ICS Whitepapers

To get your free vendor-sponsored whitepaper, visit sans.org/tools.php

DRAGOS SECURITY™ — *Industrial Control System Cyber Situational Awareness* — DragosSecurity.com

INDUSTRIAL DEFENDER® — *Securing Industrial Control Systems: The Basics* — http://id.lockheedmartin.com

iSIGHTPARTNERS — *Cyber Threat Intelligence for Industrial Control Systems* — isightpartners.com

NEXDEFENSE — *Seeing Through the Fog of Complexity* — nexdefense.com

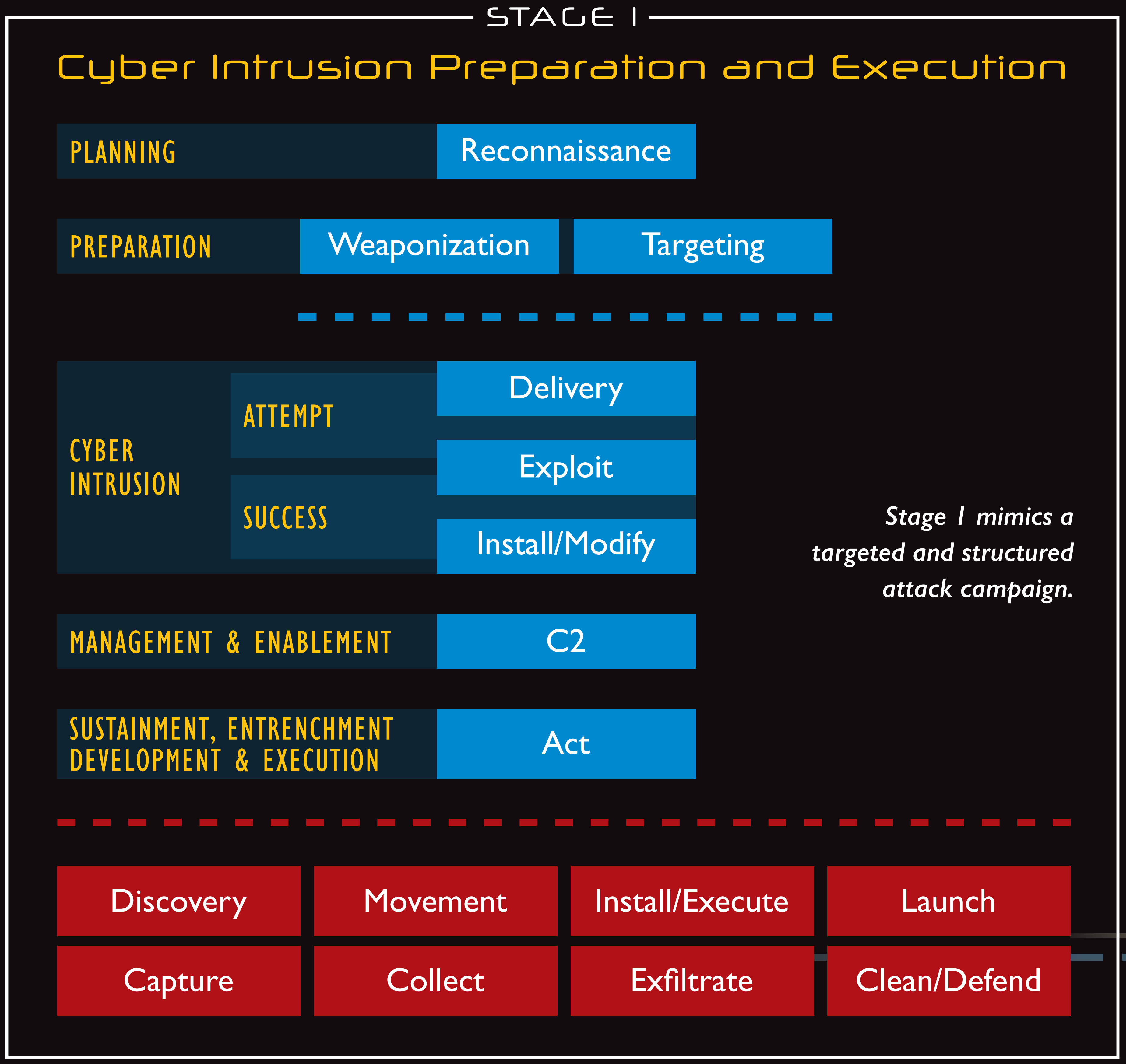
paloalto networks. — *TRAPS FOR SCADA: Prevention of Advanced Threats for Critical Infrastructures* — paloaltonetworks.com

ICS Courses

ICS410: ICS/SCADA Security Essentials — GIAC Cert — GICSP (Global Industrial Cyber Security Professional)

ICS515: ICS Active Defense and Incident Response

ICS Cyber Attacks Normally Require Two Distinct Stages



STAGE 1

Cyber Intrusion Preparation and Execution

PLANNING — Reconnaissance

PREPARATION — Weaponization — Targeting

CYBER INTRUSION
- ATTEMPT — Delivery — Exploit
- SUCCESS — Install/Modify

MANAGEMENT & ENABLEMENT — C2

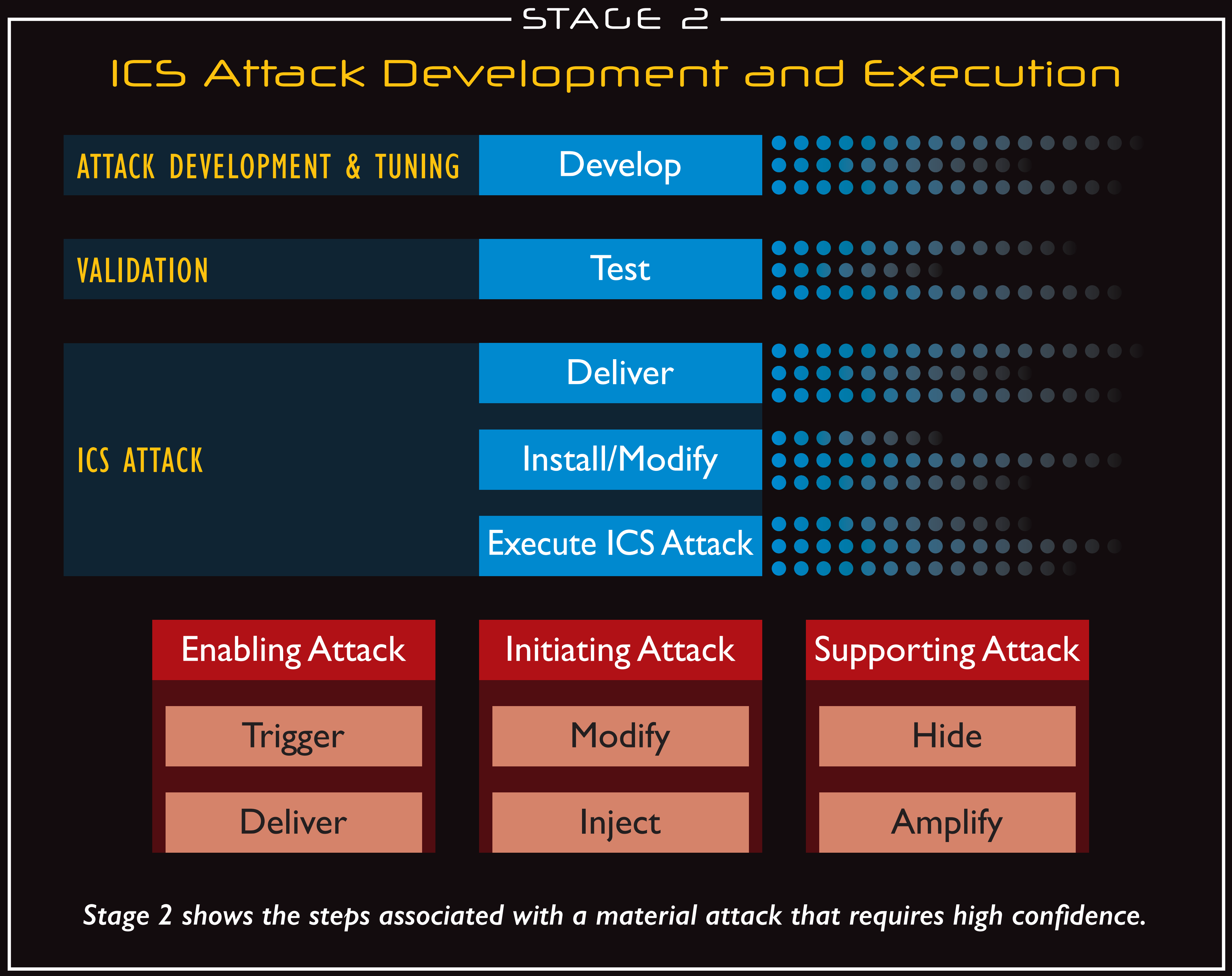
SUSTAINMENT, ENTRENCHMENT DEVELOPMENT & EXECUTION — Act

Stage 1 mimics a targeted and structured attack campaign.

Discovery — Movement — Install/Execute — Launch

Capture — Collect — Exfiltrate — Clean/Defend

Based on the Cyber Kill Chain® model from Lockheed Martin



STAGE 2

ICS Attack Development and Execution

ATTACK DEVELOPMENT & TUNING — Develop

VALIDATION — Test

ICS ATTACK — Deliver — Install/Modify — Execute ICS Attack

Enabling Attack — Trigger — Deliver

Initiating Attack — Modify — Inject

Supporting Attack — Hide — Amplify

Stage 2 shows the steps associated with a material attack that requires high confidence.

SANS

ICS

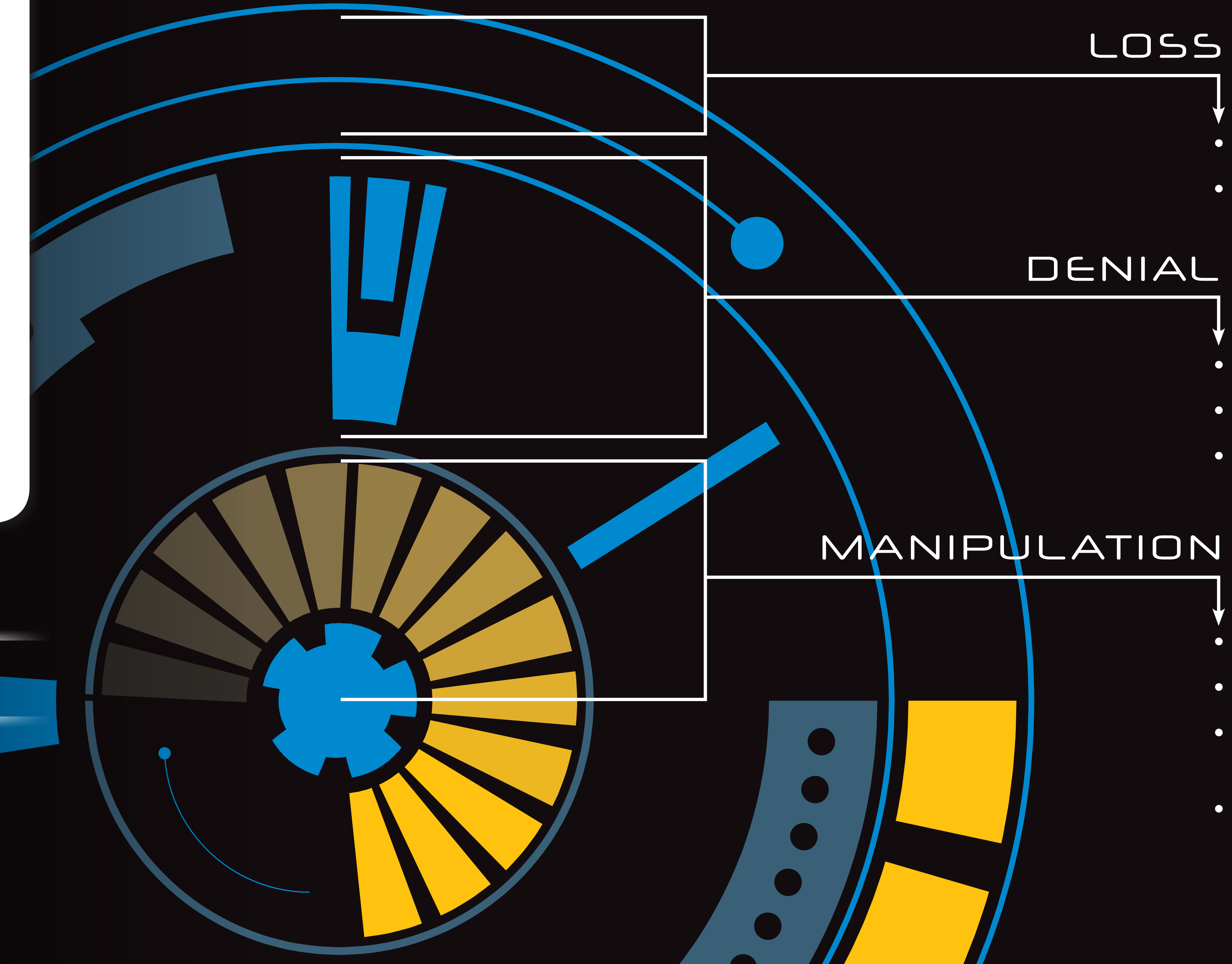
Industrial Control Systems

POSTER

40TH EDITION

ics.sans.org

Attacker Objectives

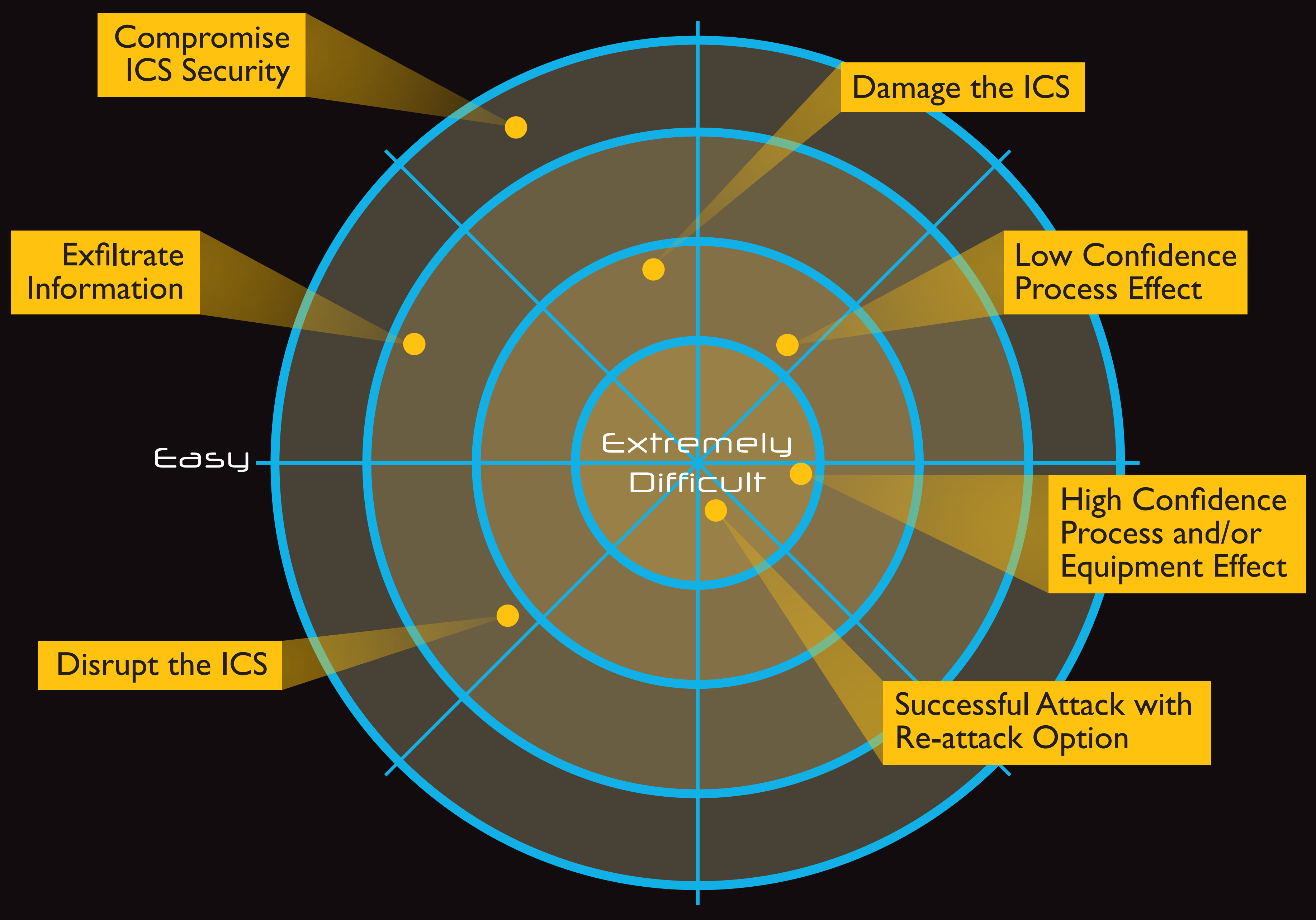


LOSS
- Loss of View
- Loss of Control

DENIAL
- Denial of View
- Denial of Control
- Denial of Safety

MANIPULATION
- Manipulation of View
- Manipulation of Control
- Manipulation of Sensors and Instruments
- Manipulation of Safety

ICS Attack Difficulty



Compromise ICS Security

Damage the ICS

Exfiltrate Information

Low Confidence Process Effect

Easy

Extremely Difficult

High Confidence Process and/or Equipment Effect

Disrupt the ICS

Successful Attack with Re-attack Option

The Sliding Scale of Cyber Security

SANS ICS410

ICS/SCADA Security Essentials

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of technical skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

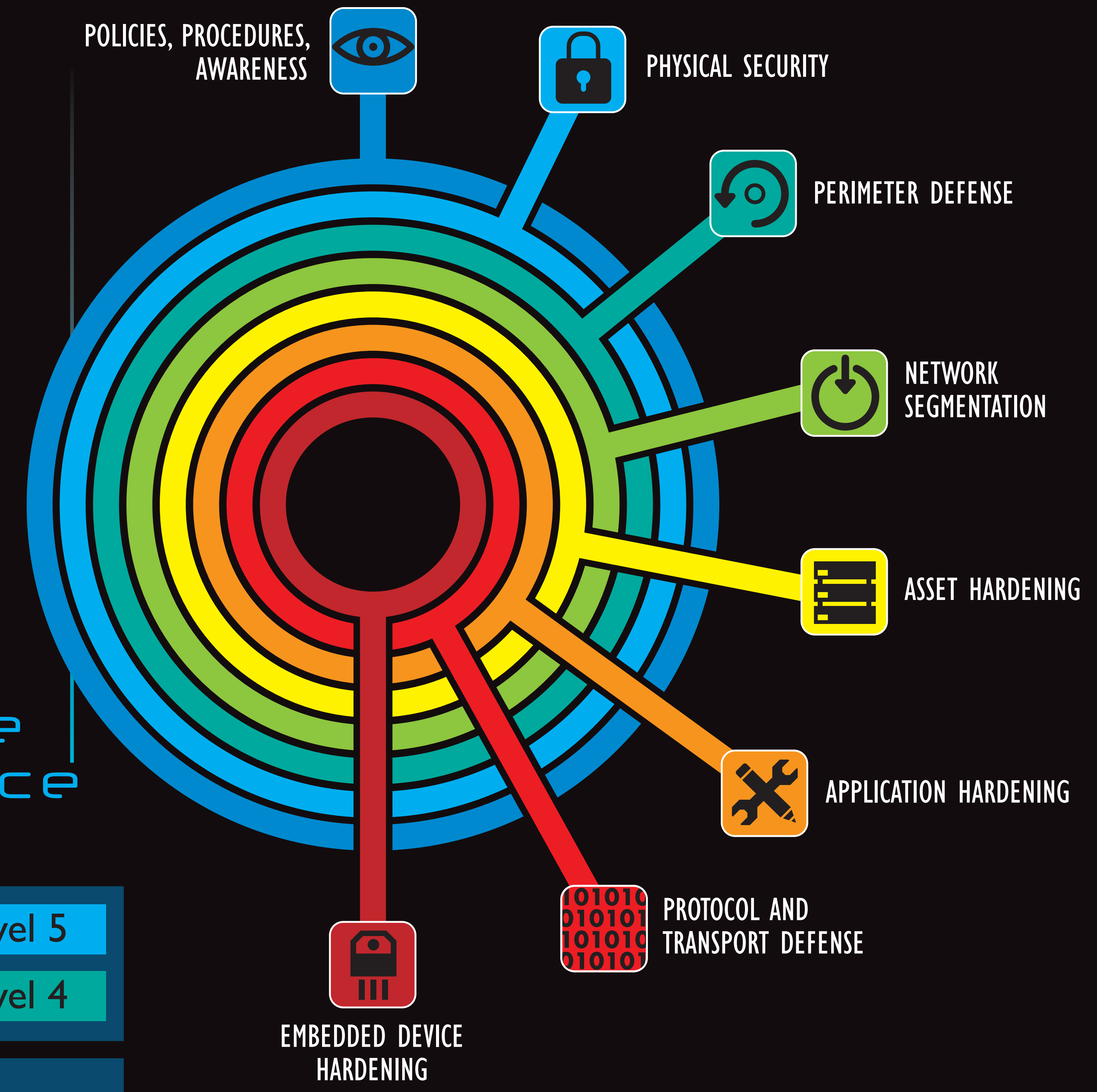
SANS ICS515

ICS Active Defense and Incident Response

ICS515: ICS Active Defense and Incident Response empowers students with the ability to understand and utilize active defense mechanisms in concert with incident response for industrial control system networks in order to respond to and deny cyber threats. The course uses a hands-on approach to give students a technical understanding of concepts such as generating and using threat intelligence, communicating control system needs to information technology personnel to deploy appropriate defenses, detecting malicious actors or threats on control system networks, and performing threat triage and incident response to ensure the safety and reliability of operations technology.

ARCHITECTURE
PASSIVE DEFENSE
ACTIVE DEFENSE
INTELLIGENCE
OFFENSE

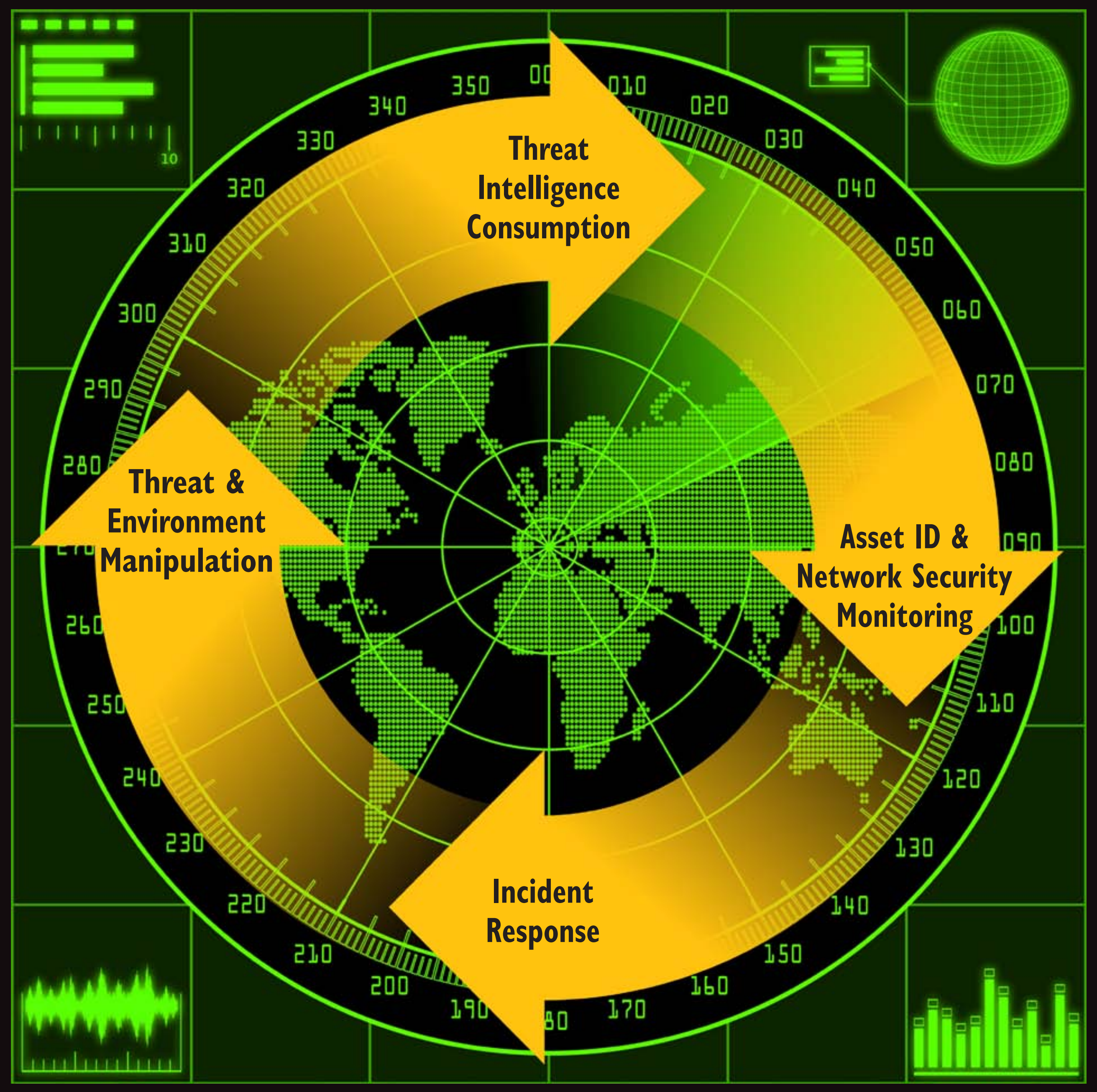
Layers of ICS Defense In Depth



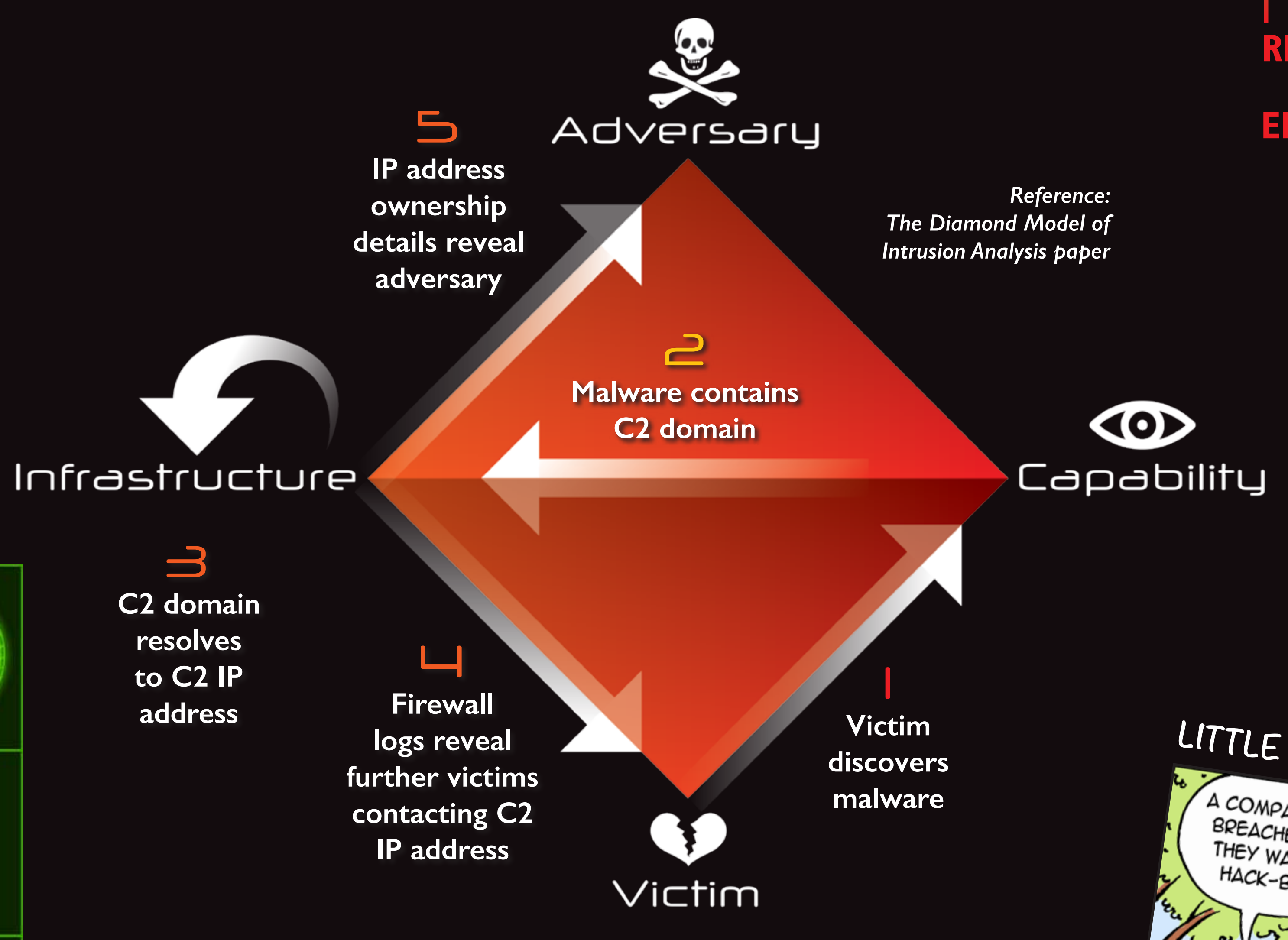
Purdue Reference Model

ENTERPRISE ZONE	Level 5 Level 4
DMZ	
MANUFACTURING ZONE	Level 3
CELL/AREA ZONE	Level 2 Level 1 Level 0

Active Cyber Defense Cycle



The Diamond Model


Adversary
Infrastructure
Capability
Victim
1
Victim discovers malware
2
Malware contains C2 domain
3
C2 domain resolves to C2 IP address
4
Firewall logs reveal further victims contacting C2 IP address
5
IP address ownership details reveal adversary

Reference: The Diamond Model of Intrusion Analysis paper

by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz

NOT RECOMMENDED IN ICS ENVIRONMENTS

LITTLE BOBBY

A COMPANY WAS BREACHED AND THEY WANT TO HACK-BACK.
SOME COMPANIES THINK IT'S A GOOD OPTION.
TIME
WIRED
WHAT DO YOU THINK? IS OFFENSE A GOOD DEFENSE?
I THINK ACTUALLY DOING SECURITY IS PROBABLY A PRETTY GOOD DEFENSE.
HAAS

by Robert M. Lee and Jeff Haas