provide a means for effective response and the investigation of cyber incidents.