Report

GCC WATER & WASTEWATER SYSTEMS CYBER THREAT PERSPECTIVE

September 2022

DRAGOS, INC.

intel@dragos.com

@DragosInc

Executive Summary

The GCC countries are situated in an area that suffers from a scarcity of fresh water, where most of the Arabian Peninsula is made up of deserts with minimal natural freshwater resources. Without sustainable drinking water sources in most of the major cities in the region, life will be challenging and almost impossible for millions of people in the vast majority of GCC countries. Thus, governments started desalinating seawater at the beginning of the last century and continue to expand, with current efforts being influenced by the approval of the GCC Unified Water Strategy, 2016-2035, in 2016 by the GCC Secretariat General. This strategy was implemented to address the challenges facing the water and wastewater systems (WWS) sector in the region and its sustainability.[1] The GCC accounts for approximately 60% of the global desalinated water produced globally, where around 70% of the desalination plants in the GCC produce approximately 40% of the total world water desalination. As of now, 70% of GCC desalination plants use thermal processes such as Multi Stage Flashing (MSF) and Vapor Compression (VC). These processes require a significant amount of heat supplied by Oil and Natural Gas (ONG) sources to power the desalination plants and produce the required energy.[2]

The importance and the criticality of the WWS make its facilities part of the critical industrial infrastructure in the region. The impact of cyberattacks targeting GCC's WWS organizations could be significant, given that the GCC countries depend mainly on seawater desalination. In addition, the high dependency of the WWS sector on ONG as a source of energy will significantly impact the WWS sector's operation in case of an ONG outage. Dragos assesses with low confidence that in the next 12 months, cyber threat activities will impact organizations in the Water and Wastewater Systems sector in the countries of the GCC for the following reasons:

- The risk of destructive cyberattacks in the Middle East targeting industrial organizations.
- The increase of regional tensions between Iran and GCC countries due to the continuous Iranian support of the Houthi militia, which has overtaken the Yemen government. Furthermore, the GCC countries' oppositional political stand against the Iranian nuclear program will likely result in Threat Groups and their supported ransomware operators impacting industrial operations.
- The continued growth in the WWS sector, reaching around 6% annual growth as of 2009, along with desalination plants under construction promoting future growth, will likely attract cyber criminals and other adversaries to increase their activities, especially against small- to medium-size WWS organizations.[3]

Threat activities designed to target Operational Technology (OT) and Industrial Control Systems (ICS) require highly technical skills and deep specific knowledge of ICS/OT designs, processes, and operations. Out of many emerging cyber threats, ransomware is a major Information Technology (IT)-focused threat that can disrupt the operation of the ICS/OT environments, mainly if the IT/OT networks are not segmented properly. The risk of ransomware is that it is not limited to region, industry, or technology and can cause operational, financial, and/or reputational damages.

Dragos has observed during the past three years, espionage activities against the WWS sector, demonstrating the adversary's interest in gathering intelligence from WWS organizations and other non-WWS targets. Even though Dragos is unaware of any Threat Group impacting the ICS/OT infrastructure of a WWS organization, Dragos assesses with low confidence that multiple Threat Groups have the technical capabilities and the political motivations to attack the ICS/OT infrastructure of WWS in GCC countries. PARISITE, CHRYSENE, MAGNALLIUM, and HEXANE are examples of Threat Groups that have impacted GCC countries' organizations for political reasons. Dragos assesses with low confidence that adversaries with little to no ICS/OT capabilities will likely target organizations within the WWS sector in the GCC countries due to the following reasons:

[1] An overview of the GCC Unified Water Strategy (2016-2035) -Research Gate
[2] Desalination in the GCC. The History, the Present & the Future - General Secretariat of GCC
[3] Water market surges in the GCC - MEED

- Low maturity of small to medium-sized WWS organizations
- Unintentional exposure of ICS/OT assets to the internet
- Poor segmentation of IT/OT networks
- Lack of asset visibility by the asset owner

Key Findings

- Cyber risk to an organization depends on organizational cyber security awareness and preparation. Given the importance of the WWS vertical in the GCC region in the context of continuous regional political tensions, WWS organizations could be prime targets for any politically motivated adversary.
- The growth in the WWS sector will likely attract cyber criminals and other adversaries to increase their activities, especially against small to medium-size WWS organizations.
- Internet exposed assets, the digital convergence of IT and OT technologies and networks, supply-chain or third-party compromises all increase the risk surface for WWS organizations in the GCC.
- Dragos assesses with low confidence that multiple Threat Groups have the technical capabilities and the political motivations to attack the ICS/OT infrastructure of WWS in GCC countries.

Threat Groups

Dragos tracks six Threat Groups and various ransomware groups impacting GCC industrial organizations. Although Dragos is not aware of any Threat Group targeting ICS/OT environments of WWS in the GCC region, these groups are known to focus on industrial infrastructure in GCC countries.

Due to the increased tensions between Iran and GCC countries based on opposing political views in regard to the Iranian nuclear program and their support for the Houthi militia, Dragos assesses with low confidence that WWS organizations could be at risk by these Threat Groups as WWS falls under the umbrella of critical industrial infrastructure.

PARISITE

According to Dragos's research, PARISITE started its operations in at least 2017. This group is related to espionage activity targeting government and non-government organizations in the US, the Middle East, Europe, and Australia. Also, PARISITE targets various ICS verticals, including aerospace; ONG; and multiple utilities, including water, electric, and gas. This group uses open-source tools to compromise infrastructure and leverages known virtual private network (VPN) vulnerabilities for initial access. Dragos intelligence indicates that PARISITE serves as the initial access group that enables further operations for MAGNALLIUM.

Associated Groups: FoxKitten, Pioneer Kitten, MAGNALLIUM

CHRYSENE

CHRYSENE has continuously targeted the IT networks of multiple Industrial Infrastructure organizations since early 2017 in the Middle East, Europe, and North America. CHRYSENE is related to various campaigns targeting ONG, petrochemical, and electric generation sectors. Although CHRYSENE has yet to demonstrate an OT capability, the group's operations are consistent with initial access and information gathering operations against OT asset owners and operators that the Threat Group could use to facilitate a future attack.

Associated Groups: APT 34, GREENBUG, OilRig

MAGNALIUM

MAGNALLIUM has targeted energy and aerospace entities since at least 2013; its activities include espionage and destructive attacks. MAGNALLIUM initially targeted an aircraft holding company and ONG firms based in Saudi Arabia and expanded its targeting to include entities in Europe and North America. The group targeted other entities in joint ventures and other Saudi-related organizations outside the region, such as an aerospace company in the United States and petrochemical firms in South Korea. In 2020, Dragos identified three malicious Hypertext Markup Language (HTML) application samples like known MAGNALLIUM behaviors; the samples indicated possible targeting in the United Kingdom and the U.S., with a possible emphasis on semiconductor manufacturing and government entities. MAGNALLIUM lacks an OT-specific capability, and the group remains focused on initial IT intrusions. Dragos has observed several events where IT-focused threats gain access to OT due to a lack of proper segmentation, network misconfigurations, and open internet connections to ICS/OT environments.

Associated Groups: APT 33, Elfin

HEXANE

HEXANE is an industrial entity-focused Threat Group operating since at least 2018, with accelerated activity in early to mid-2019. Even though the group's primary targets are industrial entities, HEXANE showed interest in espionage and intelligence gathering activities. HEXANE utilizes third-party connections from telecommunications providers to gain access to networks for intelligence collection. HEXANE targeted Kuwait's ONG sector and telecommunication providers in the Middle East, Central Asia, and Africa. In addition, the group targeted third-party services in other regions to gain access to the primary target. HEXANE operations rely on delivering malicious document files to drop malware on victim machines via macros embedded in the spear-phishing documents.

Associated Groups: OilRig, Helix Kitten

XENOTIME

XENOTIME has been operating since 2016, targeting Electric Utilities and ONG operations in the Middle East, North America, Europe, and Australia. XENOTIME is responsible for the TRISIS incident targeting a Saudi Arabian ONG company in 2017, the only known ICS attack targeting process safety. XENOTIME has displayed the ability to penetrate control system environments and deliver tailored malware targeting specific Safety Instrumented Systems (SIS) platforms for operationally disruptive and potentially destructive purposes. Dragos assesses with moderate confidence that XENOTIME likely possesses capabilities to disrupt ONG operations in the North Sea. In January 2022, Dragos observed XENOTIME activity focused on research and reconnaissance against Liquefied Natural Gas (LNG) entities in Europe and the United States, both in the midstream and downstream verticals. XENOTIME activity currently appears to be the research of LNG entities and reconnaissance of LNG entity infrastructure.

Associated Groups: Temp.Veles

RASPITE

RASPITE, operating since at least 2017, targets victims in Saudi Arabia, Japan, Western Europe, and electric utilities in the United States. RASPITE relies on credential capture and reuse for access and movement throughout victim networks. Dragos's research shows that the RASPITE infrastructure has similarities with CHRYSENE registration activity, including the same hosting provider, adversary-owned name servers, and a slight overlap in registration details. At this time, RASPITE operations are limited to initial access operations on IT networks but remain focused on industrial-related organizations.

Associated Groups: Leafminer13

Threats to the Water and Wastewater Systems sector in the GCC

ICS-focused attacks

Dragos is aware of seven ICS malware strains that specifically impact ICS/OT environments: Stuxnet, Havex, BlackEnergy CRASHOVERRIDE, TRISIS, Industroyer2, and PIPEDREAM. Although Dragos has not observed any of these seven ICS-focused malware strains disrupt WWS sector operations, Dragos assesses with low confidence that malware could be developed specifically targeting WWS systems, much like the various ICS-specific malware strains previously seen. There is no evidence to support current capabilities being developed, however, well-funded, motivated Threat Groups could develop malware with focus on specific systems or industries. The high probability of the attacks against GCC's critical industrial infrastructure, including WWS, is based on the political tension in the region between GCC countries and Iran. One of the reasons for this political tension is that Iran is continuing to support the Houthi regime, which has overtaken the government in Yemen. The other reason is that the GCC countries' oppositional political stand against the Iranian nuclear program.[4] Due to this tension in the region, the Iranian government is

[4] US, E3 and GCC on Iran, Regional Tensions – United State Institute of Peace

continuously launching cyber and physical retaliation attacks against the critical infrastructure of GCC countries and United States allies. If successful in the WWS sector, such attacks will likely cause catastrophic impacts on human life and society.

Many water desalination companies in GCC produce electricity by utilizing steam turbines to generate enough electricity to cover their plants' needs, and they sell the rest to electricity companies.[5] Electricity generation puts these companies at similar cyber risks that the electric sector faces, including Threat Groups interested in electric utilities and electric-specific, ICS-focused malware such as CRASHOVERRIDE.[6] Dragos assesses with low confidence that adversaries could target the GCC's WWS organizations that generate electricity, given that they face a combination of water, electric, and regional threat vectors.

Considering the significant expansion in the WWS sector in the GCC region, more small to medium-sized WWS organizations are starting to operate water treatment and seawater desalination plants.[7][8] Small to medium-sized companies in all industries typically struggle to afford cybersecurity tooling and appropriate staffing to secure their networks. The significant risk against these organizations is that adversaries are likely to find them more attractive to attack compared to larger organizations where more security controls are in place, and potential attacks are not as successful.[9] The risks against the WWS sector's small to medium-sized companies include the risk of the adversaries using them as a testing ground to test their tools and capabilities and gain access to the internet-exposed ICS/OT assets.

In mid-2020, a Palestinian actor (referred to as Molerats), subsequently linked to Iran, allegedly targeted multiple WWS treatment facilities in Israel. Despite the limited information regarding the incidents, Dragos learned from multiple sources that the attacks targeted several internet-exposed Programmable Logic Controllers (PLCs) in multiple Israeli WWS treatment facilities. The adversary logged in remotely to the exposed assets and attempted to change the process environment of exposed chlorine control PLCs.[10] Dragos research shows that the actor "Molerats" mainly focuses on cyber espionage in GCC countries and has not demonstrated any ICS capabilities historically. Dragos assesses with low confidence that this actor has the technical capabilities and political motivations to perform similar attacks against WWS organizations in the GCC region when opportunities exist, such as internet-exposed ICS assets.

Espionage and Destructive Attacks

Espionage campaigns have been impacting organizations within GCC countries for several years. RASPITE, PARASITE, HEXANE, and CHRYSENE are the key Threat Groups observed attempting to compromise the region's IT infrastructure, including industrial, non-industrial, government, and private entities. In previous attacks, Dragos observed these groups attempting to establish footholds in GCC infrastructure, gather intelligence, perform infrastructure reconnaissance, exfiltrate data, and use compromised entities in GCC to conduct espionage operations against other regional targets. Dragos's research shows that since 2019, multiple adversaries attempted to conduct espionage operations against various WWS organizations in the GCC, including RASPITE, PARASITE, HEXANE, and CHRYSENE.

In addition, Dragos has learned from a private source that other active adversaries in the region, such as Muddywater and other allegedly Iranian-linked Threat Groups, targeted the IT infrastructures of multiple WWS organizations in

[5] Cogeneration Power-Desalting Plants Using Gas Turbine Combined Cycle - Intechopen
[6] TPS-2021-01: Global Electric Cyber Threat Perspective - Dragos
[7] GCC desalination projects' investment to reach US$100bn by 2020 – Technical review Middle East
[8] GCC desalination projects announced, emerging and nearing completion in 2020 – World Future Energy Summit
[9] Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure – FDD
[10] Implications from Recent Water and Port Activity in the Middle East - Dragos

GCC during the last two years. Since 2017, Dragos has identified multiple IT-focused wiper malware variants possibly linked to MAGNALLIUM and PARISITE. The two Threat Groups have been associated with a long-running campaign against the GCC government, ONG entities, and utilities (especially in Saudi Arabia). In 2020, Dragos identified a variant of ZeroCleare wiper malware called Dustman that targeted ONG and electric organizations in Saudi Arabia and Bahrain. The analysis of the adversary behavior associated with Dustman deployment and victimology suggests that PARISITE and possibly MAGNALLIUM are linked to these activities.[11]

The fact that wiper variants in the region continue to rely on the EldoS RawDisk driver to enable wiping operations suggests that adversaries will likely use similar methodologies in the future. Dragos assesses with moderate confidence that the IT-focused wiper malware variant will continue to pose threats to critical infrastructure entities in GCC. The use of this malware could extend to WWS organizations in GCC as well, based on previously mentioned regional tension, historical use of wiper malware, and continual retaliation operations.

Ransomware

Ransomware continues to be one of the most common and significant threats to industrial organizations worldwide. While ransomware variants are generally IT-focused, crippling the IT systems in industrial companies can impact the ICS/OT network's ability to operate. Dragos' analysis of 37 ransomware families shows that six ransomware strains, Cl0p, MegaCortex, Nefilim, LockerGoga, Maze, and EKANS, have the capabilities to impact certain functionalities of ICS/OT systems such as process kill functionality.[12][13] Dragos's analysis of ransomware trends and behaviors shows that state actors can use ransomware for political reasons, and that certain ransomware operators focus on specific industries.

Ransomware continues to pose a threat to any industry vertical with poorly segmented networks or internet exposed OT devices. In general, ransomware operators are opportunistic and continuously try to gain access to any infrastructure. The risk of ransomware threats against the WWS sector is more significant in some geographical regions than others, given in part to the number of facilities in each region. The number of known ransomware events is higher in the United States and Europe due to the focus of the ransomware operators on those regions for potential political or financial motivations.

During recent years, ransomware groups, including Maze, Ryuk, Sodinokibi, Conti, and Lockbit 2.0, impacted the IT services of WWS entities, however, the impact to OT operations are unknown. In these ransomware attacks, there was no identified trend of focusing on the WWS sector, but it was among the sectors that the ransomware operators were attacking. The WWS sector in the GCC region is no different, as the ransomware operators would use any opportunity to impact its entities. In addition, beyond just encrypting the companies' files and crippling their systems, ransomware operators increasingly incorporate data theft techniques into their campaigns to further ransom demands by threatening to publish the victim's data if a ransom demand is not paid. The increasing integration of OT and IT in industrial organizations increases the likelihood of ransomware attacks disrupting the operations of industrial organizations.

[11] Dustman Wiper Activity in Gulf Region - Dragos
[12] Dragos ICS/OT Ransomware Analysis: Q4 2021 - Dragos
[13] Dragos ICS/OT Ransomware Analysis: Q1 2022 - Dragos

Exposed assets

One of the most significant cyber risks to industrial companies is ICS/OT assets exposed to the internet. The 2021 Dragos Year in Review Report shows that 70% of Dragos services engagements involved issues with ICS network accessibility from the internet.[14] Dragos is aware of multiple ICS-targeting Threat Groups that attempted or succeeded in gaining initial access to industrial companies through internet-exposed ICS/OT assets and exploited remote access technology or logon infrastructure. In addition, Dragos has responded to ransomware events at industrial entities that leveraged internet-connected remote access portals to infiltrate the operations network and deploy ransomware.[15] In February 2021, the Oldsmar water system in the United States was a victim of an intrusion that impacted the Oldsmar city's water supply. The adversary gained access to the Human Machine Interface (HMI) on a workstation through TeamViewer, a remote access tool. Attempting to poison the water supply, the attacker changed the level of sodium hydroxide (NaOH); luckily, Oldsmar operators noticed the activities and prevented any risk to the public.[16]

In October 2021, the U.S. Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) published an advisory regarding malicious cyber activities targeting the U.S. WWS sector. The advisory encourages asset owners and operators to take immediate actions restricting exposure of OT assets to the internet. According to the advisory, behaviors observed between 2019 and 2021 include spearphishing to gain initial access to IT infrastructures, pivoting to ICS/OT environments, and connecting to internet-accessible PLCs that require no authentication using Remote Desktop Protocol (RDP) and VPN services.[17]

Dragos found multiple WWS ICS exposed assets in GCC countries, exposing the sector to the same threats in other regions. Dragos assesses with high confidence that internet-exposed ICS assets and connected services and applications enabling remote access to WWS in GCC are at significant risk of malicious cyber intrusions from Threat Groups and ransomware operators. In 2020, allegedly, Iranian cyber intrusions targeting water infrastructure in Israel resulted in PLCs being exposed to the open internet with or without weak authentication mechanisms.[18]

Supply chain and third-party threats

Supply chain compromise is another risk to any industrial vertical, including WWS, where the vendor's service itself becomes the attack vector. The risk of a supply chain attack is that it enables the adversary to bypass security mechanisms by exploiting trusted connections to a victim environment. SolarWinds Orion is an example of supply chain attack risk, where Dragos found in 2020, through multiple incident response engagements, that many industrial original equipment manufacturers (OEMs) embedded SolarWinds Orion software as part of their management offerings, and some of the OEMs were using the tool for access maintenance service monitoring.[19] Many ICS/OT systems were compromised when owners/operators installed the modified SolarWinds software or through their third-party's Contractors, vendors, and other third-party individuals often have direct access to operational environments for activities like updates, inspections, or new equipment installations. Adversaries can compromise equipment these individuals use as an access point to their ultimate target.

[14] Year in Review 2021 - Dragos
[15] Year in Review 2021 - Dragos
[16] Oldsmar Water Treatment Facility Cyberattack - Dragos
[17] Ongoing Cyber Threats to U.S. Water and Wastewater Systems - CISA
[18] Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran – Washington Post
[19] Responding to the SolarWinds Software Compromise in Industrial Environments - Dragos

Dragos observed that many small to medium-sized third-party companies and contractors are operating or co-operating WWS facilities, exposing these facilities to the carried-over cyber risks from the third-party companies and contractors. In addition, leveraging third-party connections can enable an adversary to conduct espionage, reconnaissance, and data theft operations to pre-position themselves for a potentially disruptive OT attack.

Vulnerabilities

According to the CISA's Fiscal Year 2021 (FY21) report, 37.4% of 44 WWS scanned entities in the U.S were using potentially risky applications, including RDP and VPN services, and 16.3% were using unsupported Windows Operating Systems on some of the internet-facing assets. CISA analysis shows that adversaries exploited several vulnerabilities in WWS entities' systems, including VPN services, web applications, mail servers, and security appliances. [20] Adversaries attacking entities in the GCC region are known to quickly weaponize and exploit vulnerabilities in internet-facing services, including VPN services, RDP, and network infrastructure. This includes PARISITE, MAGNALLIUM, and XENOTIME.[21] New vulnerabilities revealed throughout 2021 impact critical network infrastructure services, including F5, Palo Alto Networks, Citrix, and Juniper network devices, and are likely targets for adversaries. These vulnerabilities can enable adversaries to gain initial access to enterprise operations or pivot into industrial operational environments.

Vulnerabilities in ICS-specific devices and services can introduce risks to the WWS environment. According to Dragos' 2021 Year in Review report, the number of reported ICS vulnerabilities doubled compared to reported ICS vulnerabilities in 2020, as the number of ICS/OT vulnerabilities that Dragos researchers analyzed reached 1,703 CVEs. In addition, 35% of the advisories that Dragos analyzed could cause both a loss of view and control in an OT system which is among the worst operational scenarios in an ICS/OT environment. For instance, a loss of view or control may cause safety concerns and potentially put human safety and the environment at risk. Dragos encourages WWS asset owners and operators to be aware of the threat these vulnerabilities pose to their operations.[22]

Recommendations

Defensible Architecture Recommendations

Every ICS/OT environment requires a defensible architecture. This reduces cyber risks from an architectural perspective and enables the human defender. A defensible environment is not a defended environment. It takes a human to turn something from defensible to defended, but not all environments are defensible. Dragos recommends the following actions to develop a defensible network architecture.

- Install anti-virus/antimalware solutions on ICS workstations.
- Audit or scan systems, permissions, insecure software, insecure configurations, etc., to identify potential weaknesses and remediate as necessary.
- Limit access to resources such as file shares, remote access to systems, and unnecessary services over the network.
- Ensure an understanding of network interdependencies and conduct crown jewel analysis to identify potential weaknesses that could disrupt business continuity.
- Leverage industrial-specific threat detection mechanisms to identify malware within OT and reinforce defense-in-depth strategies at the network level, leading to defenders' and analysts' more robust investigation ability.

[20] Cyber Risk Summary: Water and Wastewater Systems Sector - CISA
[21] TR-2020-12: Remote Access Implementations and Activity Group Threats – Dragos
[22] Year in Review 2021 - Dragos

- Conduct architecture reviews to identify all assets, connections, and communications between IT and OT networks. Identify Demilitarized Zones (DMZ) to restrict traffic between enclaves. Critically examine and limit connections between corporate and ICS networks to only known, required traffic.
- Identify security zones and conduits based on security or process requirements. ISA 62443 Part 3-2 provides guidance on this process. The Purdue Model is an example of segmenting based on how close to a process a system is and is a good baseline.
- Store IT network, OT servers, and data historians that host services or data lakes in the DMZ. These resources should be accessed in the DMZ rather than allowing a straight IT-OT connection.

Monitoring and Visibility Recommendations

Monitoring a network can come in many forms, but in the focus of these controls, it is about helping maintain a defensible architecture and enabling a human defender to make it a defended environment. Improving – or, in many cases obtaining – visibility is crucial for identifying and defending against cyber threats. This includes long-term logging to investigate potential compromises as new information about incidents comes to light from intelligence sources. Dragos recommends the following steps to improve monitoring and visibility:

- Configure all capable devices and network components in the ICS/OT environment to send logging and monitoring data to a centralized system that is ICS/OT-aware.
- Configure network components to provide an increased level of logging and monitoring for those systems that do not have the native capability of providing logging and monitoring data to a centralized server.
- Utilize a supplemental ICS/OT-aware logging and monitoring system where possible to supplement the existing capabilities.
- Coordinate the ICS/OT-aware logging and monitoring system with a SOC to allow for greater visibility and quicker response.
- Passively identify and monitor ICS network assets to identify critical assets, chokepoints, and external communications in the network.
- Leverage industrial-specific threat detection mechanisms to identify malware within OT and reinforce defense-in-depth strategies at the network level to enable defenders and analysts to conduct more robust investigations.
- Orchestrate the direction of connections so that system-to-system connections go from higher-security zones to lower-security zones, i.e., OT to DMZ and DMZ to IT.
- Implement a default "deny" access policy across the IT/DMZ/OT trust boundaries. This approach is like a firewall policy where everything is denied unless specifically allowed. This type of policy can be labor-intensive and requires more administration, working with vendors, operators, and application management to define the minimal set of allowed protocols and ports.

Incident Response Plans

Dragos recommends that asset owners and operators establish, practice, and continuously improve ICS incident response plans to be prepared for when an incident occurs. It is essential to practice these response plans and incorporate them into Tabletop Exercises (TTXs) to identify chokepoints or problems in the response plan. Incident response plan documentation should define processes and procedures that assign specific roles for remediation along with thresholds for entering the remediation phase of incident response. Documentation detailing remediation steps within each business unit should include a recovery playbook. A continuous effort to identify and document affected systems should be organized once an event alert or notification has occurred. This allows recovery operations to account for resource requirements and equipment acquisition if necessary.

Remote Access Authentication

Remote access, whether internal to the company (IT remoting into OT) or external (OEM/Integrator remoting into the OT), is a leading attack vector. Currently, the most effective control is Multi-factor Authentication (MFA). Dragos recommends that MFA be implemented whenever possible. Understandably, MFA is not always possible; however, defensible architecture can compensate if MFA cannot be implemented.

- Establish remote connections made on request instead of always being accessible and monitor their usage to identify misuse or exploitation.
- Any remote access into the OT network from internet-exposed VPNs or access portals should require MFA. Additionally, any file transfer solutions should require MFA.
- Log and monitor access to remote sites from internet-exposed VPN or remote connectivity solutions. Use a "trust, but verify" approach to third-party and vendor access, as adversaries could utilize this trust relationship to access the OT network.

Key Vulnerability Management

Defenders should not assess all vulnerabilities with the same level of risk and priority for addressing in patch management practices. They should learn the effects that different vulnerabilities have and where adversaries need to be to exploit these vulnerabilities. With defensible architecture and monitoring in place, defenders are better positioned to identify and prioritize vulnerabilities that can have the most impact on reducing the threat surface and preventing exploitation by adversaries. Insights from defenders can identify and address the highest priority vulnerabilities from either a patching process or mitigating security controls.

- Unsupported Operating systems are a high-risk asset. The end of support means that these operating systems will no longer receive patches of any kind, including security patches. If an attacker could attack an unsupported operating system, that asset is at risk of vulnerabilities that came out after the end of the support timeframe. Coordinate with applicable vendors to develop a plan to upgrade hosts running operating systems that have reached, or are approaching, the end of support. While Microsoft has extended support for Windows 2012R2, asset owners and operators should consider working with vendors to upgrade these systems before reaching the listed support date.
- Prioritizing vulnerabilities that enable effects that allow adversaries either access to or the ability to interfere or manipulate an ICS process is crucial and should have a higher priority. However, defenders should determine what proximity and security controls are in place that an adversary would have to defeat to exploit vulnerabilities. Defenders should not use this as an excuse or cause for not addressing the vulnerability but in determining and ordering patching priority.
- Audit or scan systems, permissions, insecure software, insecure configurations, etc., to identify potential weaknesses and remediate them as necessary.
- It is imperative to give field personnel, engineers, and other OT asset operators ICS/OT-specific cyber security training and to include them in security discussions and make them aware of security policies and procedures.
- Establish, document changes, practice, and secure policies and procedures to assist in responding to and recovering from an OT-specific cyber event. This will also assist in identifying process or procedure operational gaps. Below is a comprehensive but not exhaustive list of recommended policies and procedures that should be common across ICS/OT environment security:
  - Asset Management - The process of receiving, tagging, documenting, and eventually disposing of equipment. Maintaining up-to-date inventory and asset controls is critical to ensure computer/field equipment locations and dispositions are known. Furthermore, when equipment is scheduled to be decommissioned, there should be a procedure documented that defenders can follow to ensure consistency and compliance with the process.

- Decommission/Disposal - This policy primarily addresses ensuring that old equipment does not contain sensitive information before removing it from possession.
- Change Management - This policy aims to reduce security risks that arise from changing devices, software, or configurations through documentation, approvals, and notifications.
- Device Hardening - This policy aims to reduce security risks that arise from changing devices, software, or configurations through documentation, approvals, and notifications.
- Disaster Recovery - This policy establishes lines of communication and the actions necessary to continue operations in the event of a disaster.
- Mobile Device Policy - A Mobile Device Policy would define the rules surrounding using mobile devices within the corporate and OT networks. Mobile devices, including laptops, smartphones, external hard drives, and tablets, can unknowingly facilitate the transport of malicious media across network boundaries and security zones. This policy would establish expectations and procedures designed to minimize incidents or risk exposure from mobile devices.
- Vendor/Transient Device Policy – This policy would establish expectations and treatment of vendor, third-party, or guest devices that can access OT networks.
- Password Policy - This policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. ICS/OT environments should have strict password requirements and policies addressing weak passwords, password age, lockout thresholds, and reuse.
- Patch Management – The process of distributing and applying updates to software and operating systems for both routine and emergency or critical updates.
- Remote Access – This policy defines the rules and requirements for connecting to ICS/OT networks from any host, including requirements for vendors or third parties. These rules and requirements are designed to minimize the potential exposure to ICS/OT networks from damages resulting from unauthorized use of ICS/OT resources. Damages include unintended catastrophic process failures, unintended exposure (population or environment), loss of control, loss of view, loss of availability, loss of confidence in the system, regulatory fines, sustained process inefficiency, or loss of public confidence.
- Data Retention- A retention policy sets expectations for how long various logs will be kept. This can also expose weaknesses in current retention policies and enable actions to gain visibility and long-term historical data to identify malicious activity.
- Vulnerability Management - This policy attempts to ensure personnel seek information on network and system vulnerabilities and address them promptly. The process also includes identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.
- Threat Intelligence and Vulnerability Sharing with Engineers and Operators - This policy establishes the importance of threat intelligence in securing the ICS/OT environment and drives efforts to collect and act on it. It also provides engineers and operators awareness of threats and identifies possible suspicious cyber activity.
- Unmanaged and Transient Device Policy – This policy establishes procedures and policies around unmanaged devices that are consistently or temporarily but often connected to ICS/OT networks. This includes minimum specifications for device security, device hygiene, and logging to be allowed to access the network and its resources or make changes to connected ICS/OT assets.

Conclusion

The WWS sector is a crucial foundation for civil society in the GCC as WWS organizations in the region account for around 60% of the desalinated water produced globally. The WWS sector in GCC remains at risk given the continual political tensions, and the presence of other industrial vertical focused threats. Even though Dragos has not observed any Threat Group activity against WWS organizations in the GCC region, Dragos assesses with low confidence that WWS organizations in GCC are at risk of being targeted by these Threat Groups and adversaries with no or low ICS/OT capabilities as the WWS organizations fall under the umbrella of critical industrial infrastructure. In addition, the risks of continuous ransomware activities, internet exposed assets, vulnerable services, supply chain attacks, third-party compromise risks, and growing IT/OT convergence are contributing to the growing threat landscape. Dragos continues to monitor malicious threat groups and threats targeting the WWS sector in GCC.

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT

www.dragos.com.

THANK YOU