WHAT WE’VE SEEN

66% of industrial sectors face either a high or medium capability threat, typically associated with nation-states or sponsored attackers.

WHAT THE INDUSTRY THINKS

55% believe the threat is purely accidental, and only 12% believe the threat is intentional.

68% of industrial customers feel they are well prepared for an attack.

38% believe they’ve never had an incident.

WHAT THE EXPERTS KNOW

Only 7% feel they face a threat from nation-states or sponsored attackers, and only 34% feel the threat is ‘advanced’.

58% of exploits provided remote access & visibility to criminal subscribers.

28% of exploits from a recent campaign used exploits known to be used in targeted attacks against industrial systems.

The Threat is Worse Than it Seems

Highly advanced threats can be bought. Access to cybercrime infrastructure is available by subscription.

Direct access to control systems can be purchased from cybercrime organizations.

The Threat is Real

39% of malware enters the ICS via a USB device

Once in the ICS, malware can morph into highly targeted attacks

Only 21% are planning to implement further controls within the next 18 months.

Only 18% are using application whitelisting.

Only 38% of facilities are using network based threat detection or advanced monitoring.

58% believe the threat is intentional.

55% believe the threat is purely accidental.

38% believe they’ve never had an incident.

66% of industrial sectors face either a high or medium capability threat, typically associated with nation-states or sponsored attackers.

35% of incidents can be attributed to malware, while another 36% are unknown.