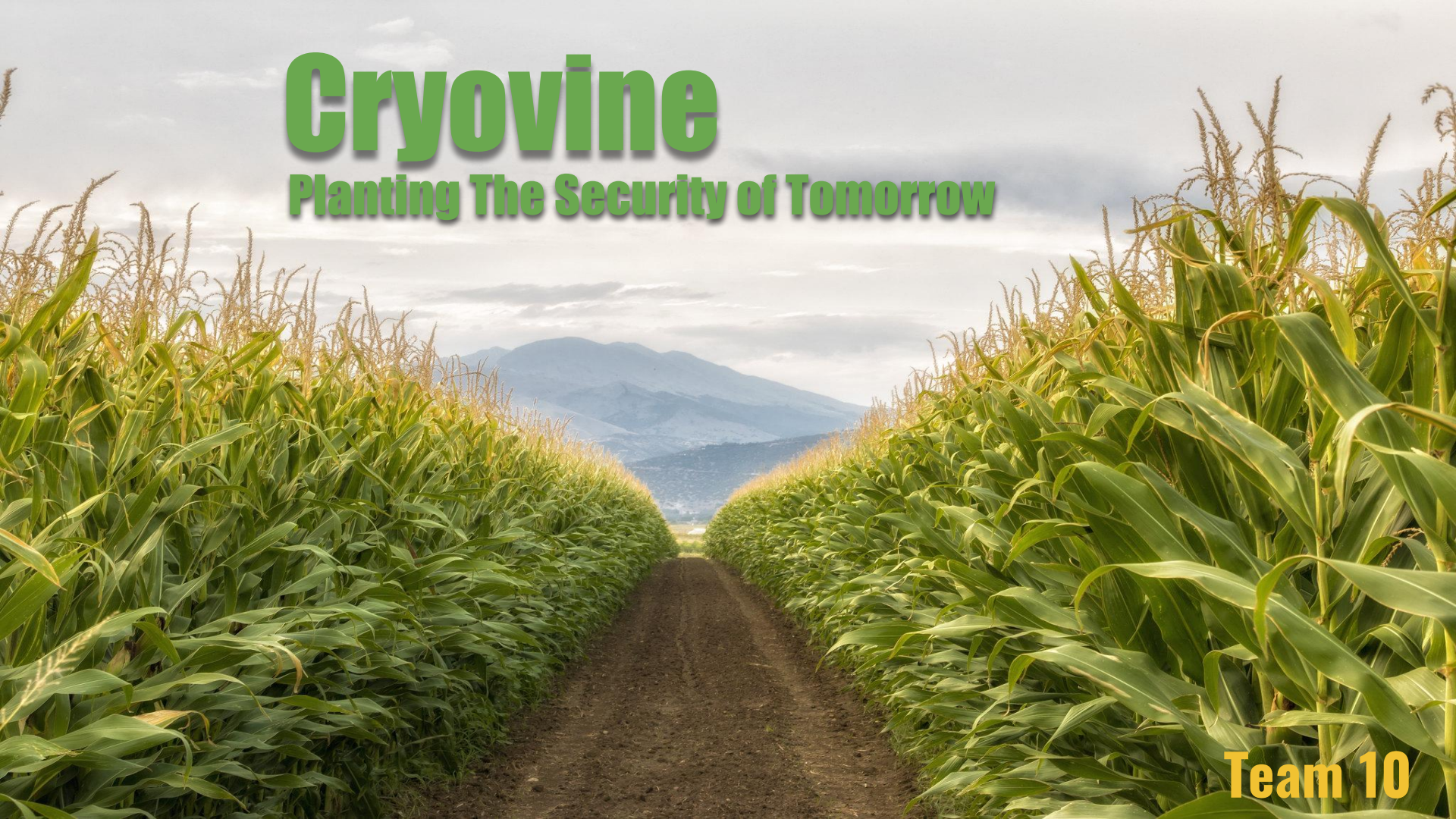
Cryovine
Planting The Security of Tomorrow
Team 10

Why Use a Standard?

- To implement **proven best practices** that can **increase reliability, accountability, and build a secure baseline**
- To promote **collaboration and open communication** with industry peers
- To arrive at a **universally approved and agreed upon configuration** for all of our production systems

Examples:

- **NIST** - NIST Cyber Framework, 800-53
- **ISO** - ISO 27001 ISO 15408 ISO 27002
- **NERC** - CIP (SCADA Systems)

“A common approach allows for a collective response to cybersecurity threats”

The NIST Cyber Framework: Cryovine's Best Option

Why Use The NIST Cybersecurity Framework?

- A set of standards, methodologies, and processes that **align policies, business procedures, and technologies to address cyber risks**.
- Prioritized, flexible, repeatable, performance-based, and **cost-effective approach for managing cyber risk assessment**.
- **Identifies areas for improvement**, addressed through collaboration within the cybersecurity sector and standards-developing organizations.
- **Promotes consistency** by aligning internal practice with recognized standards.

“Simply put, the NIST Cybersecurity Framework is a set of best practices, standards, and recommendations that help an organization improve its cybersecurity measures.”

Identify

- Develop an internal organization in charge of overseeing and managing any risk to systems, employees, assets, data, or intellectual property posed by cyber threat actors.

“Figure out where we currently are.”

Protect

- **Develop and implement appropriate safeguards to ensure that critical services are adequately protected from malicious actors.**

“Develop strategies to protect our assets”

Detect

- Develop and implement appropriate procedures to identify the occurrence of a cybersecurity event. Continually refine these to ensure that developing incidents can be discovered early.

“Detect incidents before it’s a problem”

Respond

- Create and implement appropriate procedures to take defensive action when a cybersecurity incident is detected. Update these continuously to remain resilient against new and emerging threats.

“Effectively respond to incidents, and learn from them”

Recover

- **Develop and implement appropriate recovery procedures to restore any capabilities or services that may have been impaired by a security incident.**

“Return to normal operations and maintain security”

Conclusion

- The NIST Cybersecurity Framework is **the best option for Cryovine**
- **Highlights the most critical areas** of security posture and threat response
- **Provides a clear and concise set of principles** to guide the general improvement of threat management procedures
- **Provides robust high-level coverage** of the most important organizational security concerns facing Cryovine
- Supported by a **trusted government standards body**