Brilliant *at the* Basics

Top 10 OT Cybersecurity Best Practices for Defense Industrial Base (DIB) Partners

The "Brilliant at the Basics" Cybersecurity Campaign is designed to empower our Defense Industrial Base (DIB) partners — particularly innovative small and mid-sized businesses — with streamlined, practical guidance to confidently protect their operations without the burden of massive compliance overhead. In alignment with the Department of War's (DoW) mission to supercharge the "Arsenal of Freedom," this guide distills vital cybersecurity principles into clear, actionable steps for Operational Technology (OT) environments.

As we work together to streamline compliance and remove administrative barriers, protecting operational technology, from weapon systems to critical infrastructure controls, remains a vital, shared responsibility. By adopting these foundational core practices, industry partners can fortify their OT, reduce technical debt, and ensure the rapid, secure delivery of superior technology to the tactical edge—ultimately delivering peace through technical strength.

1 *Identity and Access Control*

Manage who has access to your OT by enforcing strict identity and access control. Ensure your system verifies the identity of every user via stringent authentication methods before allowing access to your network. Enforce strong access controls and require multi-factor authentication (MFA) for sensitive systems. Under Zero Trust, users should only be granted the "least privilege" needed to do their specific job, nothing more. Adopt a "never trust, always verify" mindset to protect your business.

2 *Validated Asset Inventory*

The first step for any business is to create and maintain a rigorous, "as-operated" inventory of all physical and logical components within your OT environment. This includes tracking high-criticality assets such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Engineering Workstations, Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS). To ensure a comprehensive baseline for risk management and threat detection, the inventory must catalog not only hardware but also firmware/software versions, active communication protocols, process logic/OT programs, transient assets, and external remote-access connection points. Ensure that all systems have clear ownership, accountability, and secure configuration baseline. Finally, validate this inventory through passive network monitoring and periodic physical walk-downs to eliminate shadow systems and map critical operational dependencies without disrupting live processes.

3 *Strict Network Segmentation*

A key architectural step is to logically separate your business IT network from your critical operational systems. By creating strict partitions, or segments, you make it much harder for an intruder who gains access to one part of your network to move laterally and disrupt your core functions. This containment is a powerful defensive measure. A flat network is a vulnerable network.

4 *OT-Specific Incident Response and Recovery Plan*

A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy.

A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.

Brilliant *at the* Basics

Top 10 OT Cybersecurity Best Practices for Defense Industrial Base (DIB) Partners

5 *Manage Known Exploitable Vulnerabilities*

To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures—including strict firewall rules, network isolation/micro-segmentation, and application allowlisting—effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.

6 *Remote Access Pathways*

Grant remote access to your OT only when needed, for the shortest time possible, and with strong authentication. Eliminate "always-on" connections to reduce your exposure to external threats, particularly cellular gateways and other direct internet-exposed assets. Many businesses rely on vendors or remote employees for support, but every remote connection is a potential door to your network.

7 *Continuous Monitoring*

Extend basic monitoring to the production floor to detect unusual traffic or unauthorized access to machinery. Many firewall and antivirus solutions include logging features that can provide visibility. Regularly reviewing these logs helps you spot and respond to threats before they cause damage. Remember, you can't stop what you can't see!

8 *System Resiliency*

Build your systems to be resilient from the start by mandating secure, composable architecture. Design your industrial networks to fail safely. When upgrading control systems, prioritize resilience by grouping assets by physical location and sensitivity. A secure, modular approach ensures that critical machinery incorporates fault tolerance, physical redundancy, and localized manual overrides, meaning a cyber disruption to one component won't stop your entire production line.

9 *Supply Chain Security*

Knowing your suppliers is critical to mitigating vulnerabilities. This is accomplished thought things like proactive procurement, lifecycle management, and supply chain illumination. Your company's security is connected to the security of your suppliers. It is crucial to understand the entirety of your organization's supply chain and to hold external suppliers to the same security standards as that of the organization to maintain the overall level of security. Requiring vendors to engineer systems and system components to DoW standards ensures built-in security features before purchase. For legacy OT, programs need to set a hard schedule to replace undefendable hardware.

10 *Review Processes*

For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.

*Scan to visit our **Brilliant at the Basics** webpage for more information*

Your Security is Our Security