# WATERFALL®
## Stronger Than Firewalls

# The Top 20 Cyberattacks On Industrial Control Systems

The Top 20 Cyberattacks is a standard set of attacks spanning a wide range of physical consequences and attack sophistication. We can use this standard set as the basis for capabilities-based risk assessments and to compare the strength of security posture at different sites. The Cyber Design Basis Threat (CDBT) line separates those attacks that are reliably defeated by a given security posture from attacks that are not so defeated.

🟥 Undefeated Attacks    🟦 Defeated Attacks

## 1st Generation ICS Protection

**VS**

## Modern Unidirectional Protection

### 1st Generation ICS Protection (Undefeated)
- Sophisticated Credentialed ICS Insider
- Nation State Crypto Compromise
- Hardware Supply Chain
- Stuxnet-Class
- Vendor Back Door
- Compromised Remote Site
- Compromised Vendor Website
- Malicious Outsourcing
- IIoT Pivot
- Hijacked Two-Factor
- Cell-Phone WiFi
- Sophisticated Market Manipulation
- Market Manipulation
- Sophisticated Ukrainian Attack
- Zero Day Ransomware
- Targeted Ransomware
- ICS Insider

#### C-DBT
- Ukrainian attack
- Common Ransomware
- IT Insider

### Modern Unidirectional Protection (Undefeated)
- Sophisticated Credentialed ICS Insider
- Hardware Supply Chain
- Stuxnet-Class
- Cell-phone WIFI
- ICS Insider

#### C-DBT
- Nation State Crypto Compromise
- Vendor Back Door
- Compromised Remote Site
- Compromised Vendor Website
- Malicious Outsourcing
- IIoT Pivot
- Hijacked Two-Factor
- Sophisticated Market Manipulation
- Market Manipulation
- Sophisticated Ukrainian Attack
- Ukrainian attack
- Zero Day Ransomware
- Targeted Ransomware
- Common Ransomware
- IT Insider