تحت رعاية صاحب السمو الشيخ محمد بن زايد آل نهيان، رئيس دولة الإمارات العربية المتحدة

Under the Patronage of H.H Sheikh Mohamed Bin Zayed Al Nahyan, President of the United Arab Emirates

أديبك ADIPEC

Host

أدنــوك ADNOC

Technology for Continuous Cyber Monitoring of Offshore Assets.

ADIPEC 2023 TECHNICAL CONFERENCE

SPE-217071-MS

Capt. Zarir Irani

Technical Conference organised by SPE International Society of Petroleum Engineers

ADIPEC brought to you by dmg::events

Prelude

Technology for Continuous Cyber Monitoring of Offshore Assets.

“The increase in remote monitoring and autonomous control, IoT and digitalization has made rigs much more susceptible to attack.”

- Adam Rizika, Head of Strategy, Naval Dome

Real Case

- A Cyber attack was launched on an offshore rig with just a USB stick.
- An OEM service technician unwittingly used the USB stick with malicious software containing three zero-day exploits.

Image source: https://img.freepik.com/premium-photo/offshore-oil-gas-rig-sea-sunset-time-industry-drill-platform-ocean-futuristic-modern-3d-illustration_76964-5493.jpg

Causes leading to the problem.

Technology for Continuous Cyber Monitoring of Offshore Assets.

- **Shortage** of operational technology (OT) cyber domain skilled staff.
- **Lack** of security awareness.
- Using security controls that are **slow to evolve** and be implemented.
- **Inadequate** cybersecurity measures, such as insufficient network segmentation can make it easier for attackers to gain access.
- IT-centric approached being applied to an OT environment, causing **mismatch** between drilling rig systems and equipment and their supporting software.

Source: OnSecurity.io
https://www.onsecurity.io/blog/offshore-drilling-rigs-vulnerable-to-cyber-attacks/

Existing Cyber Threats as of 2023

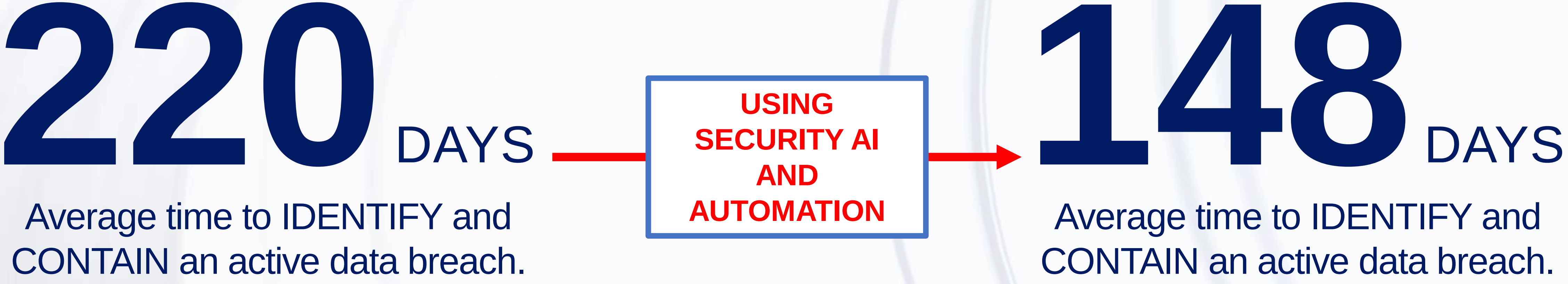
Technology for Continuous Cyber Monitoring of Offshore Assets.

Oil and gas infrastructure are vulnerable to a range of cyber threats due to their **interconnected and digitally controlled nature.**

These threats can have serious **economic, environmental, and safety implications.**

- RANSOMWARE ATTACKS
- SOCIAL ENGINEERING
- REMOTE ACCESS EXPLOITATION
- DATA LEAKAGE
- INSIDER THREATS
- INTELLECTUAL PROPERTY THEFT
- PHISHING
- SUPPLY CHAIN ATTACKS

Technology for Continuous Cyber Monitoring of Offshore Assets.



220 DAYS

Average time to IDENTIFY and CONTAIN an active data breach.

USING SECURITY AI AND AUTOMATION

148 DAYS

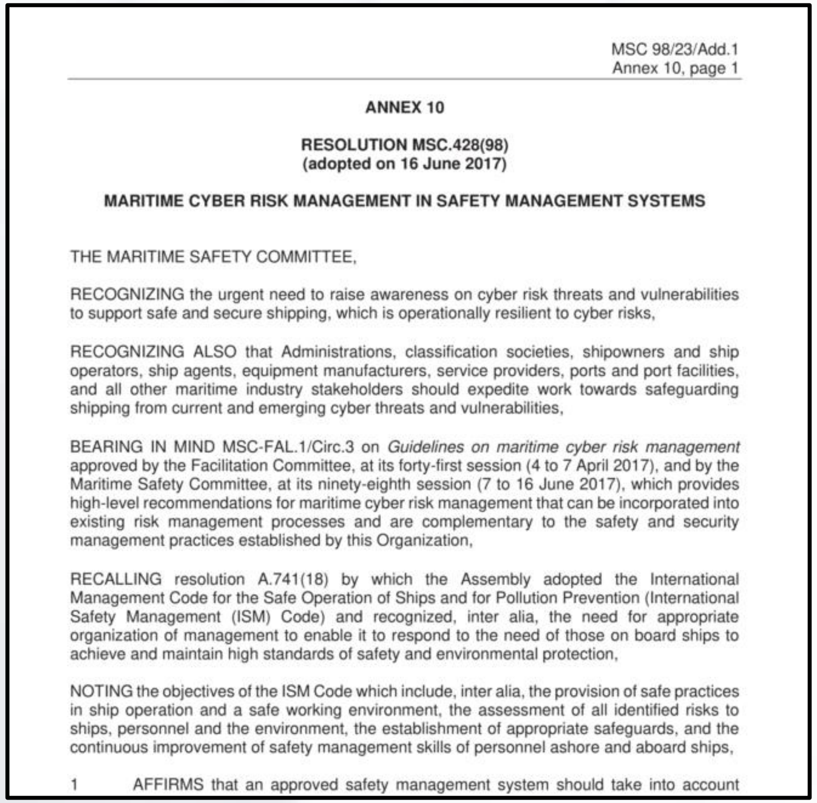
Average time to IDENTIFY and CONTAIN an active data breach.

SOURCE: IBM REPORT 2023

Existing Offshore Cybersecurity Framework

Technology for Continuous Cyber Monitoring of Offshore Assets.

IMO INTERNATIONAL MARITIME ORGANIZATION



MSC 98/23/Add.1
Annex 10, page 1

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

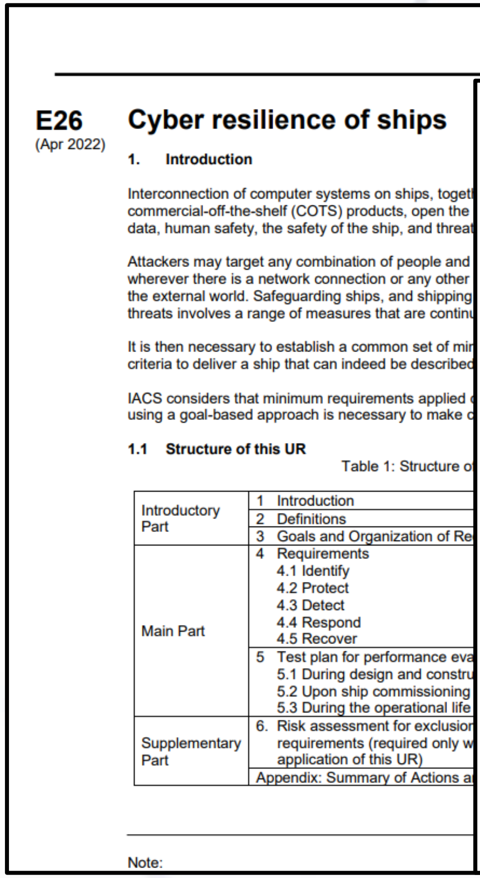
BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account

IACS International Association of Classification Societies



E26

E26
(Apr 2022)

Cyber resilience of ships

1. Introduction

Interconnection of computer systems on ships, togetl
commercial-off-the-shelf (COTS) products, open the
data, human safety, the safety of the ship, and threat

Attackers may target any combination of people and
wherever there is a network connection or any other
the external world. Safeguarding ships, and shipping
threats involves a range of measures that are continu

It is then necessary to establish a common set of mir
criteria to deliver a ship that can indeed be describec

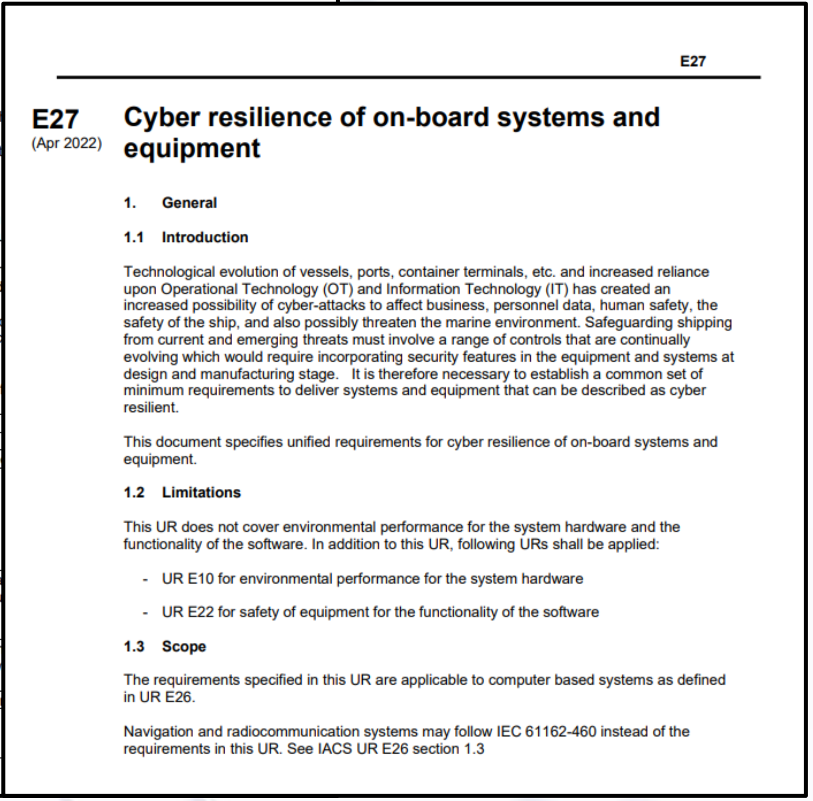
IACS considers that minimum requirements applied c
using a goal-based approach is necessary to make c

1.1 Structure of this UR

Table 1: Structure o

Introductory Part	1 Introduction
	2 Definitions
	3 Goals and Organization of Re
Main Part	4 Requirements 4.1 Identify 4.2 Protect 4.3 Detect 4.4 Respond 4.5 Recover
	5 Test plan for performance eva 5.1 During design and constru 5.2 Upon ship commissioning 5.3 During the operational life
Supplementary Part	6. Risk assessment for exclusior requirements (required only w application of this UR)
	Appendix: Summary of Actions ai

Note:



E27

E27
(Apr 2022)

Cyber resilience of on-board systems and equipment

1. General

1.1 Introduction

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

This document specifies unified requirements for cyber resilience of on-board systems and equipment.

1.2 Limitations

This UR does not cover environmental performance for the system hardware and the functionality of the software. In addition to this UR, following URs shall be applied:

- UR E10 for environmental performance for the system hardware
- UR E22 for safety of equipment for the functionality of the software

1.3 Scope

The requirements specified in this UR are applicable to computer based systems as defined in UR E26.

Navigation and radiocommunication systems may follow IEC 61162-460 instead of the requirements in this UR. See IACS UR E26 section 1.3

Possible Risk Mitigation Means using NIST Framework

Technology for Continuous Cyber Monitoring of Offshore Assets.

NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY (NIST) FRAMEWORK

- A robust **framework** is essential for effectively **tracking the cyber resilience** and policy adherence of offshore assets.
- Using a **continuous cyber monitoring** framework helps monitor the key components and processes involved in the platform such as *asset inventory, threat intelligence, vulnerability assessment, security controls, incident detection and response, and compliance monitoring.*

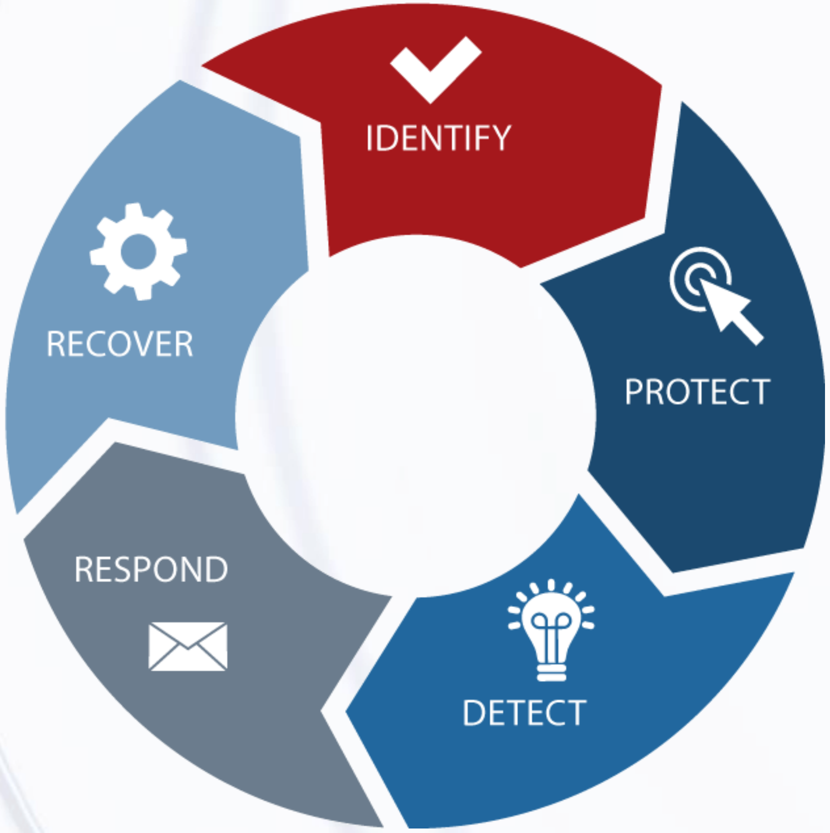


Image source: https://nemep.unl.edu/images/cyberframework-circle1.png

Existing Cyber Risk Mitigation

Technology for Continuous Cyber Monitoring of Offshore Assets.

To achieve effective continuous cyber monitoring, a combination of technologies and strategies can be employed, maintaining operational integrity and safeguard against disruptions.

- Network intrusion and detection system (NIDS)
- Security orchestration, automation and response (SOAR)
- Security information and event management (SIEM) system
- Encryption and secure communication
- Endpoint protection
- Vulnerability assessment
- Anomaly Detection
- Security awareness training
- Multi-factor authentication
- Remote monitor and management

Source from: National Institute of Science and Technologies (NIST)

New Proposed Solution for Application

Technology for Continuous Cyber Monitoring of Offshore Assets.

1. A system capable of **identifying, containing, eradicating, and recovering** from any security incident.

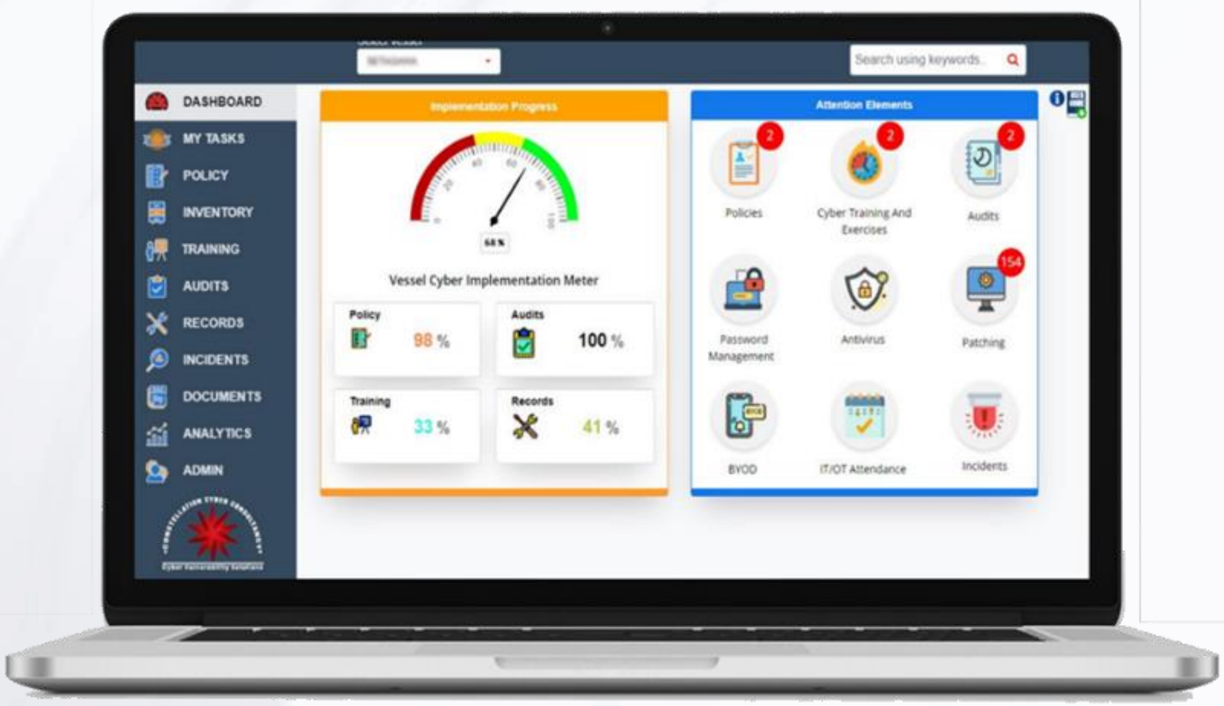
2. Integration of security information and event management platforms and other **external systems and tools.**

3. Using **machine learning algorithm** for anomaly detection and behavioral analysis to identify any suspicious activities or potential security breaches.

4. Assesses an organization's assets, **evaluates their potential value**, and compares that value to potential dark web prices to estimate potential losses in case of a data breach or security incident.

The NEW platform for Continuous Cyber Compliance.

Technology for Continuous Cyber Monitoring of Offshore Assets.



Vessel Cyber Implementation Meter

Policy 98 %

Audits 100 %

Training 33 %

Records 41 %

CYBER SOLUTION WITH REAL TIME VISUALISATION OF COMPLIANCE ON BOARD

COMPLIANCE MONITORING

CYBERSECURITY ALERTS

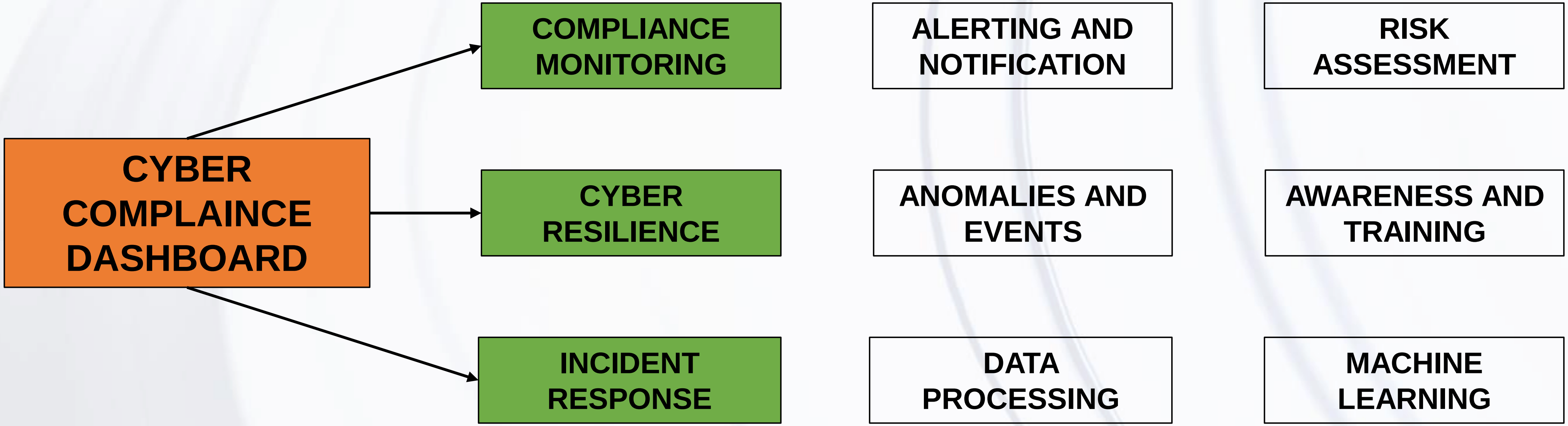
REAL-TIME DATA PROCESSING

AWARENESS AND TRAINING

Potential Features of the Application

Technology for Continuous Cyber Monitoring of Offshore Assets.

Assure compliance with up-to-date cybersecurity policies using a dedicated compliance monitoring solution to review the offshore assets' cybersecurity and governance.



Compliance Monitoring by the Cyber Application

Technology for Continuous Cyber Monitoring of Offshore Assets.

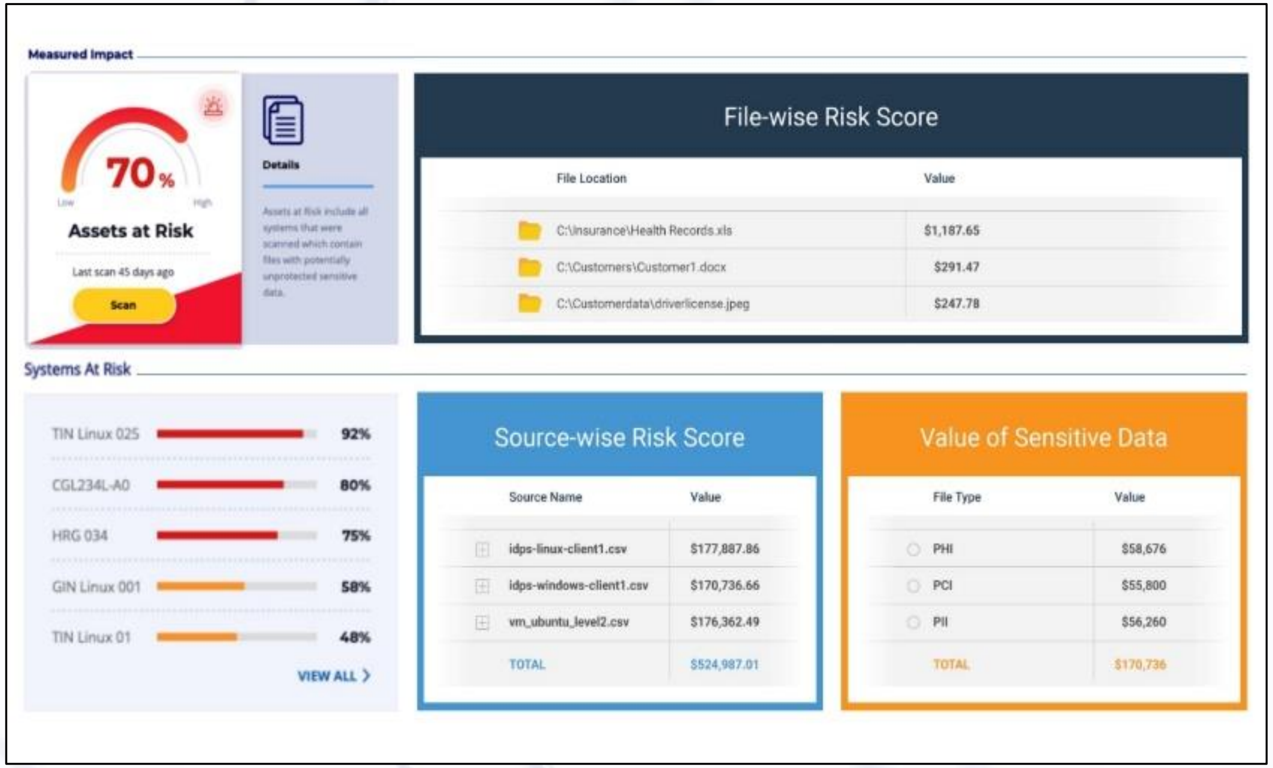
- **Performance dashboard** with overview of compliance status, allowing stakeholders to monitor progress and make informed decisions.
- **Monitor network and system events** continuously to identify unusual patterns or behavior and Automated Solutions for Managing and Mitigating the event.
- **Flexibility in monitoring tool** to handle emergencies and unexpected events that could impact compliance and reputation, such as oil spills or cybersecurity breaches.
- **Machine Learning** for evaluating the cyber resilience of vessels in real-time through risk scoring, threat modeling, and gap analysis.
- **Priority based Alerting System** to indicate critical assets that needs to be addressed immediately during a breach.

Monetary-Value based File Evaluation

Technology for Continuous Cyber Monitoring of Offshore Assets.

Raise awareness across the Board Management by **putting a “dollar” value on your files** and system by comparing your exposure in the digital space with the Dark Web.

- **Data classification system** categorize files into various tiers based on their value.
- **Value** of different types of data are based on factors like **sensitivity, rarity, and demand.**
- **Protect sensitive information during valuation** process by anonymizing personal and sensitive data.
- Set up tools to **regularly scan the dark web for mentions** of the organization's data or sensitive information.



Measured Impact

Assets at Risk include all systems that were scanned which contain files with potentially unprotected sensitive data.

File-wise Risk Score

File Location	Value
C:\Insurance\Health Records.xls	$1,187.65
C:\Customers\Customer1.docx	$291.47
C:\Customerdata\driverlicense.jpeg	$247.78

Systems At Risk

TIN Linux 025	92%
CGL234L-A0	80%
HRG 034	75%
GIN Linux 001	58%
TIN Linux 01	48%

VIEW ALL >

Source-wise Risk Score

Source Name	Value
idps-linux-client1.csv	$177,887.86
idps-windows-client1.csv	$170,736.66
vm_ubuntu_level2.csv	$176,362.49
TOTAL	$524,987.01

Value of Sensitive Data

File Type	Value
○ PHI	$58,676
○ PCI	$55,800
○ PII	$56,260
TOTAL	$170,736

Cybersecurity Awareness and Training

Technology for Continuous Cyber Monitoring of Offshore Assets.

- Cybersecurity awareness and training for offshore oil rigs are essential to mitigate the risks associated with cyber threats and attacks in these critical environments.
- Implementing cybersecurity awareness and training program tailored to the unique challenges of offshore oil rigs can empower personnel to actively contribute to the cybersecurity posture of the rigs, reducing the risk of cyber incidents and operational disruptions.

REGULAR ASSESSMENT

SIMULATED PHISHING

PHYSICAL SECURITY

EMERGENCY RESPONSE

Benefits of using the Cyber Compliance Application

Technology for Continuous Cyber Monitoring of Offshore Assets.

MAINTAINING REGULATORY COMPLIANCE.

The compliance tool can help ensure that the offshore assets are complying with regulations, avoid legal penalties, and improve the overall security of their critical systems and data.

MANAGING MULTIPLE OFFSHORE ASSETS.

Using a network of sensors, Intrusion Detection Systems and AI-driven analytics, a company can constantly evaluate the digital infrastructure of several offshore oil rigs in a single remote locations.

MONITORING THE SECURITY POSTURE.

Providing real-time data on the status of critical assets, such as their security vulnerabilities and risks, can ensure that the asset is operating in a compliant manner using latest frameworks.

Security vs. Usability Trade-off

Technology for Continuous Cyber Monitoring of Offshore Assets.

- **Security:** High security typically involves stringent measures, such as complex passwords, multifactor authentication, encryption, and restricted access. These measures are essential to protect sensitive data and prevent unauthorized access.

- **Usability:** Usability focuses on making systems or interfaces easy to use and accessible to a wide range of users. This includes considerations like user-friendly interfaces, minimal steps to complete a task, and clear instructions.

SECURITY USABILITY

The challenge is finding the right balance between security and usability.

Potential handicaps with the Compliance Application

Technology for Continuous Cyber Monitoring of Offshore Assets.

- **Resource Constraints** - Limited resources, including power, bandwidth, and computational capacity
- **Data privacy and Compliance** - Legal and compliance challenges related to data privacy and data transfer across borders
- **False Positives** - Overly sensitive cybersecurity systems can generate many false positive alerts, missing the real security threats
- **Human error** - Employees or contractors on offshore assets might inadvertently compromise security protocols.
- **Cost Considerations**– Implementing and maintaining robust cybersecurity measures can be expensive
- **Integration Complexity:** Integrating these systems and ensuring they work seamlessly together can be complex, causing compatibility issues and operational problems.

Advantages with the Compliance Application

Technology for Continuous Cyber Monitoring of Offshore Assets.

- **Maintaining Reputation** - Effective measures for offshore assets to protect the organization's reputation by demonstrating a strong commitment to security and resilience.
- **Preventing Environmental Impact** - Protecting the integrity of offshore assets also reduces the risk of environmental incidents that could result from cyberattacks affecting critical systems.
- **Reduced Downtime** - Identification and response to security incidents can reduce downtime and operational disruptions caused by cyberattacks, ensuring uninterrupted operations.
- **Reduced Attack Surface** - Implementing strong security measures helps reduce the attack surface and limit potential entry points for attackers.
- **Employee Awareness** - Regular security training for employees help foster a cybersecurity-conscious culture, reducing the likelihood of human errors that can lead to breaches

Key Takeaway

Technology for Continuous Cyber Monitoring of Offshore Assets.

- Technology for monitoring of offshore assets is a crucial investment for ensuring the cybersecurity and operational resilience of these critical components of the energy and maritime sectors.
- Detecting a cyber threat early can safeguard the business and its operations by rapid respond and mitigating the threat.
- While challenges exist, the benefits in terms of threat detection, risk mitigation, regulatory compliance, and operational continuity make continuous monitoring a vital strategy in today's cybersecurity landscape.

SCAN TO DOWNLOAD
THIS PRESENTATION

THANK YOU