



DEFENSIBLE CYBER POSITION IN INCIDENT RESPONSE

Abstract

Defensible Cyber Position refers to an organization's ability to quickly harden and isolate its digital environment – maintaining only essential operations – in the face of a cyber incident. In practice, this means having a pre-planned “safe mode” for your network and systems that can be activated during attacks. The goal is to reduce the attack surface and contain threats while keeping critical business or industrial processes running in a limited capacity. This concept originated in industrial control system (ICS) security, but it now applies broadly to IT environments as a key part of incident response preparedness. In a defensible cyber position, non-essential connectivity is cut off and only the minimum required systems remain operational, allowing incident responders to **“fight through” an attack** without total shutdown. Below, we provide a comprehensive guide to what a defensible cyber position entails, the controls needed, real-world examples, industry-specific practices, relevant frameworks, and tools to achieve it.

What Constitutes a Defensible Cyber Position?

A defensible cyber position is a state of enhanced security posture that an organization can enter during heightened cyber threat conditions or active incidents. It is characterized by deliberately **reverting to a resilient, minimal operating state** that is easier to defend. SANS Institute defines a defensible architecture as one that “reduces as much of the agreed-upon risk as possible through system design and implementation while also facilitating the efforts of human defenders”. One attribute of such an architecture is *“the ability to go into a ‘defensible cyber position’ with reduced connectivity and devices during heightened situations.”* In other words, the organization can temporarily shut off unnecessary network pathways and devices, isolating critical systems into a hardened enclave.

In a defensible cyber position, **connectivity is limited to known-essential communications only**, greatly constraining an attacker’s freedom of movement. This often involves **network segmentation** “choke points”, strict access controls, and use of pre-established safe modes. The control system or business can continue to function in a degraded but safe state while responders work to neutralize the

threat. For example, an industrial plant might disconnect external IT networks and move certain operations to manual control; a corporate IT network might isolate infected segments and run critical applications from clean backup infrastructure. The key is that these actions are **planned and tested in advance** as part of the incident response plan, not ad-hoc. Having the option to quickly transition into a defensible state is now considered a hallmark of mature cyber preparedness.

Common features of a defensible cyber posture include robust asset identification (knowing what must be kept running), **network segmentation**, understanding which communications can be one-way or disabled, comprehensive logging/monitoring to inform decisions, and predefined procedures to isolate or shut down systems if needed. Ultimately, a defensible cyber position lets an organization contain damage and *control the battlefield* during an incident, rather than being forced into complete outage or remaining fully exposed to attackers.



Tactical and Strategic Controls Enabling a Defensible Position

Achieving a defensible cyber position requires implementing both strategic architectural controls *before* an incident and tactical controls that can be executed *during* an incident. Strategic controls establish technology and processes to make your environment defensible, while tactical controls are the specific actions taken in real time to actually harden or isolate systems. Below we outline key controls and practices in both categories:



- **Network Segmentation and Zone Isolation:** Strategically divide networks into segmented zones (e.g. by business function or sensitivity) with strict controls at connection points. This limits pathways for threats and allows sections to be isolated when needed. For example, ICS networks should be separated from corporate IT via firewalls and demilitarized zones (DMZs). During an incident, defenders can then **isolate affected segments** by closing firewall gateways or physically disconnecting links. Strong segmentation creates “choke points” that make it feasible to contain malware spread. CISA and the FBI specifically recommend “**robust network segmentation between IT and OT networks**” as a mitigation to improve resilience against ransomware. (See Figure 1 below)

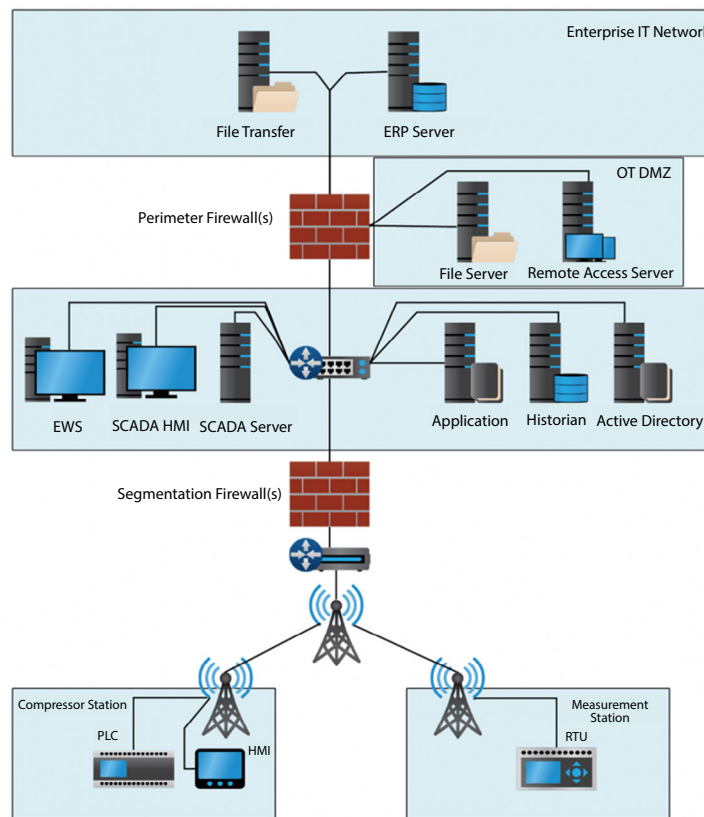


Figure 1: Example of a segmented ICS network architecture with an enterprise IT zone, an OT DMZ, and separated control system layers. Defensible architecture uses such segmentation and firewall choke points so that critical systems can be isolated from threats if necessary.



- **Rapid “Kill-Switch” Isolation Capabilities:** Tactically, organizations need the ability to **quickly disconnect or power down systems** and networks when an incident escalates. This could be a literal network kill-switch (e.g. cutting power to network gear, or an emergency shutoff for wireless access points) or logical isolation (such as invoking a script that updates firewall rules to block all traffic to a certain subnet). In practice, incident responders often have to quarantine infected servers or PCs – for example, by yanking network cables or disabling switch ports. In the 2017 NotPetya attack, Maersk **physically unplugged devices and disconnected its entire global network** within a couple of hours to stop the malware’s spread. Such drastic isolation is a hallmark for entering a defensible cyber position. It’s important, however, to plan these kill-switch actions carefully: **test them** in advance and understand the impact. Guidance for industrial networks suggests attempting logical isolation (firewall blocks, disabling services like RDP) before resorting to pulling cables or shutting down equipment, to avoid unintended safety impacts. Nonetheless, having a last-resort mechanism to sever connectivity is crucial for containment.



- **Disabling Non-Essential Services and Accounts:** A key tactical measure during incidents is to **turn off any services, processes, or user accounts not needed for core operations**. This reduces the attack surface immediately. For example, if a server is only needed to perform a specific task, administrators should be ready to stop or disable ancillary services (print spoolers, file shares, etc.) in an emergency. In ICS environments, this might mean switching off data flows that aren't critical to keeping the physical process running. During incident response in an OT plant, defenders might block certain PLC communication paths or kill workstation applications that aren't required for safety. The Public Safety Canada guidance for ICS incident response explicitly notes that countermeasures can include *"disabling services that are not in use currently"* as part of hardening during an incident. Likewise, **unnneeded remote access sessions should be terminated** and VPN accounts disabled. Disabling or blocking these "noise" services makes it harder for an attacker to maneuver and easier for defenders to monitor the truly important systems.



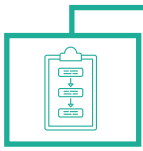
- **Limiting Remote Access (and Cutting It in Emergencies):** Remote connectivity often serves as a gateway for attackers, so both strategic and tactical controls are needed. Strategically, enforce **secure remote access**: use jump servers, VPNs with multi-factor authentication, strict hours, and limit remote access privileges to only what's necessary (principle of least privilege). Segment third-party access into its own zone. Tactically, when threat levels are high or an incident is detected, be ready to **"completely disconnect remote access during an incident response"**. Many organizations have an internal playbook step to shut off VPN concentrators or remote desktop gateways if ransomware is spreading, for example. By cutting external access, you prevent attackers or malware from using those pathways to spread or exfiltrate data. In effect, the environment is put into **local mode only**. This was seen in the Colonial Pipeline incident (2021) – although the ransomware hit IT, the company **preemptively halted all OT operations and remote connections** as a precaution, isolating the control network from any IT infiltration. Testing this capability is important so that, in a crisis, flipping the switch to block remote access (or enabling a pre-configured "maintenance mode" firewall policy) can be done smoothly.



- **Pre-Defined Segregation of Critical Assets:** Strategically, identify your "crown jewels" – critical databases, industrial controllers, payment systems, etc. – and **architect their environment such that they can run independently if needed**. This may involve maintaining redundant local control for critical ICS components or offline access to key business data. For example, a bank might ensure that its core transaction processing can be isolated from the internet and continue operating from backup sites if the corporate network is under attack. A hospital may keep certain life-support systems on a separate network that can be run if the hospital IT network must be shut off. By **mapping dependencies in advance**, you can create emergency configurations that supply power, network, and authentication to critical systems in a standalone fashion. This might also include having *manual workarounds* (see below). The idea is to **minimize interdependencies** so that you can safely pull the plug on non-essentials without causing critical functions to fail.



- **Comprehensive Monitoring and Visibility:** You cannot defend or isolate effectively without visibility. As a strategic measure, deploy extensive logging and network monitoring so that you know what "normal" looks like and can quickly spot malicious activity. Collect network traffic from key segments and enable system logs on critical hosts. This not only helps detection, but during an incident it guides where to isolate – e.g., knowing which subnet shows abnormal traffic. Good visibility also means you can be surgical: perhaps isolated at a specific firewall choke point to block an attacker's movement while avoiding taking down an entire site. In ICS, one attribute of defensible architecture is *"collecting network traffic and logs from systems of value"* – this situational awareness is vital when deciding to activate a defensible cyber position. Additionally, monitoring tools should have triggers or automation to assist in the transition (for instance, an IDS that can signal a firewall to cut a connection when a certain condition is met).



- **Tested Manual Operations and Fallback Procedures:** A defensible cyber position often entails running in a degraded mode. **Ensure that personnel know how to operate systems manually or in offline mode.** This is both a strategic preparation and a tactical action when needed. In industrial settings, this may mean operators can control the process via local panel HMIs or by manual valves if the SCADA system is isolated. In enterprise IT, it might involve shifting to read-only access of a recent data snapshot, or using pre-prepared spreadsheets to track transactions while systems are down. For example, **many hospitals train for “downtime procedures”** – if their electronic health records are unavailable, staff revert to paper forms and manual scheduling. Such fallback modes were critical during the 2020 Universal Health Services (UHS) ransomware attack, where UHS had to **shut down IT systems across 250 hospitals** and revert to offline documentation for nearly two weeks; patient care continued via these backup processes. The Joint Commission (hospital accrediting body) overtly *requires* healthcare providers to have manual downtime procedures as part of continuity plans. Testing these procedures via drills or tabletop exercises is crucial so that the “people” part of your defensible position is as ready as the technology.

In summary, enabling a defensible cyber position involves building a resilient architecture (segmented networks, safe fail-safes, visibility) and having decisive actions defined (kill switches, service shutdown, access restrictions, manual failovers). These controls work in concert: **architecture provides the means, and response playbooks provide the execution.** An organization that has invested in both can confidently isolate threats while keeping the lights on in a crisis.

Case Studies: Defensible Posture in Action

Real-world cyber incidents illustrate the importance of having a defensible cyber position – or suffering the consequences of not having one. Below are a few prominent examples from recent years (LockBit ransomware, NotPetya wiper malware, and Colonial Pipeline ransomware) and how organizations responded, highlighting lessons about defensible postures.



NotPetya (2017) – Global Outbreak and Network Shutdown: The NotPetya malware struck dozens of companies worldwide in June 2017, spreading rapidly inside networks via automated propagation. A notable victim, Maersk (a shipping giant), experienced an *almost total IT meltdown*. NotPetya moved laterally through Maersk’s flat network, knocking out servers and PCs in minutes. In response, Maersk’s IT staff **raced to isolate the infection by disconnecting machines and pulling the company off the network.** Employees were literally running through hallways unplugging ethernet cables. It took about *two hours* to disconnect Maersk’s entire global network – but this drastic action prevented further corruption of systems. With their network and applications down, Maersk resorted to manual operations (e.g. using personal phones, whiteboards, and paper) to keep critical port operations running until systems were rebuilt. This case highlights the value of a kill-switch equivalent: Maersk had no pre-planned network kill-switch, so humans served as one. Organizations learned from NotPetya that **segmentation and prepared isolation procedures** could have dramatically limited the worm’s spread. NotPetya’s impact (over \$10 billion in damages globally) became a rallying point for embracing defensible cyber postures in both IT and OT: if you can swiftly compartmentalize your network, you can contain even fast-moving threats. Companies subsequently invested in redesigning network topologies to avoid the one-big-network vulnerability that NotPetya exploited.



Colonial Pipeline (2021) – Isolating OT from IT Ransomware: In May 2021, Colonial Pipeline, which operates a major fuel pipeline, suffered a ransomware (DarkSide) attack that impacted its business IT network. **While the OT control systems were not directly hit,** the company immediately took a defensible stance by shutting down OT operations to prevent any spillover and to err on the side of safety. Colonial Pipeline’s decision to break the pipeline was an *OT isolation maneuver* – they severed the integration points between IT & OT to make sure the ransomware could not reach pipeline controls. This caused a temporary operational outage (with societal impacts, e.g. fuel shortages), but it was deemed the safest option given the uncertainties. The incident underscored how interwoven IT and OT had become; Colonial’s network segmentation was not strong enough to guarantee the malware couldn’t jump, so the **only defensible position was a full stop of data flows.** Following the incident, U.S. government advisories urged critical infrastructure operators to implement better segmentation between corporate and control networks, regularly test manual controls for operations, and ensure backups of critical OT data are offline. Colonial’s experience is a prime example that sometimes **the most defensible action is a proactive shutdown** of parts of the network – a tough call that must be planned in advance with management’s buy-in. With proper network design (e.g. one-way data diodes, layered access) and an exercised incident response plan, operators can isolate threats with more nuance than simply “pull the plug,” potentially avoiding a total outage. This case prompted many in the energy sector to revisit their incident response plans and ensure they include steps to quickly isolate or disconnect OT in a crisis.



LockBit Ransomware (2020s) – Containment in Enterprise Environments: LockBit is a prolific ransomware-as-a-service operation that has victimized organizations across sectors (including financial services, government, manufacturing, and healthcare). A common theme in LockBit incidents is the race between the spreading of ransomware vs. defenders isolating systems. For instance, in early 2023 the UK's Royal Mail was hit by a LockBit attack that encrypted critical servers used for international mail. **Royal Mail had to resort to manual processes for several weeks**, such as hand-processing customs forms and offline logging of shipments, because the affected systems were isolated. International mailing was halted until systems could be safely restored. Royal Mail's response – isolating the compromised IT systems from the rest of the network and switching to fallback procedures – prevented wider IT collapse but at the cost of operational slowdown. In other LockBit cases, organizations with strong endpoint detection and network segmentation have managed to contain the damage. For example, if ransomware starts encrypting a file server, a well-prepared incident response team might **quickly disconnect that server and its network segment**, limiting LockBit's reach to only a subset of systems. CISA and international CERTs have emphasized that network segmentation, offline backups, and incident response drills are key mitigations against LockBit. Unfortunately, some victims discovered their defenses were not "defensible" enough only after the fact – e.g., flat networks allowed LockBit to traverse and encrypt hundreds of machines. On the other hand, companies that implemented measures like admin credential vaulting, network isolation protocols, and one-click host quarantine via EDR fared much better in limiting the blast radius. The takeaway from LockBit and similar ransomware is that **speed and preparation determine outcomes**: if you can isolate the threat swiftly (network-wise and process-wise), you turn a potential organization-wide catastrophe into a contained incident.

These cases reinforce that a defensible cyber position is not theoretical – it has very tangible benefits. Whether facing a fast-spreading worm (NotPetya), a critical infrastructure ransomware (Colonial), or an enterprise-wide ransomware (LockBit), those who could rapidly isolate and maintain partial operations suffered far less impact than those who could not. The cost of implementing such capabilities is far less than the cost of business downtime or compromise. Next, we'll look at how different industries incorporate these principles, since the approach must be tailored to the environment.



Industry-Specific Guidance and Considerations

Different industries have unique operational requirements and constraints that shape how a defensible cyber position is implemented. Below we examine three contexts – **Industrial/OT (Operational Technology)**, **Financial Services (BFSI)**, and **Healthcare** – and highlight sector-specific guidance and best practices for establishing defensible positions.

OT/ICS Environments (Industrial Control Systems)

Industrial control system (ICS) and OT networks (found in manufacturing, energy, transportation, etc.) were the birthplace of the “defensible cyber position” concept. In these environments, **safety and availability are paramount** – any incident response action must avoid causing physical process disruptions that could harm people or equipment. Thus, OT defenders plan carefully how to isolate or degrade systems in an incident. Key industry guidance includes the **Purdue Model** of ICS network segmentation and standards like **ISA/IEC 62443**, which provide frameworks for securing control system architectures. The aim is to have layered defenses so that if one part of the system is compromised, it can be walled off.

Segmentation and “Safe Mode” Operation:



OT networks are typically segmented into levels (Level 0/1 for field devices, Level 2 for control systems, Level 3 for operations management, and Level 4 for enterprise IT, etc.). Strict firewalls or data diodes are used between these levels. SANS recommends *strict separation between IT, OT, and the Internet* for a defensible architecture. By narrowing digital pathways, ICS operators can enter a defensible position by closing the few junctions between OT and external networks. For example, an electric utility could disconnect its control center from external networks (including corporate IT and vendor connections) if a cyber threat is detected, effectively islanding the grid’s control systems. The **goal is to isolate operations as much as possible to reduce impact on physical processes**. This might mean running a pipeline or factory in a local-manual mode, with remote monitoring cut off. Indeed, official guidance in Canada and the U.S. suggests that a defensible cyber position for ICS may involve disconnecting from business networks, OT DMZ, and even segmenting within ICS (separating process A from process B) to contain threats.

Manual Operations and Failsafes:



Unlike purely digital businesses, industrial systems often have analog or manual fallbacks. Industry best practice is to **ensure the ability to run the process in “manual mode” or fallback control** if the digital systems must be isolated. This can involve local control panels on machines, manual safety interlocks, and procedural workarounds. For instance, a chemical plant might have a procedure to have operators physically adjust valves and maintain safe operation if the central SCADA is unavailable.

Testing these scenarios is critical. The SANS ICS security framework urges organizations to *test their defensible cyber position, perhaps via drills during scheduled downtime, to verify that operators can actually run in that constrained mode*. Only 56% of organizations in a recent ICS cybersecurity survey had tested their “manual mode” plans, highlighting room for improvement in the industry. When an incident occurs, having pre-trained the engineering staff on how to maintain production (perhaps at reduced capacity) while cut off from corporate IT or internet makes a huge difference. A famous example was the 2017 Triton malware attack on a Saudi petrochemical plant – the plant was able to safely shut down due to fail-safe controls even as the attackers tried to tamper with safety systems. This underscores that **safety instrumented systems and manual shutdown procedures** are part of a defensible posture in OT.

Operational Constraints:



One challenge in ICS/OT is that systems often cannot be patched or rebooted frequently, and incidents might have to be contained for a long time before full remediation (perhaps waiting for a maintenance window). This places extra emphasis on containment and monitoring. Guidance from CISA and others often notes that in OT incidents, *containment can occur safely, yet eradication (e.g., wiping malware) may have to wait until the next scheduled outage*. Therefore, OT incident response plans focus on **securely maintaining operations in a compromised environment** – truly “fighting through” the attack. Defensible positions in this context might last for days or weeks, requiring continuous monitoring of the threat while the process keeps running in isolation. Tools like unidirectional gateways (one-way data diodes) are sometimes used to allow outbound monitoring data without inbound control, as a way to keep an eye on things during isolation. Additionally, **in OT, every isolation step must consider safety**: e.g., if you cut off a remote station’s network, does the local controller have everything it needs to run safely? These details are hashed out in incident response playbooks specific to ICS. The **NIST SP 800-82** “Guide to ICS Security” and sector-specific standards (like **NERC CIP** for electric utilities) provide guidance on designing networks and response plans that can achieve these goals. In summary, industry advice for OT is to *prepare a “limp along” mode for critical processes*, invest in network architecture that supports isolation, and practice switching to that mode. When done correctly, a defensible cyber position in ICS can allow continued production or at least a safe shutdown, while cyber teams contain the adversary in a corner.

Financial Services (BFSI)

Banks, financial services firms, and insurance companies have been prime targets of cyber-attacks, from ransomware to nation-state hacking. The financial sector has a strong emphasis on resilience and has developed extensive incident response and business continuity plans. For BFSI, a defensible cyber position centers on **protecting the integrity of transactions and data** even under attack, and meeting tight regulatory requirements for continuity. Key considerations in this industry:

Ring-Fencing Critical Systems:



Financial institutions typically identify certain systems as critically important (e.g., core banking systems, payment processing systems like SWIFT connectivity, trading platforms) and apply extra isolation around them. For example, SWIFT – the inter-bank messaging network – has its own Customer Security Controls Framework (CSCF) that mandates members to implement a secure zone separated from the rest of their IT. One requirement “emphasizes the importance of isolating SWIFT-related systems from other, potentially less secure, parts of the network.” Banks comply by hosting SWIFT servers in dedicated secure enclaves with strict access controls, no internet connectivity, and unidirectional access rules. In practice, if the bank’s office IT is breached, the SWIFT environment should remain walled off – and in an extreme case, the bank can disconnect the SWIFT zone entirely and revert to contingency procedures for payments. Similarly, core banking databases might be replicated to a hot DR (disaster recovery) site that isn’t reachable from the user LAN, so that if the user network gets hit by ransomware, the core data remains safe.

Regulatory and Crisis Management Requirements:



The BFSI sector is heavily regulated in cybersecurity. Regulators and industry bodies (like the FFIEC in the US, ECB in Europe, MAS in Singapore, etc.) require robust incident response and often conduct sector-wide exercises. Banks must have *disaster recovery (DR) sites, cyber incident response plans, and conduct regular drills*. A defensible cyber position for a bank often means **failing over to backup systems or alternate networks** in a controlled way. For example, many large banks have completely separate infrastructure for critical processes that can be activated if the primary is compromised – akin to a parallel environment that is maintained in isolation and kept updated (sometimes called a “sterile recovery environment” or “cyber recovery vault”). In incident response terms, a bank might decide to isolate its primary data center and switch operations to the DR site if an attack cannot be contained otherwise. This was practiced during industry simulations like SIFMA’s **Quantum Dawn** exercises, where firms respond to massive cyber attacks by isolating affected business units and relying on backup communication channels.

Another aspect is communication with central banks and regulators. Financial services firms need to coordinate on sector stability. If a major bank is compromised, regulators may even

instruct them to disconnect from certain networks (to prevent, say, malware propagating to the interbank network). Thus, defensible posture might extend beyond one organization to *sector-wide isolation measures*. The **Financial Stability Board (FSB)** has issued guidance on response and recovery, urging firms to address gaps in their cyber incident response capabilities and ensure continuity of critical clearing and settlement functions [fsb.org](https://www.fsb.org). In practical terms, the industry has developed playbooks for scenarios like “ransomware on a trading day” – e.g., the playbook might say to move trading to a contingency system and isolate the affected trading floor network.

Examples and Controls:



A notable banking incident was the 2016 Bangladesh Bank heist, where attackers breached the bank’s network and attempted fraudulent SWIFT transfers. In response, some banks globally **segregated their SWIFT terminals** from the general IT and put in place “circuit breakers” to swiftly disconnect those systems if suspicious activity is detected. Banks also employ **Network Access Control (NAC)** tools to isolate infected endpoints – for instance, if an employee laptop is found with malware, NAC policies can auto-quarantine that device on a separate VLAN. Many large financial institutions also use **user behavior analytics and anomaly detection** to catch intrusions early and enact containment. For ransomware, the common defensive position is to *isolate branch office networks or subsidiaries to prevent spread to the core*. Because banks often have many interconnected subsidiaries, they use segmentation to make sure a compromise in a smaller affiliate doesn’t pivot into the main bank. Additionally, BFSI has a big focus on **data vaulting**: keeping immutable backups of critical data offline (the concept of *Sheltered Harbor* in the U.S. is an initiative to store critical account data in a vault that can’t be electronically wiped). This means if systems are ransomed, the bank can disconnect the infected systems and later restore from the vault with minimal data loss.

In summary, financial industry guidance encourages a **conservative, readiness-focused approach**: assume you will be hit, ensure you can cordon off the incident, and continue serving customers (even if at reduced capacity). That could mean processing transactions in batch mode once a day instead of real-time, or using manual trade booking if systems are down. The combination of stringent **regulations, sector drills, secure enclaves (like the SWIFT secure zone)**, and heavy investment in redundancy makes BFSI relatively well-prepared to adopt defensible cyber positions. However, the complexity of large financial networks still poses challenges – ensuring every connection has an off switch is non-trivial. Thus, ongoing efforts in this sector include adopting **zero trust architectures** (to continually enforce segmentation at a granular level) and improving orchestration so that isolation actions can be executed rapidly across a sprawling infrastructure.

Healthcare

Healthcare organizations (hospitals, clinics, pharmaceutical companies) face the dual challenge of protecting sensitive data and ensuring patient safety. Cyber attacks on healthcare can directly impact human life, as evidenced by ransomware incidents leading to delayed treatments or diverted ambulances. Therefore, the concept of a defensible cyber position in healthcare revolves around **maintaining the ability to deliver patient care, even if that means reverting to pen and paper**, while containing the IT threat.

Network Segmentation of Medical Devices:



Modern hospitals are full of network-connected medical devices (imaging machines, IV pumps, monitors) often running legacy software. Segmentation is crucial to defensibility – a common practice is to group medical devices on separate VLANs or networks isolated from the hospital administrative network. For example, an MRI machine network might be firewalled such that it only communicates with the PACS (image storage) server and nothing else. If ransomware hits the hospital's PCs, the hope is it cannot easily reach the medical device network. Healthcare cybersecurity frameworks like the HHS 405(d) **Health Industry Cybersecurity Practices (HICP)** explicitly recommend network segmentation to prevent attackers from moving from low-risk systems to high-risk clinical systems. Many hospitals implement **"biomed VLANs"** and apply internal firewalls or NAC to lock down communications. In an incident, the IT team might take the step of cutting off those medical device networks entirely from the rest of the hospital as a defensive posture – allowing devices to continue functioning locally while the infection is contained to, say, the admin network.

Maintaining Care During Downtime:



Healthcare is unique in that it routinely plans for IT downtime due to either technical failure or cyberattack. **Manual backup procedures** are a lifeline. As noted, the Joint Commission requires hospitals to have detailed downtime procedures. This can include having "downtime forms" (paper forms) ready to register patients and record treatment, fallback communication methods (like radios or phones) if email is down, and even stockpiled printouts of schedules or patient lists. A defensible cyber posture for a hospital means that if ransomware hits, the clinical staff knows how to switch to these manual processes immediately, **without waiting for IT directives**. For instance, during the 2017 WannaCry attack, many UK National Health Service hospitals had to revert to paper and cancel noncritical appointments. Those that had robust downtime plans were able to continue emergency services safely. In the UHS ransomware case in 2020, the hospital chain's prior training on offline documentation was credited with enabling them to continue urgent care for patients while IT systems were offline. The tragic opposite example occurred in Düsseldorf, Germany, also in 2020: a hospital hit by ransomware could not treat an emergency patient due to system outage, and the patient died after being re-routed – underscoring that lack of an effective defensible position (no accessible backups or alternate hospital procedures) can have fatal consequences.

Protecting Patient Data and Services:



Strategically, healthcare organizations are aligning with frameworks like NIST and adopting **zero trust** principles inside their networks. This means authenticating and authorizing every connection, which helps limit an intruder. Many are also deploying network anomaly detection specialized for medical devices, which can flag if a device starts behaving oddly (e.g., a lab analyzer suddenly trying to communicate with an accounting server could indicate a breach). Tactically, a hospital IT security team, upon detecting a cyberattack, will isolate affected segments – for example, if an ER's workstation network is infected, they might isolate that from the rest of the hospital and provide the ER with a standalone documentation method.

Another important aspect is **availability of backups**. Under HIPAA, healthcare providers must have contingency plans including data backup and *emergency mode operation*. This means that not only is data backed up offline, but there are procedures to operate on backup data if primary systems are down. An example would be periodically printing or exporting critical patient information so that it's available even if the EHR system is locked by ransomware.

Industry Collaboration:



Healthcare has seen a surge in guidance from agencies like CISA, the Department of Health and Human Services (HHS), and the healthcare ISAC. Best practice playbooks suggest steps like "preemptively disconnect elective systems when ransomware is detected" – e.g., a hospital may decide to shut down outpatient clinic networks early in an incident to prevent spread to inpatient networks. HHS's 405(d) program and publications like "Healthcare System Cybersecurity Readiness & Response" advocate for tiered response plans where non-critical systems can be taken offline to preserve critical ones. This is essentially a defensible posture approach: sacrifice the less critical to save the critical.

In summary, healthcare organizations strive to be **"cyber resilient"** – continuing core clinical operations even under attack. This is achieved through rigorous segmentation (so an attack in one area doesn't cripple all), well-practiced downtime procedures (so care delivery continues if IT is shut off), and data protection (so that patient records can be restored or accessed via alternate means). A defensible cyber position in healthcare might involve isolating the hospital from external networks (to stop an ongoing breach) and running it as an island for a period of time. Given the stakes, the healthcare sector has made this a high priority, but challenges remain (limited IT budgets at many hospitals, legacy devices that can't easily be secured, etc.). Nonetheless, the trend is toward networks that can be more **surgically isolated** (e.g., segment per department or device type) and staff that are ready to roll with the punches when digital systems become unavailable. As one healthcare CIO put it, it's about *"clinical continuity under cyber duress"* – the show must go on, even if that means pulling plugs and opening paper chart binders.

Frameworks, Playbooks, and Government Guidance

Fortunately, organizations do not have to invent the concept of defensible cyber positions from scratch – there are numerous **authoritative frameworks and guidelines** that incorporate these principles. Below are some key resources and how they relate:

NIST Cybersecurity Framework (CSF) and NIST SP 800-61:

NIST CSF's functions (Identify, Protect, Detect, Respond, Recover) give a high-level roadmap. The **Respond** and **Recover** functions inherently cover the idea of containing incidents and maintaining resilience. NIST Special Publication 800-61 "*Computer Security Incident Handling Guide*" proposes best practices for incident containment, eradication, and recovery. While not using the term "defensible cyber position," it stresses preparation of containment strategies (e.g., network isolation, shutting down systems) and planning for continuity of operations during incidents. NIST's guidance for ICS, **SP 800-82** (Guide to ICS Security), specifically addresses the need for incident response in OT environments, noting differences from IT (such as prioritizing availability and safety). Adhering to NIST guidelines helps organizations build the processes needed for a defensible posture. For example, NIST suggests having predefined criteria for when to disconnect networks or shut down systems – these criteria can feed into your playbook for switching to the defensible state.



SANS Institute and Community Best Practices:

The SANS ICS team (experts like Robert Lee and Tim Conway) have published the "Five Critical Controls for ICS Security" which explicitly includes **Defensible Architecture** as Control #2 and **ICS Incident Response** as Control #1. They outline the attributes we discussed: asset inventory, segmentation, secure remote access, monitoring, and the ability to shift to a defensible cyber position. SANS and other training organizations often provide incident response playbook templates. One useful resource is the **SANS ICS Incident Response Cheat Sheet/Poster**, which advises testing a safe shutdown (defensible position) and lists steps like acquiring forensics, isolating networks, etc., tailored to industrial settings. For enterprise IT, SANS and CERT guides emphasize similar containment steps. Many companies develop their incident response runbooks following these community best practices, adapting them to their own networks.



CISA and Government Agency Guidance:

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has been active in promoting cyber resilience. In the wake of major attacks, CISA released joint advisories with recommendations. For instance, after Colonial Pipeline, CISA and FBI urged critical infrastructure operators to "*implement robust network segmentation..., regularly test manual controls, and ensure backups are offline*" as key steps to mitigate ransomware risk. These are directly supportive of being able to go into a defensible state. CISA also published the "**Shields Up**" initiative (during geopolitical tensions) which advises organizations to be prepared to disconnect from the internet temporarily if targeted by cyberattacks, among other things. Another CISA resource is the **Cybersecurity Performance Goals (CPGs)**, a set of baseline practices for critical infrastructure released in 2022. The CPGs include items like segmenting networks and isolating backups, which are building blocks of a defensible posture. Sector-specific agencies have playbooks too – for example, the U.S. Department of Energy has incident response templates for electric utilities, and the FDA has cybersecurity guidance for medical device continuity. In Canada, the **Public Safety Canada** guidance (which we cited earlier) explicitly discusses establishing a defensible cyber position for ICS and advises testing it in exercises. The UK's NCSC has guidance on "Cyber Incident Response" that similarly highlights containment and isolation strategies. Collectively, government guides stress *advance preparation and testing* of isolation capabilities as a must. Many also provide checklists – e.g., CISA's Ransomware Response Guide includes steps like isolating affected hosts, disabling network shares, etc., which map to implementing a defensible posture.



MITRE ATT&CK® and Engage Frameworks:



The **MITRE ATT&CK framework** for Enterprise and for ICS is a knowledge base of adversary tactics and techniques. Organizations use ATT&CK to understand likely attack paths and then plan mitigating controls. For example, ATT&CK might highlight that adversaries often try to move laterally via Remote Desktop Protocol (RDP) – the mitigating control is to have the ability to disable RDP enterprise-wide (a tactic we’ve discussed). Using ATT&CK can help justify and prioritize certain defenses in your architecture (like segmentation to counter lateral movement, or isolating admin networks to counter credential theft). MITRE also has the **ATT&CK for ICS matrix**, which covers tactics adversaries use specifically in industrial settings – this can inform what an ICS defensible position should guard against (e.g., isolate safety systems if an attacker is known to try to manipulate them). Another MITRE effort, **MITRE Engage (formerly Shield)**, provides a framework for active defense and adversary engagement. Engage includes techniques like segmentation, service isolation, and sandboxing attackers – essentially cataloguing ways to control and contain adversaries. While more specialized, these frameworks can inspire improvements to incident response playbooks. For instance, MITRE Engage suggests techniques for isolating an attacker’s access *without them immediately knowing*, which could be useful if you want to observe their behavior (though in many ransomware cases, immediate hard isolation is preferred). Overall, MITRE’s resources are more about understanding threats and defensive techniques, complementing the prescriptive guidance of NIST or CISA.

Industry Frameworks and Playbooks:



Many industries have their own consortia and guidelines. We touched on SWIFT’s CSCF in finance, which is essentially a framework ensuring members can isolate their payment systems. In healthcare, the HHS 405(d) program’s **HICP** document (Health Industry Cybersecurity Practices) provides best practices for hospitals of different sizes, mapping out steps like network segmentation, backup, and incident response planning. The **National Healthcare ISAC (NH-ISAC)** also shares threat reports and suggested actions for containment when certain threats are detected. In manufacturing, organizations look to ISA/IEC 62443 standards for building secure, segmentable control systems. Another example is the **Energy Sector Cybersecurity Framework Implementation Guidance**, which translates NIST CSF into power/oil/gas context with an emphasis on being able to isolate critical generation or refining systems. Many large companies also develop internal playbooks – for example, an **Incident Response Playbook for Ransomware** that details the steps from detection to isolation to recovery. The U.S. government mandated federal agencies to develop standard playbooks after some high-profile attacks, resulting in a **Federal Incident Response Playbook (2021)** which, while federal-specific, is a useful outline of stages (it emphasizes containment and communication).

In conclusion, there is a rich ecosystem of frameworks and resources to guide the establishment of defensible cyber positions. Organizations should leverage these: use NIST and ISO standards for the foundational controls, SANS and ISAC guidance for industry nuances, government advisories for up-to-date threat tactics and recommended mitigations, and incorporate MITRE ATT&CK knowledge to ensure no major gap in coverage. Importantly, **any framework should be customized** – a defensible position must be tailored to your specific environment, threat model, and risk appetite. But by aligning with well-known standards, you not only follow best practices but also can demonstrate to stakeholders (and regulators) that your incident response posture is built on proven principles.



Tools and Technologies Supporting Defensible Cyber Strategies

Implementing the strategies above requires the right tools. Both open-source and commercial solutions can help an organization build and execute a defensible cyber position. These tools span network security, endpoint security, monitoring, and incident response orchestration. Below is an overview of some useful tool categories and examples in each:

Network Segmentation and Firewalling:

To enforce network zones and choke points, organizations use firewalls, switches, and routers capable of creating access control layers. On the open-source side, **pfSense** and **OPNsense** (open-source firewall platforms) can be used to segment networks with fine-grained rules. Linux's built-in **iptables/nftables** can also enforce segmentation policies (though they require expertise to manage at scale). Commercially, almost every enterprise uses firewall appliances or software from vendors like **Palo Alto Networks**, **Cisco**, **Fortinet**, **Check Point**, etc. Modern next-generation firewalls allow defining security zones (e.g., IT, OT, DMZ) and can even automate shutting down traffic if certain alerts trigger. In industrial settings, specialized industrial firewalls like **Belden Hirschmann/Tofino** or **Honeywell's Experion** firewall are deployed at control system enclaves. **Software-Defined Networking (SDN)** solutions and **microsegmentation** tools (e.g., **VMware NSX**, **Illumio**) are also used in data centers to create on-the-fly isolated segments around critical assets. These technologies support a defensible position by making it easier to isolate portions of the network with a few clicks or an automated policy.



Endpoint Detection & Response (EDR) and Isolation:

EDR tools not only detect suspicious behavior on endpoints but also often provide a one-click "isolate host" function – essentially turning the host into a silo that's only connected to the security console. Leading commercial EDR platforms like **CrowdStrike Falcon**, **Microsoft Defender for Endpoint**, **SentinelOne**, **Carbon Black** and others have this containment feature. For example, if a workstation is suspected to be patient-zero of ransomware, a responder can issue an isolate command through the EDR console, which firewalls that machine off from the rest of the network (while still allowing the EDR agent to communicate for forensic data collection). This is immensely valuable for implementing a defensible posture on the fly. On the open-source side, **OSSEC** or its fork **Wazuh** provide host intrusion detection and can be scripted to do containment actions, though not as advanced as commercial EDR. Another open tool is **CimSweep** (PowerShell-based) for detecting compromised hosts – it can be used in combination with PSRemoting to disable network adapters on suspect machines. While not as slick as commercial tools, creative sysadmins can leverage scripts and tools like **PDQ Deploy** or **Ansible** to push a "disable network" command or firewall rule to endpoints as a DIY containment mechanism. Additionally, for servers, **allowlisting software** (like AppLocker on Windows or open-source OSquery) can be used to lock down what can run, thereby indirectly helping maintain a safe state under attack.



Monitoring and Detection (Network Security Monitoring/IDS):

Early detection is part of being defensible – you can't throw the switches if you don't know there's trouble. Open source **IDS (Intrusion Detection Systems)** such as **Snort**, **Suricata**, and **Zeek** are widely used to monitor network traffic for malicious patterns. These can be deployed at key network junctions and configured to detect scanning, malware signatures, command-and-control traffic, etc. Suricata, for instance, has rulesets for ICS protocols that could alert if, say, an unexpected command is sent to a PLC. While IDS are typically passive (alerting), they can integrate with firewalls for automated blocking (an approach known as intrusion prevention, IPS). Some organizations use the open-source **Bro/Zeek** IDS logs in real-time to decide when to manually isolate a network segment (e.g., an alert for multiple machines beaconing to an unknown IP might prompt immediate containment of that subnet). On the commercial side, **network detection and response (NDR)** tools like **Darktrace**, **Cisco Stealthwatch**, **RSA NetWitness**, **Corelight (commercial Zeek)**, etc., use AI/anomaly detection to flag incidents. In ICS, vendors like **Dragos**, **Nozomi Networks**, **Clarity**, **Tenable.ot** provide specialized monitoring for OT traffic and can integrate with OT firewalls to quarantine suspicious activity. These monitoring tools support a defensible posture by giving the visibility needed and, in some cases, automating the initial containment (for example, an NDR might trigger a software-defined microsegmentation policy to isolate a detected threat). Even simpler, network management tools (like switch management consoles) can be scripted or manually used to shut down a rogue device's port when monitoring flags it – many incidents have been contained by an admin rapidly disabling a switch port after an alert.



Identity and Access Management (IAM) Tools:

Since limiting remote access and disabling accounts is a key part of response, IAM and Privileged Access Management (PAM) tools are important. Commercial PAM solutions such as **CyberArk**, **BeyondTrust**, **Thycotic** allow centralized control of privileged accounts – during an incident, they can mass-rotate passwords or lock down administrative accounts to prevent abuse. Some also have session kill features to terminate active connections. For general IAM, integration with directory services (Active Directory, LDAP) means security teams can quickly apply group policies to harden many systems at once (for example, a GPO to disable all domain user logins except incident responders, which was a tactic used in some ransomware recoveries). There are fewer open-source tools in this realm, but one can script against directory services or use **free PowerShell modules** to disable accounts in bulk as needed. Additionally, **Multi-Factor Authentication (MFA)** tools (even simple ones like Google Authenticator for VPN, or commercial like Duo, Okta) help ensure if you haven't cut off remote access entirely, at least it's hardened. In practice, during high alerts some companies have enforced MFA or additional verification even for internal access, essentially stepping up access requirements as part of entering a higher security posture.



Incident Response Orchestration and SOAR:

Orchestration tools can automate parts of the defensible position activation. **SOAR (Security Orchestration, Automation, and Response)** platforms like **Cortex XSOAR (Palo Alto)**, **Splunk Phantom**, **IBM Resilient**, **D3 Security** or even open-source **Shuffle**, can be pre-programmed with playbooks. For instance, a SOAR playbook for “ransomware detected” might automatically: isolate affected hosts via EDR API, block known malicious IPs on the firewall, disable certain user accounts, send an alert to IT to prepare backups, and so on. This speeds up response when every minute counts. Open-source **TheHive** combined with **Cortex** can serve a similar function – TheHive is an IR case management tool where analysts track an incident, and Cortex can execute analyzer/responder scripts (like one to ban an IP or isolate a host through integrations). Many organizations integrate their EDR, firewall, and Active Directory with such platforms so a single console can initiate multi-faceted containment. Even without a full SOAR, simple automation like PowerShell or Python scripts triggered by SIEM alerts can do wonders (e.g., a script listens for a “malware outbreak” alert in Splunk and then runs commands to shut down SMB service on all servers to stop worm propagation).



Data Backup and Recovery Tools:

While more for recovery, these tools enable the “recover” part of a defensible position. The quicker you can restore or switch to backups, the more willing you might be to take systems offline. Open-source backup solutions (like **Bacula**, **Amanda** for file systems, or database-specific ones like **pgBackRest** for Postgres) allow you to maintain offline backups. Commercial backup suites (e.g., **Veeam**, **Veritas NetBackup**, **Dell EMC Data Domain** with Cyber Vault features) increasingly offer **immutable storage** options – backups that can't be encrypted or deleted by malware. In a ransomware scenario, a company with an immutable backup can confidently isolate and wipe infected systems, then restore from backup. Backup tools often have automation to promote a backup to production or run critical services from a secondary site (for instance, some banks use backup software to spin up core systems in an isolated enclave for testing – the same could be used in a crisis to run operations in that enclave). **Cloud-based backups** with versioning (AWS, Azure Backup, etc.) also play a role – cloud consoles can be used to detach or “lock” those backups when an attack is unfolding. The main point is that backup tools undergo your ability to recover after holding the fort in a defensible state.



Specialized OT Security Tools:

In industrial contexts, there are additional tools worth noting. **Data diodes** (from vendors like Waterfall Security, Owl Cyber Defense) are hardware devices that allow one-way data flow. They are used to ensure certain segments (like a safety system or a plant control network) can only send data out to monitoring systems, but nothing can come in. This is a strong way to maintain a defensible posture by default – even during normal times, the critical segment is protected, and during incidents there's physically no way for the adversary to get to it. **ICS-specific forensics and incident response tools** are also emerging. For example, Microsoft's open-source tool, ICSpector, aims to help collect forensic data from PLCs and other devices for analysis. While this doesn't directly isolate, it helps responders analyze incidents in OT environments without disrupting operations. In terms of asset visibility (crucial for planning isolation), tools like **GRASSMARLIN** (an NSA-released open-source tool) can map ICS networks to identify all connections – useful to simulate what happens if you cut one link or another.



Communications and Collaboration Tools:

Often overlooked, but during an incident when you've isolated parts of your network, you need out-of-band communications. Many organizations prepare alternate communication means: for example, **satellite phones, two-way radios, or an external email system** not dependent on the internal network. If corporate email or VoIP is down or untrusted (maybe the email system is compromised), having tools like **Signal (encrypted messaging app)** or a cloud-based communication platform on standby is important for coordination. From a defensible posture perspective, maintaining command and control of your incident response team requires resilient comms. Some companies have used **pager apps or emergency mass notification systems** (like Everbridge) during cyber incidents to reach employees and give instructions like "disconnect from VPN, do not turn on PCs until further notice," etc. Ensuring these tools are available and people know how to use them is part of incident preparedness.



In deploying tools, it's critical to **integrate and test them in your response plan**. Simply buying a fancy segmentation solution won't help unless playbooks and people are tuned to use it swiftly under pressure. Many organizations do test runs: e.g., simulate a ransomware outbreak and practice hitting the isolation script, see if the EDR truly isolated the hosts, verify that critical apps continued on the isolated segment, etc. Tools should be configured with "break-glass" options – for instance, a firewall admin might prepare a special ruleset that cuts all internet traffic and have it ready to deploy. Some tools even support a big red button concept: one vendor's solution allowed a single click to disconnect an entire enterprise from the internet (not commonly used, but possible!).

Finally, **balance is key**. Open-source tools can often achieve defensible architecture at lower cost, but they may require more manual effort to use during an incident. Commercial tools tend to offer more automation and user-friendly kill-switch capabilities. Many organizations use a blend: perhaps open-source logging/IDS for detection, but commercial EDR for endpoint isolation, etc. The exact tools will depend on the environment – an ICS plant will invest in specialized OT monitoring and safety controls, a bank might invest more in SOAR and network access control, a hospital in network segmentation and backup systems for EHR. Regardless of tool choice, the outcome to strive for is the same: **the ability to rapidly shrink your attack surface, shield your crown jewels, and sustain critical ops when the alarms go off**. With the right preparation and toolkit, a defensible cyber position moves from a theoretical ideal to an actionable, achievable state that could save your organization in its worst hour.



References:

1. Lee, R. M., & Conway, T. (2022). *The Five ICS Cybersecurity Critical Controls* – SANS Institute. (Attributes of defensible architecture including the “defensible cyber position” concept)
2. Public Safety Canada. *Developing an OT and IT Incident Response Plan (2023)* – Section: Defensible Cyber Position. (Guidance on isolating operations, e.g., disconnecting networks or segmenting processes, and example countermeasures in ICS incident response)
3. Dragos. *Colonial Pipeline Cyber Attack – Recommendations (2021)*. (Colonial Pipeline halted OT operations as a precaution due to IT ransomware, illustrating an extreme defensible posture)
4. Greenberg, A. (2018). *WIRED: The Untold Story of NotPetya*. (Maersk’s response to NotPetya – physically disconnecting its entire network in 2 hours – a dramatic example of network kill-switch by manual means)
5. Xage Security. *Defensible Architecture in ICS (2025)*. (Explanation of reducing connectivity and unnecessary devices during heightened situations, and isolating infected assets so operations can continue)
6. CereCore Briefings on HIPAA. *Recent cyberattacks highlight importance of downtime procedures (Nov 2020)*. (UHS hospital ransomware case – 250 facilities on backup processes for 2 weeks; patient care continued via offline methods) (Joint Commission requires manual downtime procedures for accredited hospitals)
7. CISA/FBI Joint Advisory. *DarkSide Ransomware: Best Practices (AA21-131A, May 2021)*. (Recommendations for critical infrastructure: network segmentation between IT/OT, test manual controls, offline backups – to reduce ransomware impact)
8. TrueFort. *Complying with SWIFT CSCF (2023)*. (Emphasizes isolating SWIFT systems from less secure networks – a BFSI example of mandated segmentation for a defensible posture)
9. Royal Mail Attack Timeline – Cyber Management Alliance (Mar 2023). (LockBit attack on Royal Mail forced a switch to manual processes, illustrating containment of IT systems while business continuity fell back to manual operations)
10. *Summary of SANS ICS Controls (2023)*. (Reiterates defensible architecture attributes per SANS, including reduced connectivity mode during incidents)



Conclusion:

In an era where cyber threats are fast, sophisticated, and increasingly disruptive, a Defensible Cyber Position is not a luxury — it is a strategic necessity. By pre-planning how to harden, isolate, and sustain operations in the face of a cyberattack, organizations can contain threats with confidence and reduce both business and societal impact.

Whether in critical infrastructure, healthcare, financial services, or enterprise IT, a defensible posture allows responders to “fight through” incidents without being forced into a full shutdown. The most resilient organizations are those that:

- Segment and architect their networks for isolation,

- Define tactical actions like kill-switches and fallback operations,
- Regularly test their incident response plans including degraded operations,
- Align with frameworks like NIST CSF, ISA/IEC 62443, and SANS ICS Controls.

The ability to rapidly move into a safe, controlled mode under duress separates prepared organizations from those overwhelmed by chaos. As threats grow in scale and speed, the defensible cyber position emerges as a cornerstone of modern cyber resilience and business continuity.

About the Author



Michel Bruggeman

Principal Consultant | EMEA IoT & OT Lead

Michel is a distinguished cybersecurity leader with over 25 years of experience specializing in operational technology (OT) security, cyber resilience, and industrial cybersecurity architecture. He has held strategic roles across the insurance, manufacturing, energy, and semiconductor sectors, focusing on ICS/OT risk assessments, secure cloud adoption, and incident response readiness.

Michel is a SANS /ISA Mentor and Microsoft Certified Trainer, with deep expertise in IEC 62443, NIST, ISO 27001, DORA, and NIS2, and in his spare time he is a volunteer firefighter for more than two decades.

For more information, contact askus@infosys.com



© 2025 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.