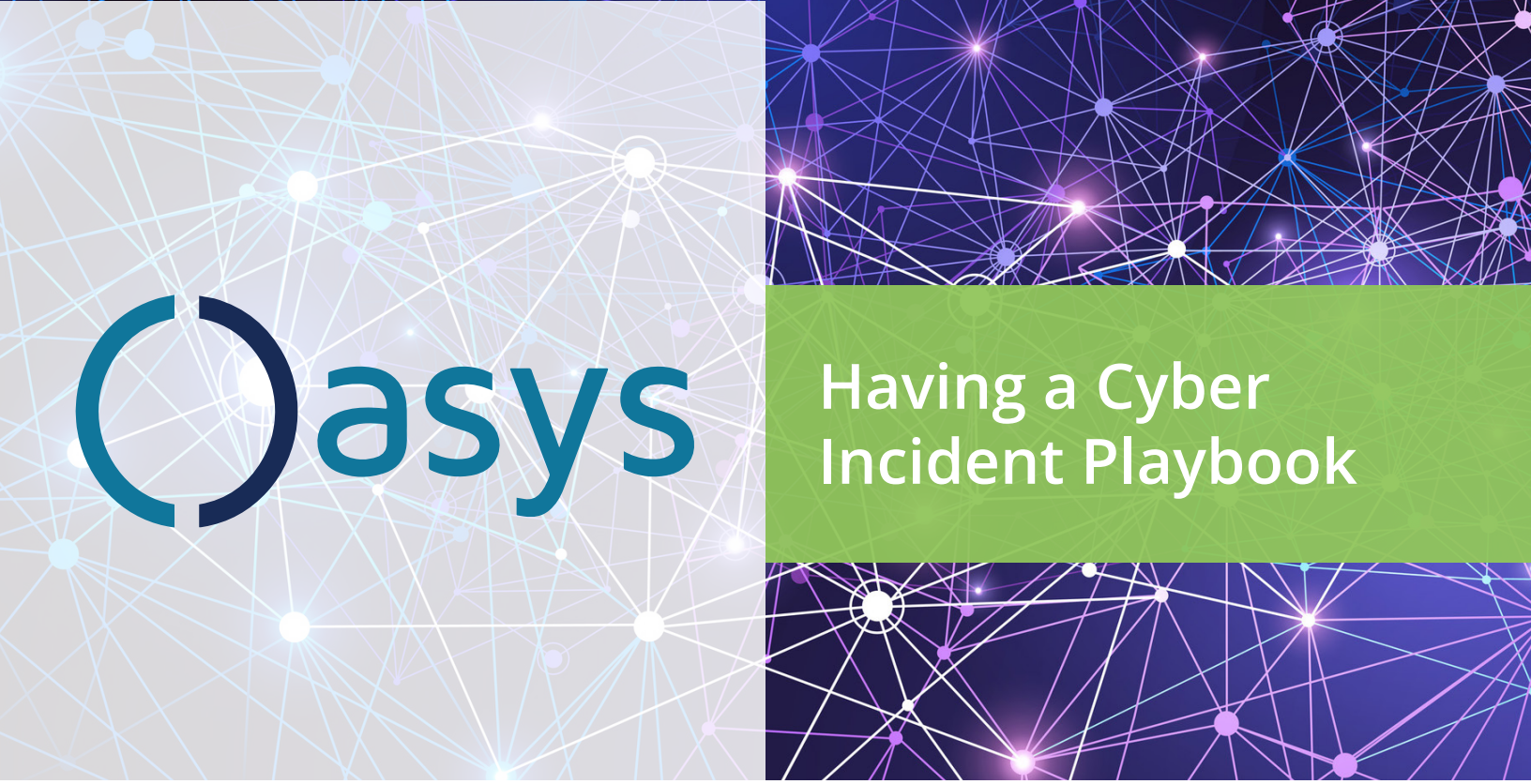


Having a Cyber Incident Playbook

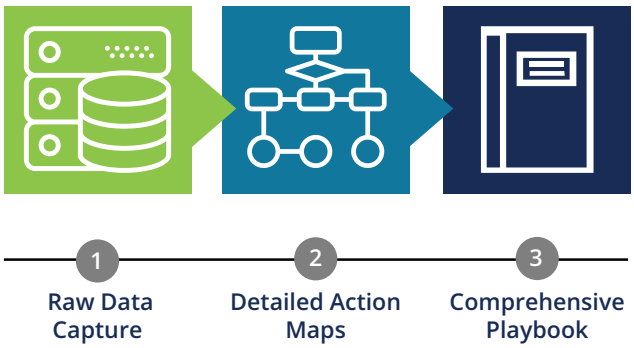
Overview

It's the call no C-suite executive wants to get—notification you've had a cyber incident. As you process the caller's information, you're likely thinking, "what's the next move"? With high visibility disasters like those experienced by Target, Equifax, Sony, and the Office of Management and Budget (OMB), wouldn't it be nice to be able to ask the caller simply "what page should I look at in the response playbook".

High-threat environments like flight operations, nuclear power generation and healthcare don't shoot from the hip when they have an incident. Neither should your organization in the face of a cyber incident response. The value of a creating a playbook, beyond the focus it provides when you get the call, includes

- **Maturing** cyber capabilities by identifying assets, processes and response gaps
- **Creating** a shared organization-wide response plan
- **Identifying** shared corporate priorities
- **Improving** response time by making critical resources readily available
- **Raising** threat awareness and advancing risk management capability in the organization

Proven Framework



The Oasys Framework moves from raw data capture to detailed action maps to the comprehensive Playbook.

Oasys International Corporation (Oasys) is highly experienced in producing valuable organizational playbooks for both cyber and non-cyber incident response. We work with our clients to create their authoritative tool, providing the entire organization with the plan, resources and checklists it needs. We use cyber and business sector subject matter experts who identify, design and craft based a proven framework that includes:

Generating Organization-specific Knowledge

- Articulating your threat environment
- Understanding your core processes
- Capturing and clarifying your internal and external policy compliance
- Clearly defining roles and responsibilities for your team
- Ensuring visibility of your full host and network

Creating Your Team's Response Action Maps

- Scoping the entire incident and providing decision trees and action maps
- Understanding the attacker's intent and thrust

Incorporating Detailed Communication Activities

- Providing checklists and information templates that deliver timely and clear notification across the organization
- Clearly articulating authorizations and providing checklists for properly escalating issues

Creating the Remediation Processes

- Generating incident-specific checklists for containing the attack and eradicating the attacker from the environment
- Process recommendations for implementing long-term strategic changes to your environment

Unfortunately, it isn't a question of if you will have a cyber incident; it's when it will occur. To learn more about preparing your organization through development of a customized, easy to employ playbook, please contact Oasys at **info@oasysic.com** or **757.272.2604.**