

# Triton: Wake-Up Call for Collective Action

## Building resilient cybersecurity in a newly connected world

As the world's first known cyberattack on an industrial safety system, the Triton malware attack on August 4, 2017, shifted the thinking of an entire industry. One year later, we examine what's changed and what's yet to be done.

## An Urgent Call for Change

The system operated as designed and shut down the plant properly, averting disaster, but an immediate joint investigation uncovered an attack perpetrated by a state-sponsored actor exploiting onsite security lapses.



The incident led to worldwide realization that similar attacks will likely be carried out, and could happen at any time on any worldwide industrial safety system, no matter who designed, engineered or provided it.

35 years after safety instrumented systems were first brought to market, the attack led many industrial plant operators and suppliers to overturn the status quo, identify risks, and be open and collaborative in addressing them.



**It's now clear that no single entity can solve this global issue:** suppliers, designers, engineers, industrial plant operators, third-party providers, integrators, standards bodies and government agencies must collaborate to address the ongoing and ever-changing cybersecurity threats in both legacy and emerging technologies.

## What Now? Time for Action

Governments, operators, designers, engineers and suppliers must recognize and aggressively act to address the risks to industrial control and safety systems, especially those built pre-IIoT, prior to the notion of cyber warfare.

Industry leaders must apply cybersecurity standards for industrial control and safety systems that take the entire threatscape into account, while governments encourage adherence to these standards.

The industrial safety system supply chain must commit to cyber hardening of platforms, while plant operators and owners adopt and educate on practices and procedures to address today's cybersecurity risks.