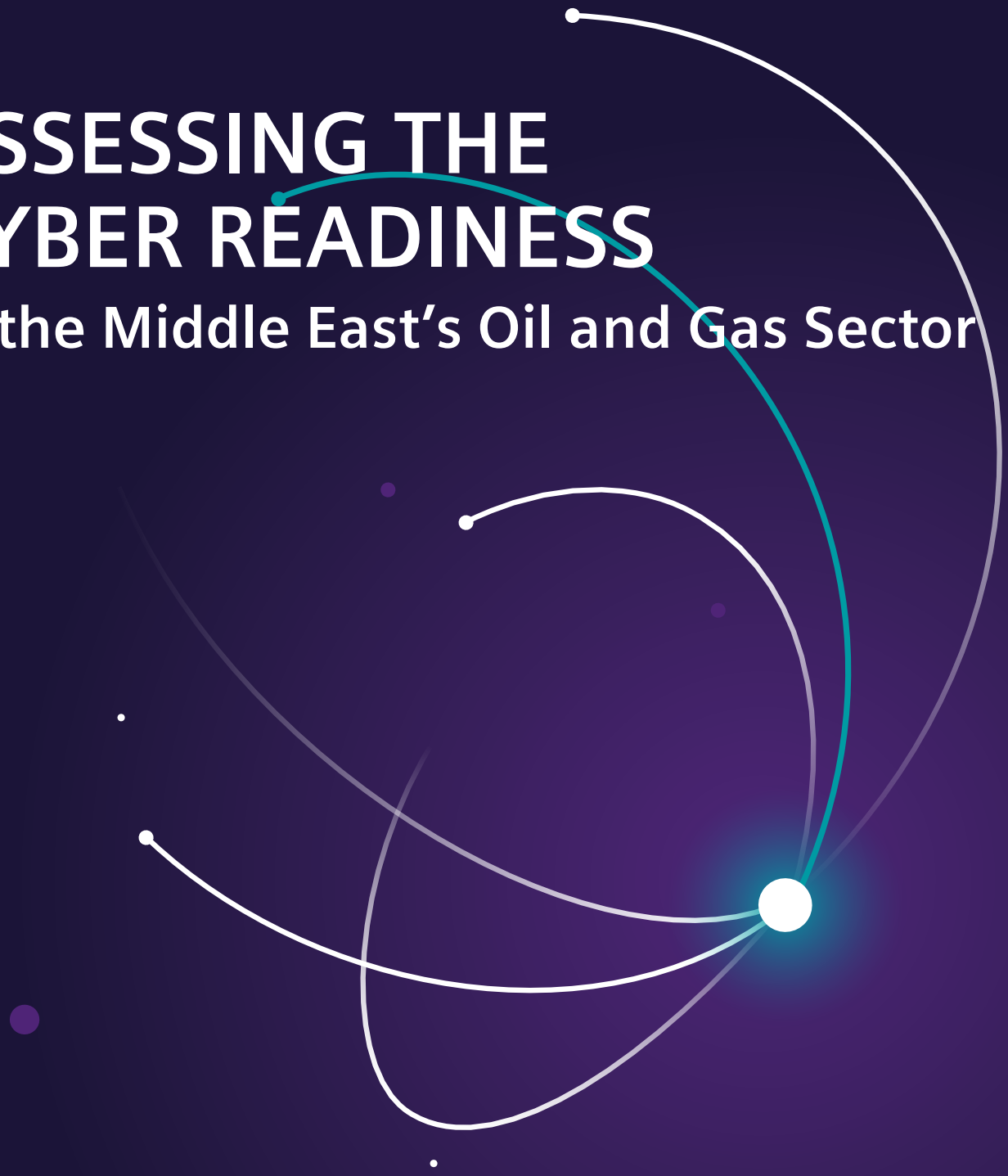
SIEMENS energy

ASSESSING THE CYBER READINESS

of the Middle East's Oil and Gas Sector



Contents

Foreword	**06 – 07**
Executive summary	**08 – 09**
Introduction	**10 – 13**
OT cyber risk today	**14 – 21**
Readiness to address the OT cyber challenge	**22 – 27**
Solutions to the OT cyber challenge	**28 – 33**
Conclusion	**34 – 35**
Methodology	**36 – 37**

An emerging trend of cyber attacks is designed to disrupt physical devices or processes used in operations.



Ponemon Institute

The Ponemon Institute conducts independent research on privacy, data protection and information security policy. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

In addition to our research, Ponemon Institute provides strategic consulting to private and public sector organizations interested in establishing or enhancing their privacy, data protection, and security practices. To ensure that their goals are achieved, organizations engage us to assess their practices and conduct workshops and training programs.

Ponemon Institute is the parent organization of the Responsible Information Management (RIM) Council. The RIM Council draws its name from the practice of Responsible Information Management, an ethics-based framework and longterm strategy for managing personal and sensitive employee, customer and business information.

Assessing Cyber Readiness Of The Middle East's Oil & Gas Sector

Siemens Energy Industrial Cyber

Given the probability of a cyber breach is nearly 100 percent, the question for executives and security professionals becomes not whether to act, but how? Holistic cyber security emphasizes not only the need to prevent an attack but also the game plan for how to respond.

At Siemens Energy, we take our customers on a cyber security journey that brings maturity to their industrial enterprise. This means starting with a risk-based strategy that deals in fundamentals, transforms an organization's response to the environment, and most importantly, builds their capacity to monitor and respond to threats. These threats range from connected assets in the field to control centers that run critical infrastructure, to the enterprise networks that make up the new energy value chain.

This agility is essential to dealing effectively with the growing cyber threat. The organizations that move proactively to build their capability to detect vulnerabilities, and respond to attacks, will be best positioned to meet the challenges and opportunities of a digital economy. For Siemens Energy, a secure industrial world is an essential component of our vision for an energy industry that leverages digitalization and intelligent infrastructure.

In the past decade, Siemens Energy has invested over $10 billion to make digitalization a core part of our own business transformation. Now we are making our industrial cyber capability and its complementary external offerings available to our customers.

Foreword

Until recently, most cyber attacks have targeted the Information Technology (IT) environments, comprised of PCs, work stations, and mobile devices. As the process of digitalization has accelerated, so too has the convergence of IT and operational technology (OT) connectivity. This provides a wide range of benefits that enable organizations to optimize processes, capture cost savings and turn data into value. At the same time, connectivity has also created a larger cyber "attack surface" that is harder than ever to secure.

Attackers have identified this convergence of IT and OT as a key opportunity to penetrate an organization. As a result, an emerging trend of cyber attacks is designed to disrupt physical devices or processes used in operations.



In fact, OT now comprises an estimated

30% **of all cyber attacks around the world**

The disruption of critical infrastructure in industries can have catastrophic security, economic and environmental implications. In the Middle East, we have recently seen the Triton malware targeting industrial control systems in the energy sector by exploiting a previously unknown zero-day vulnerability. This OT-specific malware was designed to impact safety control systems, and underscores the potential OT cyber risk to health, safety and the environment.

These trends - accelerating digitalization, the convergence of IT and OT, more frequent, sophisticated cyber attacks, and an energy sector in the crosshairs – led Siemens Energy, in conjunction with the Ponemon Institute, to delve more deeply into the cyber readiness of the oil and gas industry in the Middle East. The impact of these cyber intrusions against OT assets in the Middle East, especially in the oil and gas

Assessing Cyber Readiness Of The Middle East's Oil & Gas Sector

sector, especially in the oil and gas sector, the target of 50 percent of all cyber attacks in the region, is more significant than in other parts of the world: greater frequency relative to return on investment (ROW), more expensive relative to ROW and with greater downtime.

To their credit, organizations in the region have been early enthusiasts for digitalization, ahead of many others in the world in recognizing the unprecedented business value. They have also recognized the greater cyber risk associated with greater connectivity. Oil and gas companies in the region are beginning to invest in protecting their assets from cyber intrusions, while lagging behind in terms of awareness and the rate of deploying technology that can protect their operating environment. In the government sphere, regulations intended to address the OT cyber threat are being rolled out, though, admittedly, these are mostly at an early stage.

Throughout this report, we seek to shed light on the state of cyber readiness of oil and gas companies in the region and hope you will find the insights drawn from this report illuminating.



Leo Simonovich
VP and Global Head
Industrial Cyber, Siemens Energy



Gianluigi Di Giovanni,
Chief Executive Officer,
Power Generation Services, Middle East and North Africa, Siemens Energy

Executive Summary

This report is the result of the second collaboration between Siemens Energy and the Ponemon Institute. It consists of a survey of 176 individuals in the Middle East responsible for securing or overseeing cyber risk.

Among the findings from these respondents in the Middle East and discussed in this report:



of respondents believe they face a greater risk in the OT than in the IT environment.

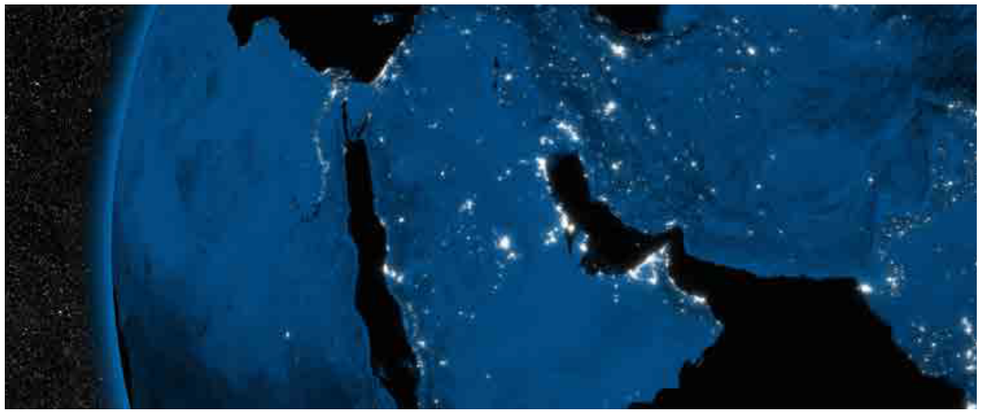


of respondents believe the risk level to industrial control systems over the past few years has substantially increased because of cyber threats.



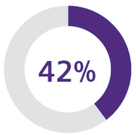
of organizations have suffered at least one security compromise that resulted in the loss of confidential information or disruption to operations in the OT environment over the past 12 months.

The process of digitalization is creating benefits for oil and gas companies (e.g., greater efficiencies, operational insights) but also generating significantly increased cyber risks, according to 62 percent of respondents.

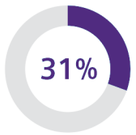




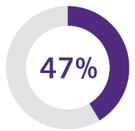
of respondents say the top cyber security threat is the negligent or careless insider.



of Middle East respondents said that outdated and ageing control systems pose a serious risk to their organizations.



of respondents say their organization's industrial control systems' protection and security are adequate.



respondents say they continually monitor all infrastructures to prioritize threats and attacks.

43% thought they had the internal expertise necessary to manage cyber threats in the OT environment.

The objective of this research presented here is to gain insight into how the oil and gas industry in the Middle East region understands the OT cyber risk it is facing, and how ready it is to meet this challenge.

1 Introduction

Siemens Energy and the Ponemon Institute are pleased to present the results of 'Assessing the Cyber Readiness of the Middle East's Oil and Gas Sector' report. This survey provides a first-of-its-kind assessment of the readiness of Middle East oil and gas companies to deal with the emerging cyber threat to Operational Technology (OT).

The OT cyber risk is particularly acute in the Middle East. Given the critical importance of oil and gas to the region's economies, OT cyber security is an especially pressing topic. We have already seen sophisticated cyber attacks targeting oil and gas organizations (Aramco in 2012) and OT specifically (Triton in 2017). The financial impacts of these attacks in the Gulf last year were estimated to be more than USD$1 billion. In addition to these financial costs, OT cyber-attacks raise significant health, safety and environmental risks to the industry. This potent combination of substantial costs and heightened risk will keep OT cyber security top of mind for Middle East oil and gas companies.



To increase our understanding of the ot cyber landscape, this report focuses on:

OT CYBER RISK TODAY

First, we will look at the current OT cyber risk landscape for oil and gas companies in the Middle East. This section will provide insights into the types of risks companies face, where they are most vulnerable, and the impacts associated with OT cyber risk.

READINESS TO ADDRESS THE OT CYBER CHALLENGE

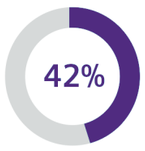
Second, we will evaluate these organizations' readiness to secure their operating environments and capture the full benefits of digitalization.

SOLUTIONS TO THE OT CYBER CHALLENGE

Lastly, we will analyze the survey results to identify the best path forward for oil and gas companies. Specifically, we will delve into the strategies, technologies and policies best-suited to help secure the entire operating environment.

OT cyber security presents unique challenges to oil and gas organizations that are different from traditional IT security concerns.

Cyber security challenges arise, in part, from the extended lifecycle of OT technologies.



of Middle East respondents said that outdated and ageing control systems pose a serious risk to their organizations.

Systems running older technologies are hard to patch due to their continual utilization and integration into wider production chains. The unique features of OT underscore the importance of purpose-built, multi-vendor solutions in the operating environment.

The operating model of some oil and gas organizations in the region often serves to introduce additional OT cyber risk. We have seen joint ventures between national and international oil companies with an absence of clear ownership of OT cyber risk. This disconnect – between operations and OT cyber – can expose dangerous gaps in cyber asset management and detection, and severely hamper cyber teams attempting to secure the environment.

Exploratory information is the area most vulnerable in the oil and gas value chain to a cyber attack.

When asked to identify the areas of greatest risk,

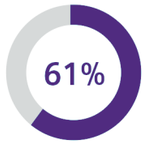


of respondents say it is exploratory information



say it is production information.

Other areas of vulnerability include:



potential partners and acquisition targets



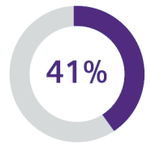
financial and organizational reports



operational information



details on drilling sites



and field production information from sensors

There is an absence of clear ownership of OT cyber risk in joint ventures.

The OT Cyber Risk Today

Oil and Gas OT environments face significant and mounting cyber security risk.

Sixty percent of respondents believe they face a greater risk in the OT than in the IT environment. Sixty-seven percent of respondents believe the risk level to industrial control systems over the past few years has substantially increased because of cyber threats.

These perceptions are, in fact, borne out in reality. A heightened risk environment is being driven by:

DIGITALIZATION OF INDUSTRIAL CONTROL SYSTEMS

The digitalization of industrial control systems and greater connectivity is creating a dramatically larger cyber "attack surface"

INTENSE GEOPOLITICAL COMPETITION

Intense geopolitical competition and aggressive nation-state actors actively targeting OT in the oil and gas industry

TAILORED MALWARE

The emergence of tailored malware designed to specifically impact OT

OUTDATED TECHNOLOGY

Outdated, legacy devices with little embedded security

Assessing Cyber Readiness Of The Middle East's Oil & Gas Sector

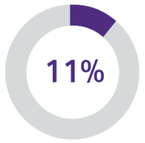
There are the critical differences between Operational Technology (OT) and Information Technology (IT)

IT INFORMATION TECHNOLOGY		OT OPERATIONAL TECHNOLOGY
3-5 years	Component lifetime	10-20 years & legacy systems
Mature stages & advanced cyber knowledge	Cyber market maturity	Early stages & limited awareness
Loss of data	Key concerns	Impact to production, health, safety & environment
Recover by reboot	Recovery ability	Fault tolerance essential
Continuous	Connectivity	Intermittent
Straightforward upgrades, automated changes	Ability to update	Typically difficult to patch, changes made by vendors

Cyber breaches in the OT environment are widespread and regularly go undetected



of organizations have suffered at least one security compromise that resulted in the loss of confidential information or disruption to operations in the OT environment over the past 12 months.



reported that they had experienced more than 10 cyber breaches in the OT environment in the preceding 12 months, a rate nearly three times the global average.

These numbers, moreover, likely under-report the true figures: forty-six percent of cyber-attacks are believed by respondents to go undetected. This data underscores that the OT cyber risk is not just theoretical, and that companies across the region are already being impacted.



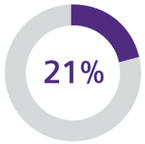
The process of digitalization is creating benefits for oil and gas companies (e.g. greater efficiencies, operational insights) but also generating significantly increased cyber risk, according to 62 percent of respondents.

This survey highlights the close linkage between digitalization and cyber security for the oil and gas sector. In order for organizations to capture the full benefits of digitalization, it is essential that they rigorously address the OT cyber risk.

Insider threat is viewed as the top threat to OT cyber security.



of respondents say the top cyber security threat is the negligent or careless insider



of respondents say it is the malicious or criminal insider, underscoring the need for advanced monitoring solutions to identify atypical behavior among personnel.



Insider Threat Risk

The prevalence of insider threat risk shows that traditional strategies of "air-gapping" networks are not an adequate security measure.

This approach cannot, for example, prevent the introduction of compromised transient assets like USB sticks. Instead of attempting to air-gap networks that cannot ever be truly isolated, organizations can strengthen their cyber defences by looking to gain visibility into their entire operating environment. This asset transparency is especially critical with remote sites like offshore platforms and wellheads.



WHAT RESPONDENTS SAY

HIGHLIGHTS

01 The majority of respondents believe that the OT environment is at greater risk of a cyber attack than that of IT.

02 Respondents attribute the cyber risk their organizations face to uncertainty about the cyber security practices of third parties in the supply chain and the difficulty in mitigating cyber risks across the oil and gas value chain.

03 Only one in three say their organizations' industrial control systems protection and security are adequate.

04 Three out of four say their organizations have suffered a security compromise that resulted in the loss of confidential information or disruption of operations in the OT environment in the past year. On average, respondents believe half of all cyber attacks in the OT environment go undetected.

05 Two-thirds say the primary cyber security threat they face is the negligent or careless insider.

06 Less than half the respondents say they continually monitor all infrastructure to prioritize threats and attacks.

07 Exploration data is most vulnerable to a cyber attack in the oil and gas value chain, according to the majority of respondents, followed by potential partners and acquisition targets, and product information.

08 Respondents believe the primary reason their organizations are at risk is a lack of cyber security awareness and training among employees. Other important factors perceived are a limited cyber security culture among vendors, suppliers and contractors, and the use of standard IT products with known vulnerabilities in the production environment.

09 While acknowledging that digitalization brings benefits, it also generates greater cyber risk, according to two thirds of respondents.

10 Two in three say security analytics are essential or very important to achieving a strong security posture.

2 Readiness To Address The OT Cyber Challenge



Best Practice In Cyber Security

Our study finds that oil and gas organizations in the Middle East recognize the growing OT cyber threat, as well as the imperative to strengthen their cyber readiness. In fact, Middle East organizations have already begun to take critical steps to improve their OT cyber security preparedness. Specifically, oil and gas companies in the Middle East have undertaken crucial steps such as:

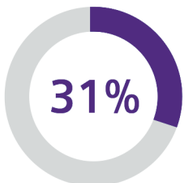
Creating dedicated, empowered OT security organizations, with a strong mandate and reporting lines up to senior leadership

Leveraging security analytics in order to enhance detection capabilities in their production environments

Partnering with OT security experts to develop a strong OT cyber strategy and create a culture of OT cyber security within their organizations

Deploying cutting-edge monitoring tools into their operating environments in order to gain transparency and rapidly identify potential cyber threats

Challenges To Cyber Readiness



of respondents say their organizations' industrial control systems' protection and security are adequate.

Oil and gas organizations in the Middle East face a similar set of challenges in maturing their OT security programs. First, companies often lack the internal expertise and trained personnel to build strong OT security programs. Second, many organizations do not have visibility into the assets in their operating environment, and cannot protect what they have not identified. This lack of visibility is compounded by the reality of multi-vendor environments, full of legacy assets, that have often grown over time without a clear plan to secure them.

Industry Needs To Keep Up

Despite awareness of rising OT cyber risk, budgets for OT cyber services and solutions have not kept up with the threat.

Oil and gas organizations in the Middle East are today dedicating only a third, on average, of their total cyber security budget to securing the OT environment. Given the risk shift we are witnessing in oil and gas – from the IT to the OT – this suggests that Middle East organizations are not aligning their cyber investments with where they are most vulnerable. This OT investment shortfall is all the more alarming as Middle Eastern oil and gas organizations reported smaller average total (IT + OT) cyber budgets than their global peers.

Cyber Security Journey

Most organizations are only at the early stage of their OT cyber security journey.

Just under two-thirds of respondents considered their OT cyber security programs at an early or middle maturity, with nearly a quarter saying they had the lowest level of OT cyber security maturity. In these lower maturity organizations, we see recurring traits that undermine effective OT security:

LACK OF DEDICATED PROGRAM

There is a lack of a dedicated OT program and ownership at many organizations. Often, IT departments attempt to simultaneously run OT security operations on the side. This approach rarely proves successful given the IT security group's limited understanding of unique OT technology, risks and culture.

ABSENCE OF CLEAR CYBER SECURITY STRATEGY

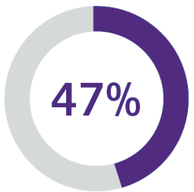
The absence of a clear OT cyber security strategy is another challenge. This greatly hampers the ability to detect and respond to cyber threats.

DEPLOYMENT OF TOOLS NOT SUITED TO OT ENVIRONMENT

Companies often deploy IT tools and technologies that are not suited for the OT environment. Traditional IT tools are not designed to work in OT networks, and introducing these solutions can pose serious risks to the production environment.

Completing Critical Tasks

Many tasks critical to OT security have not been completed.



of respondents say they continually monitor all infrastructures to prioritize threats and attacks.



of all cyberattacks in the OT environment go undetected, suggesting the need for investment in a solution that can detect cyber threats to oil and gas operations.

Fewer respondents say their organizations have the ability to assess risks to determine resources necessary to address the risks or pinpoint sources of attacks and mobilize to remediate the attack, according to 27 percent and 42 percent of respondents, respectively.

Oil and gas companies often struggle to address the fundamentals of OT cyber security.

For example, only 27 percent of respondents expressed confidence in their ability to, first, assess cyber security risks, and second, allocate the resources necessary to address those risks. This limitation is exacerbated by a widespread shortage of OT cyber talent. In order to address this acute talent shortage, governments and the private sector have important roles to play in supporting capacity building.

Assessing Cyber Readiness Of The Middle East's Oil & Gas Sector

Support From Ot Cyber Experts

Companies need experts that understand both cyber security and industrial control systems, a combination that is hard to find. Fewer than half of respondents (43 percent) thought they had the internal expertise necessary to manage cyber threats in the OT environment and, as a result, are increasingly seeking out external support. In particular, significant talent gaps exist for:



OT CYBER CONTROL ENGINEERS



INDUSTRIAL FORENSICS SPECIALISTS



OT CYBER PROGRAM MANAGERS



IN-FIELD OT CYBER FIRST-RESPONDERS

Middle East governments recognize this challenge, and have clearly prioritized developing domestic high-tech expertise through such efforts as Saudi's Vision 2030 plan.



3 Solutions To The Ot Cyber Challenge



Solutions To Achieve Cyber Readiness

While our study indicates that oil and gas organizations in the Middle East increasingly recognize the OT cyber challenge, there are fewer signs that they are adopting the most effective measures to address OT risk. Many have not moved past approaches that no longer work in an era of digitalization. For example, too many organizations are still attempting to "air gap" their operating environment, rather than using smart, secure connectivity to gain transparency. Moving from the mentality of "dig a deeper moat" to continuous asset visibility and intelligence is a foundational step in building a robust OT security program. More broadly, we see six, key principles underlying the most effective OT cyber programs:

Assign and empower dedicated ownership for OT cyber	1
Overcome the fear of connectivity and gain continuous visibility into your OT assets	2
Secure control of your operating environment all the way to the edge	3
Leverage analytics to make smarter, faster decisions	4
Demand purpose-built, OT cyber solutions	5
Partner with OT cyber experts with real domain expertise	6

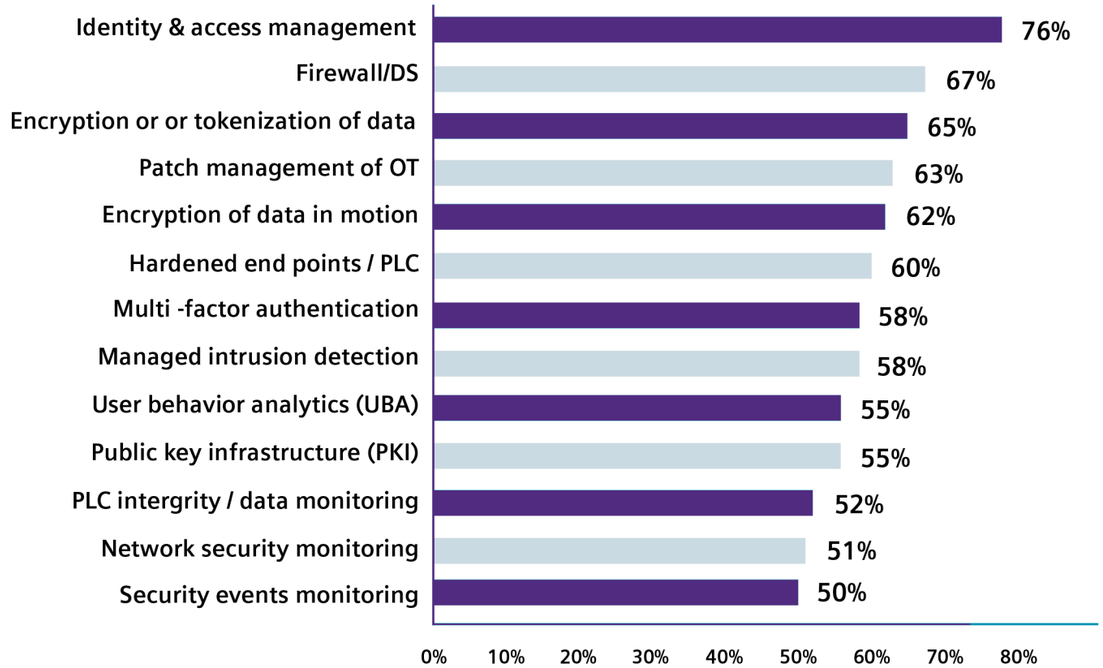
Many Companies Are Not Investing In The Most Effective Ot Cyber Tools

Only 39 percent plan to ensure hardened endpoints in the next 12 months, and only 20 percent will adopt analytics. The disconnect between establishing priorities and placing investments against those priorities highlights the importance for having a rigorous, long-term OT cyber security strategy.

Most Effective Security Technologies

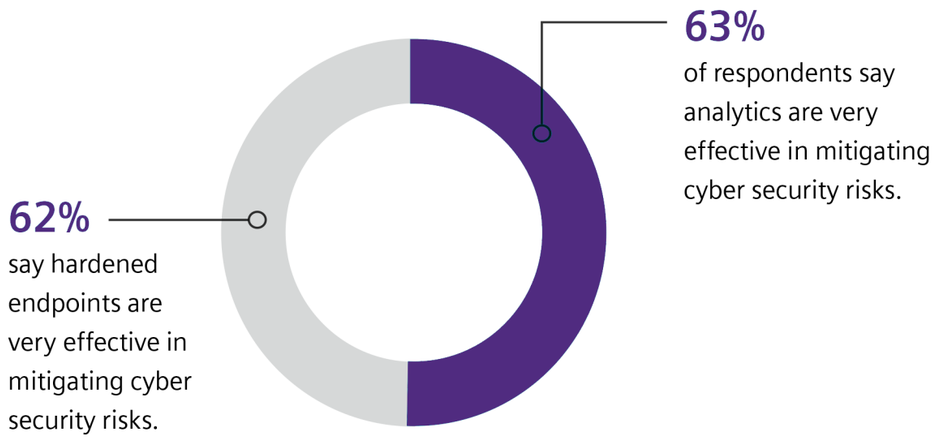
Respondents recognize and call for solutions to address insider threat, aging control systems and secure connectivity.

Very effective and effective responses combined



The Importance Of Security Analytics

Security analytics are widely considered to be the most effective technology in managing OT cyber risk.



The survey data shows the importance of addressing the fundamentals (e.g., hardening endpoints), as well as leveraging advanced technologies (e.g., analytics) to secure the OT environment. Oil and gas companies can also build on security analytics data to safeguard and optimize operational processes. By combining data from the network, controls and asset layer, organizations are enabled to reap important benefits around, for example, process safety in refining.

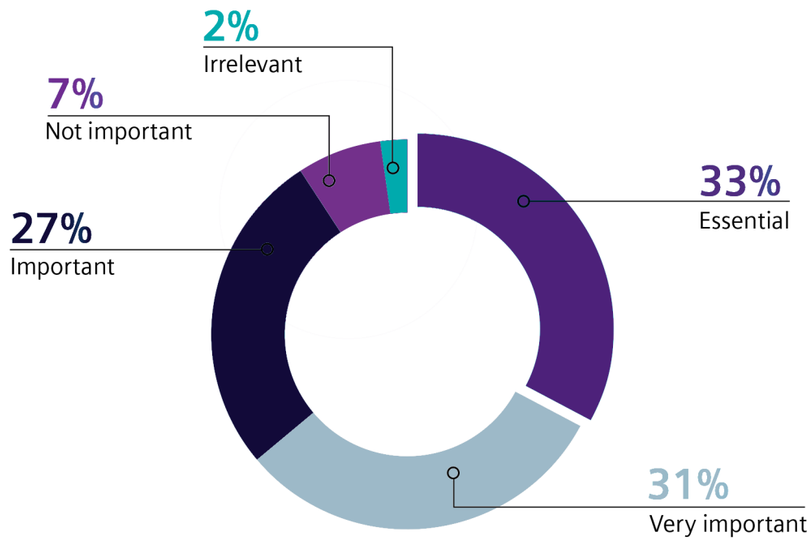
Organizations need to develop integrated OT cyber strategies that are adopted across the organization.

As shown in this research, organizational challenges create difficulty in strengthening OT security. Only 9 percent percent of respondents say there is full alignment between OT and IT with respect to cyber security. Though employee training and awareness is critical to developing a robust internal cyber culture, sixty-five percent of respondents say their organizations do not have initiatives in place that would build such a "cyber-safety" culture.

Assessing Cyber Readiness Of The Middle East's Oil & Gas Sector

The majority of respondents believe security analytics technology is essential or very important.

How important is security analytics technology to achieving a strong security?

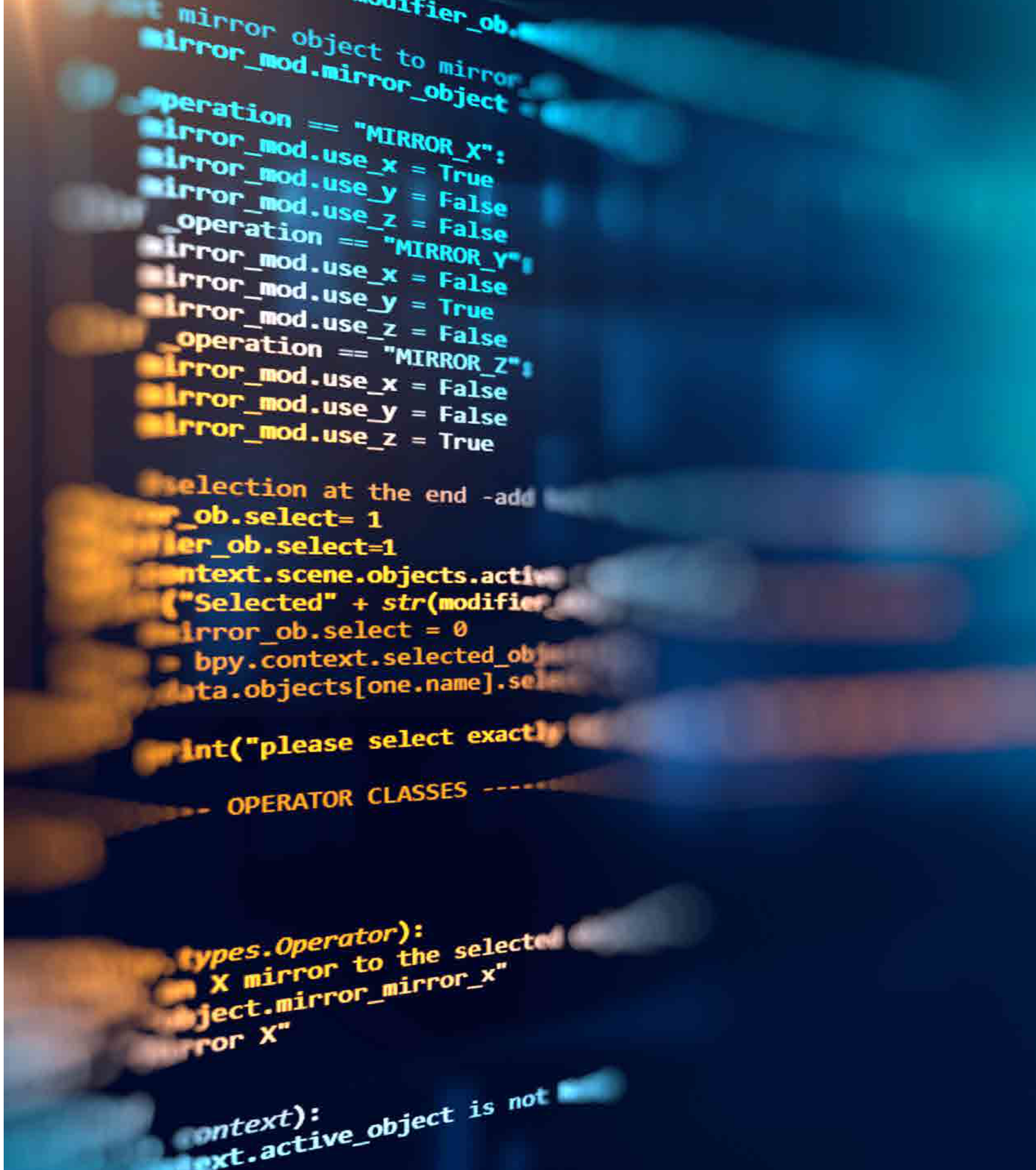




Conclusion

Our study reveals that oil and gas companies in the Middle East are aware of the growing OT cyber risk they face. They also increasingly recognize the actions they must take to strengthen their defences. They are investing more resources to develop the capabilities required, including qualified staff, to close this OT cyber readiness gap. These signs of leadership are welcome.

Taking the next step in this OT cyber security journey will require a more holistic strategy. Organizations that adopt both a risk-based and compliance-based approach to their OT security programs will be those who close the cyber readiness gap soonest. Those who show leadership in this challenge will look to leverage security analytics backed by deep domain expertise. Mature OT cyber programs will prioritize continuous visibility into their assets and vulnerabilities, so that they can intelligently, effectively prioritize. By ensuring asset transparency and rapid detection, organizations can best manage OT cyber risk and unlock the broader benefits of digitalization in the oil and gas industry.



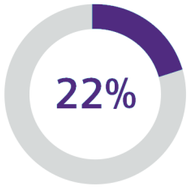
4 Methodology

In creating this report, we surveyed

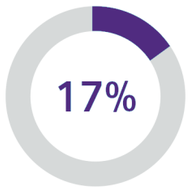


176

individuals in the Middle East



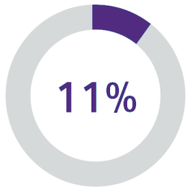
The majority of individuals surveyed report to the head of industrial control systems



Head of process engineering



OT security leader



IT security leader

who are responsible for securing or overseeing cyber risk in the OT environment. To ensure a knowledgeable respondent:

Respondents worked across upstream, mid-stream and downstream oil and gas operations.



Copyright of Siemens Energy Middle East
Masdar City
+971 2 616 5100

Siemens Energy is a registered trademark licensed by Siemens AG.