What Will Your Attack Look Like?

Adversary campaigns often use similar and recognizable techniques. As an ICS defender, your defensive actions (or lack of actions) will determine what your next attack will look like.

1 **SYSTEM VARIABLES**
The various cyber, physical, and support components found in an environment

2 **CYBER MATURITY VARIABLES**
Organization culture, investment, and management programs that shape cybersecurity capability

3 **ADVERSARY CAPABILITIES**

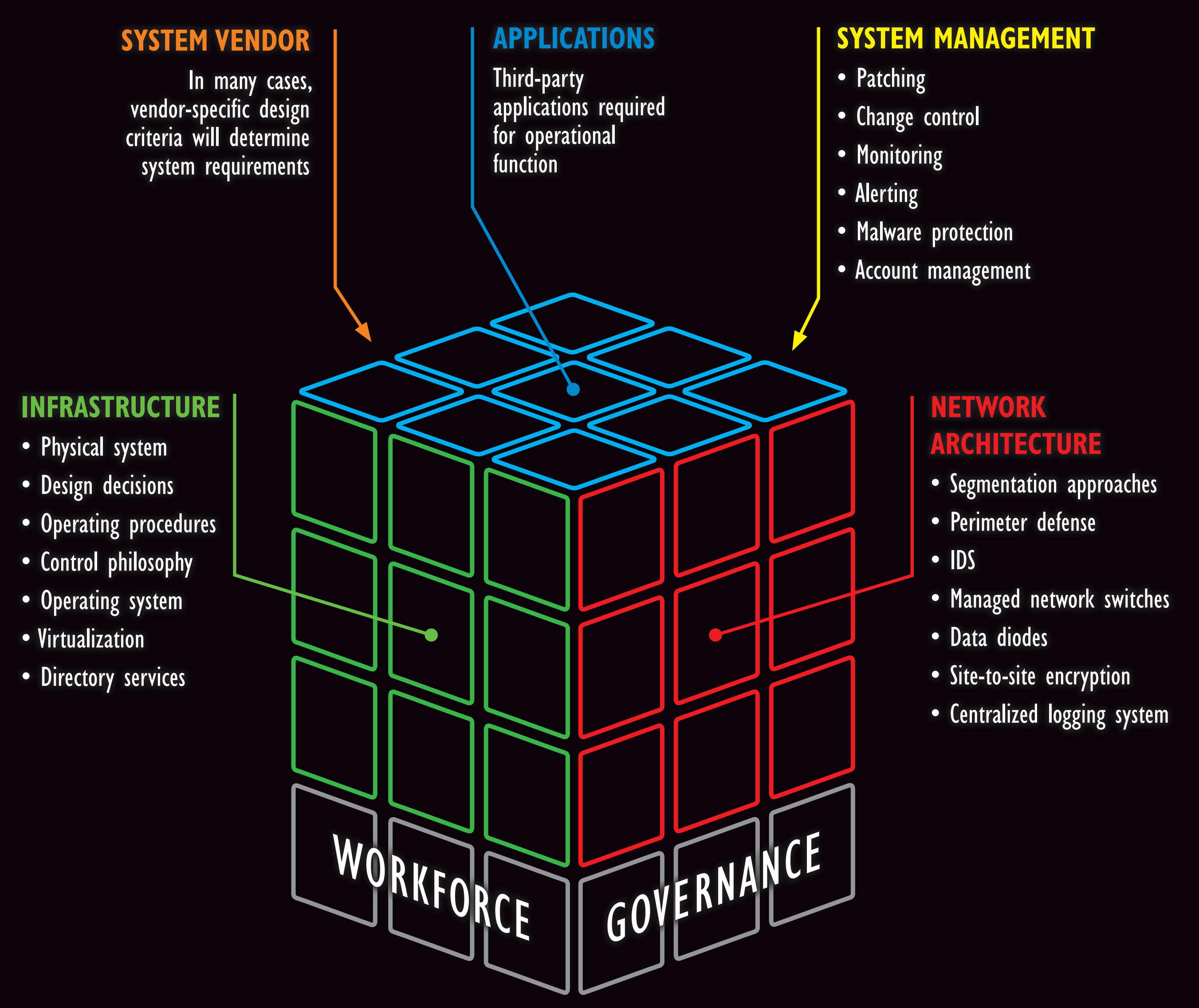
4 **ADVERSARY INTENT**

5 **EXTERNAL DRIVERS**

1 SYSTEM VARIABLES

Your cyber environment includes many elements specific to your implementation, engineering, and operational needs. Those elements combine to create a unique environment to defend and protect.

Altering any element affects the overall security of the system, with each element dependent upon other elements in the overall system.



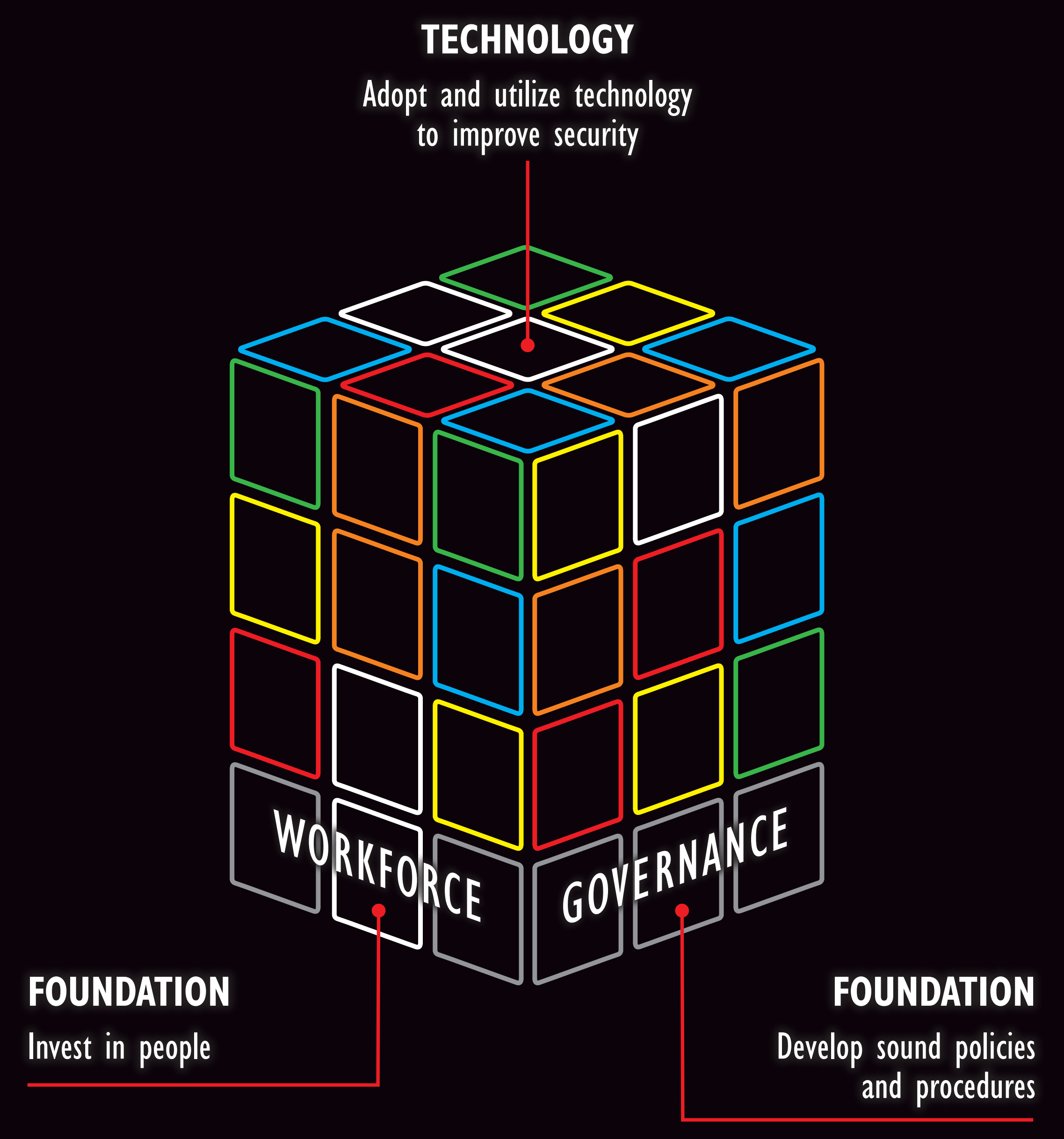
SYSTEM VENDOR
In many cases, vendor-specific design criteria will determine system requirements

APPLICATIONS
Third-party applications required for operational function

SYSTEM MANAGEMENT
- Patching
- Change control
- Monitoring
- Alerting
- Malware protection
- Account management

INFRASTRUCTURE
- Physical system
- Design decisions
- Operating procedures
- Control philosophy
- Operating system
- Virtualization
- Directory services

NETWORK ARCHITECTURE
- Segmentation approaches
- Perimeter defense
- IDS
- Managed network switches
- Data diodes
- Site-to-site encryption
- Centralized logging system



TECHNOLOGY
Adopt and utilize technology to improve security

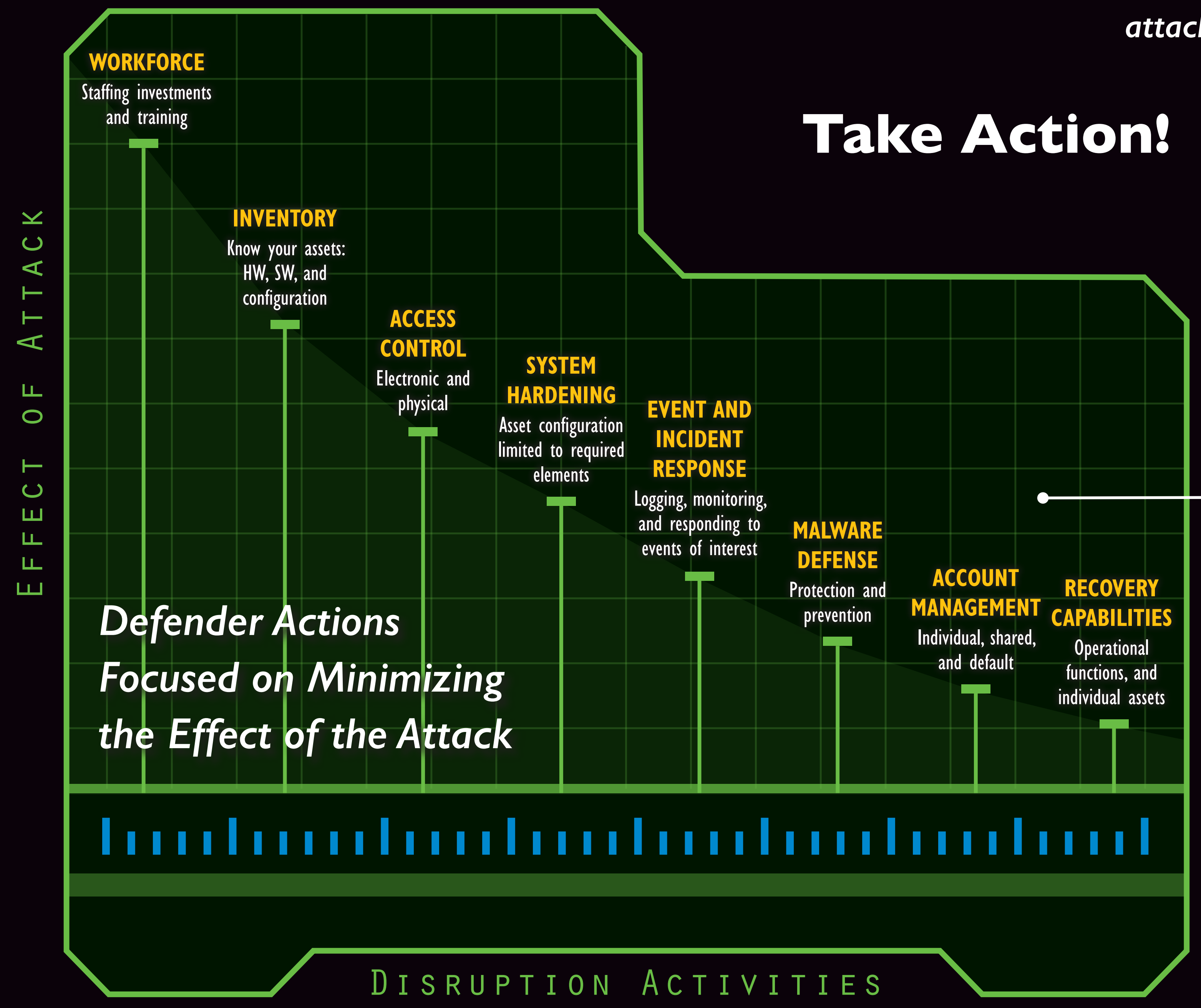
FOUNDATION
Invest in people

FOUNDATION
Develop sound policies and procedures

2 CYBER MATURITY VARIABLES

Your actions as the system owner will affect the attacker's strategy and possibly the outcome.

Take Action!



WORKFORCE
Staffing investments and training

INVENTORY
Know your assets: HW, SW, and configuration

ACCESS CONTROL
Electronic and physical

SYSTEM HARDENING
Asset configuration limited to required elements

EVENT AND INCIDENT RESPONSE
Logging, monitoring, and responding to events of interest

MALWARE DEFENSE
Protection and prevention

ACCOUNT MANAGEMENT
Individual, shared, and default

RECOVERY CAPABILITIES
Operational functions, and individual assets

Defender Actions Focused on Minimizing the Effect of the Attack

ICS defenders must consider opportunities to disrupt adversarial actions with the goal of minimizing the impact of the attack on the process or operation.

The adversary tactics, techniques, and procedures (TTP) used in your attack will be influenced by the maturity of your cybersecurity program, the effectiveness of your processes, and the capabilities of your defenders.

INITIAL STAGE

Organizations at this maturity level may be unaware of an ongoing prolonged enterprise-targeted attack with potential elements of an ICS-focused attack.

What an attack at this maturity will look like:
- Information exfiltrated
- Multiple access points obtained
- Privileged accounts obtained
- External party or adversary may identify the attack

DEFINED STAGE

Organizations at this maturity level may have already undergone an enterprise-targeted Stage-1 attack or an ICS-focused Stage-2 attack and are working on mitigation.

What an attack at this maturity will look like:
- Movement throughout the environment using in-place tools and software
- C2 channel hidden in trusted communications
- Targeted organization or external party may identify the attack

OPTIMIZED STAGE

Organizations at this maturity level are proactively monitoring and responding to potential attacks with Active Defense techniques to defend the enterprise and ICS environments.

What an attack at this maturity will look like:
- Relatively silent
- Relies on external communications paths with trusted parties
- May utilize zero-day elements
- Targeted organization will likely identify the attack

SANS ICS Industrial Control Systems

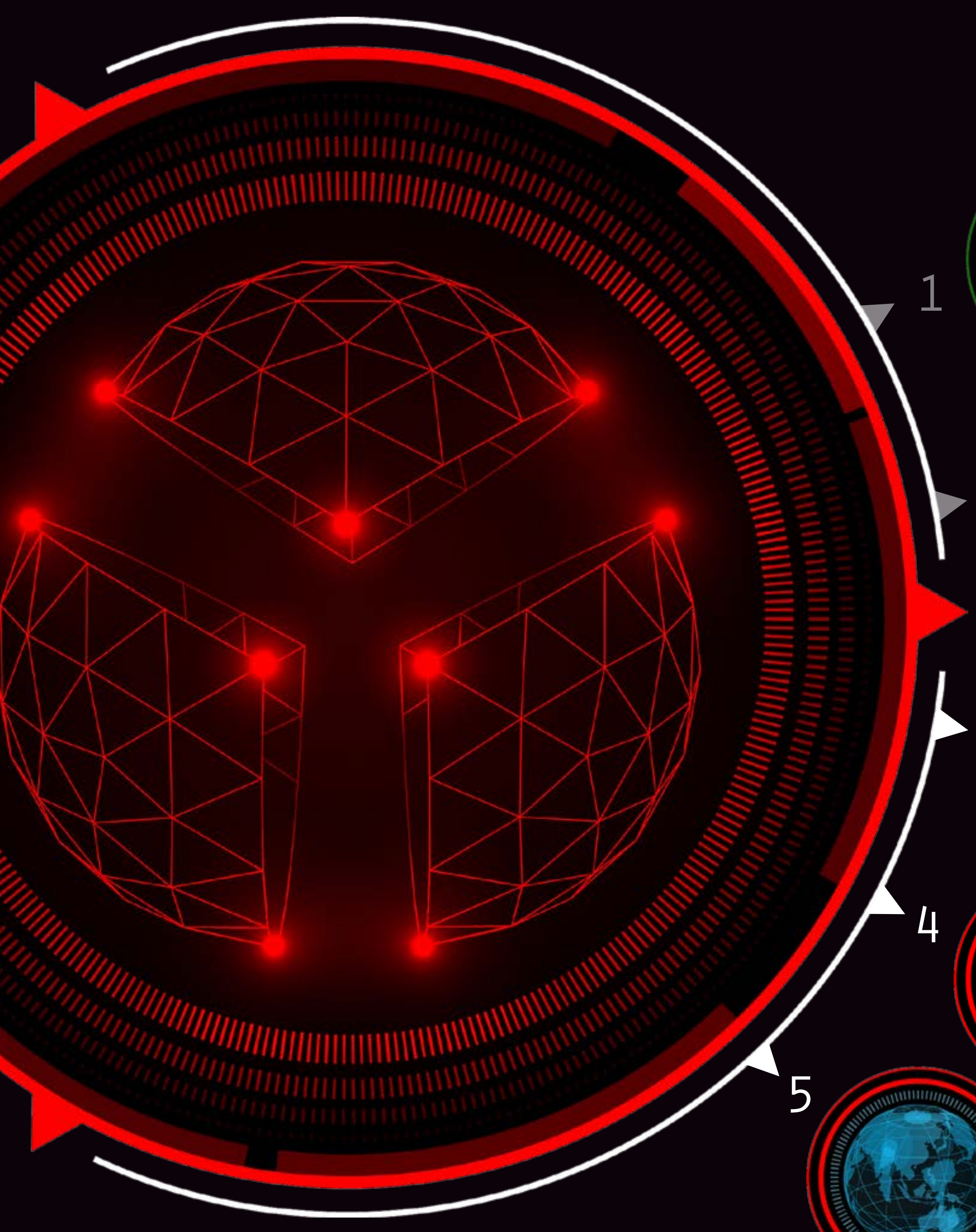
Perspectives of a Cyber Attack

POSTER

ics.sans.org

JOIN THE ICS COMMUNITY
https://ics-community.sans.org/signup

ICS-PSTR-ATTACK-0117-v1



1 **SYSTEM VARIABLES**

2 **CYBER MATURITY VARIABLES**

3 **ADVERSARY CAPABILITIES**
As an ICS defender, you can't control whether your organization becomes the target of a capable adversary.

4 **ADVERSARY METHODS**
ICS defenders do not control the intent, objectives, or scope of the campaign.

5 **EXTERNAL DRIVERS**
Adversary objectives and scope can be fluid and may change with external drivers such as geopolitical or economic events.

Adversary campaigns often use similar and recognizable techniques. As an ICS defender, your defensive actions (or lack of actions) will determine what your next attack will look like.

3 ADVERSARY CAPABILITIES

Seven Habits of an Effective APT

> "ADVERSARIES HAVE MANAGERS AND POWERPOINT TOO"
> -ROBERT M. LEE

Start with the Why
Define the goal of the campaign and what success looks like: data sets, project files, operational data, and capability demonstration.

Execute
Perform final-stage attacks systematically, create collateral impacts to confound and confuse recovery efforts, and follow up on ICS defender's defensive actions.

Flexibility
Target environments change – maintain a variety of accessible tools and capabilities to adapt to changes.

Lead
Stay several steps ahead of the ICS defender. Anticipate defensive responses upon discovery to ensure continuation of attack.

Understanding Human Behavior
Targeted employees generally have a desire to do a good job and help others, but they typically do not assess technical risks very well and may have a limited understanding of the interconnectedness of cyber systems.

Test to Win
Validating the exploits will achieve desired outcomes in target environment. Limit damage to non-target environments.

Avoid Discovery by Appearing Normal
Eliminate reliance on initial attack footholds and blend in to behave like a trusted user utilizing existing communication paths and tools.

4 ADVERSARY METHODS

Stage 1: Cyber Intrusion Preparation and Execution

- PLANNING → RECONNAISSANCE
- PREPARATION → WEAPONIZATION, TARGETING
- CYBER INTRUSION → ATTEMPT, SUCCESS → DELIVERY, EXPLOIT, INSTALL/MODIFY
- MANAGEMENT & ENABLEMENT → C2
- SUSTAINMENT, ENTRENCHMENT DEVELOPMENT & EXECUTION → ACT

DISCOVERY	MOVEMENT	INSTALL/EXECUTE	LAUNCH
CAPTURE	COLLECT	EXFILTRATE	CLEAN/DEFEND

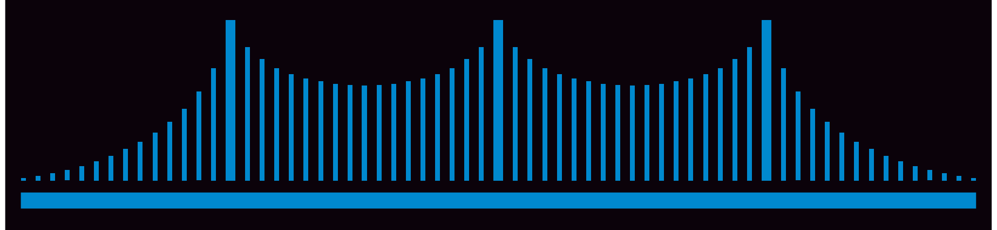
Stage 1 is based on the Cyber Kill Chain® model from Lockheed Martin

Building a bridge from Stage 1 to Stage 2

REMOTE ACCESS
- Vendors
- Support personnel
- Alternate sites
- Dial-up
- Waterholing
- Social engineering

SYSTEM MGMT
- Patching
- Monitoring
- Alerting
- Backups
- Configuration
- Change management

SYSTEM USE
- Data historians
- Environmental reporting
- Process performance
- Billing
- Metering



PLAN A
Utilize existing connections, credentials, and tools

PLAN B
Install tools, escalate privileges, and manipulate the environment

PLAN C
Utilize physical access approaches to deliver autonomous attacks or "phone home" when connectivity allows

Stage 2: ICS Attack Development and Execution

- ATTACK DEVELOPMENT & TUNING → DEVELOP
- VALIDATION → TEST
- ICS ATTACK → DELIVER, INSTALL/MODIFY, EXECUTE ICS ATTACK

ENABLING ATTACK	INITIATING ATTACK	SUPPORTING ATTACK
TRIGGER DELIVER	MODIFY INJECT	HIDE AMPLIFY

5 EXTERNAL DRIVERS

SUCCESSES
- Information sharing following Ukraine electric system attack
- Information sharing following German steelmaker attack
- Emerging and improving standards and certifications

Cyber
Scale

FAILURES
- Not patching assets
- No inventory of ICS components
- Lack of segmentation
- Internet-facing devices
- Auto run and unapproved removable media use
- No antvirus or malicious code detection
- No logging
- No monitoring

OUT OF BALANCE
- Important opportunities to share, learn, and improve