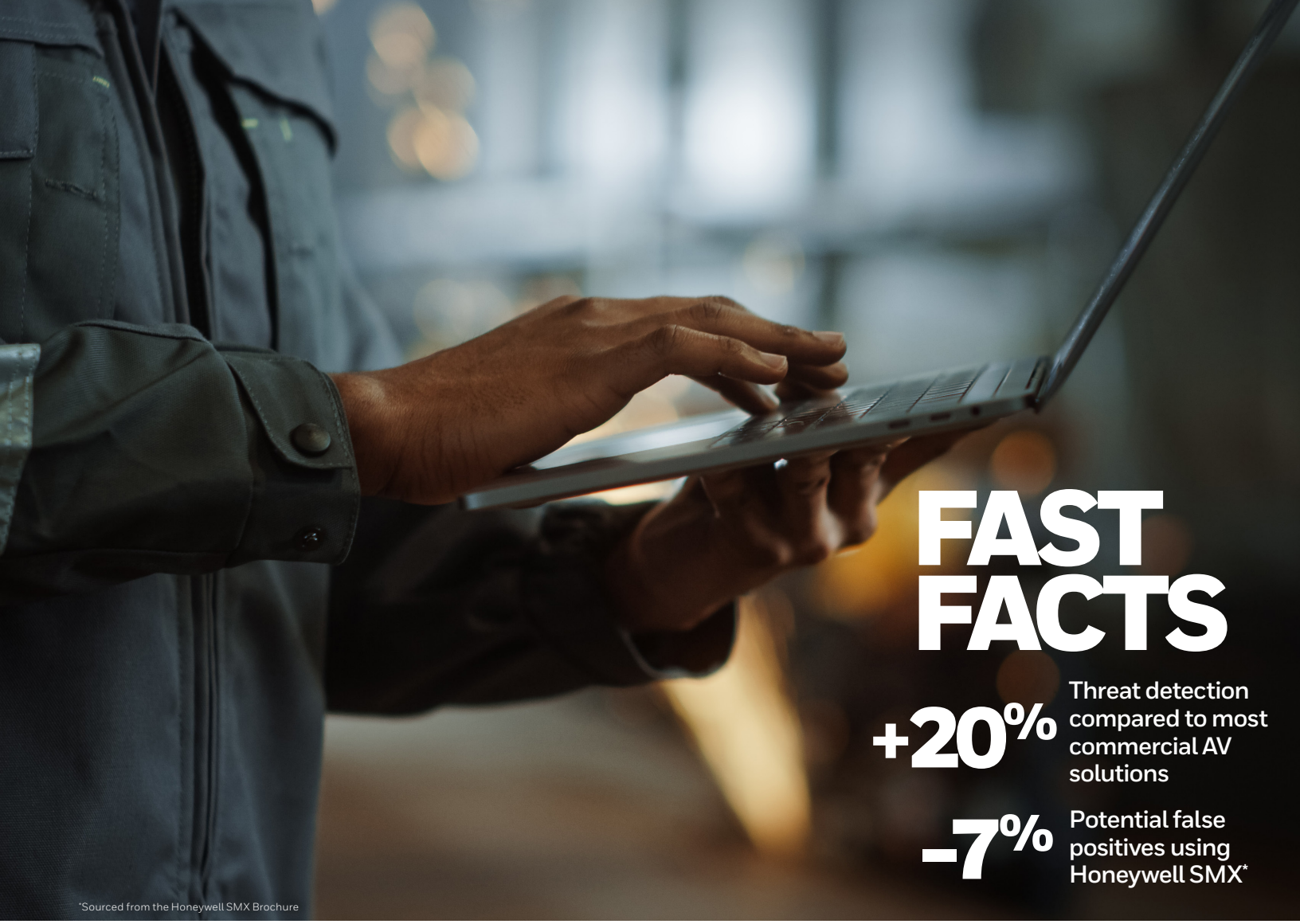
Honeywell

BATTLING TRITON

A petrochemical plant avoids potential catastrophe in Honeywell SMX trial

Case Study



A NEAR MISS

Industrial facilities have a responsibility to keep operations, employees and the surrounding environment safe from potential harm. That's why it's imperative to have numerous safety measures and processes to reduce risk and help prevent operational disruptions. But what happens when a cyber threat slips through the first line of defense and disables the last line of defense?

A petrochemical company was trialing Honeywell Secure Media Exchange (SMX) in their plant. At the time, the customer used an offline USB scanning station, with one positioned at the hydrogen-sulfide[1] operators' station. An engineer arrived on site and plugged in a USB drive to the offline scanning station and no threats were detected. The engineer then plugged in the same USB device to Honeywell SMX and immediately received an alert for a positive detection of malware. Believing this was a false positive, the engineer repeated the process three times with the same outcome; the legacy solution found no threats while SMX detected the threat each time.

As part of the trial, the customer called the Honeywell Global Analysis, Research & Defense (GARD) Team directly to report the perceived false positives from SMX. This prompted the GARD team to perform an in-depth analysis where they uncovered Triton malware which was designed to target the safety system.

This near miss compelled the customer to immediately order SMX with a secondary order to amplify their cyber defenses. Had the SMX trial not been activated, the Triton malware could have accessed and infected the network potentially impacting the safety system. This infection could have caused major operational disruptions resulting in production delays, environmental damage, financial losses, and worst-case scenario, loss of lives.

MURDEROUS MALWARE

Triton malware, also known as TRISIS or Hatman, was designed to specifically target and manipulate industrial control systems (ICS) with researchers believing its intention is to cause physical damage.[2] When the ICS emergency response systems detect potential manipulation, this initiates an immediate shutdown of processes at critical infrastructure facilities with the intent to protect human life. If the Triton malware bypasses the emergency response system and accesses a plant's network, it can interfere with the safety controller, the last line of defense, preventing the necessary shutdown with the potential to cause environmental disasters and even human casualties. The delivery method for Triton to access these facilities is either a network transfer or USB media transfer. If that doesn't seem threatening enough, the private cybersecurity industry has referred to the cyber actor behind Triton malware as, the most dangerous threat activity publicly known"[3] and, "the world's most murderous malware."[4]

SMX AND GARD

Honeywell SMX reduces cybersecurity risk and helps limit operational disruptions by providing visibility and better management of removable USB devices, activity, and content across any organization, including remote sites, off-shore facilities, or air-gapped environments in an enforceable security portal.

The GARD engine provides more secure OT threat detection, designed to help find more threats than commercial IT solutions, plus our GARD Threat Research team boasts expert support from seven Honeywell cybersecurity centers of excellence around the world.

[1] Hydrogen-sulfide: A naturally occurring, highly toxic and extremely flammable colorless gas

[2] Hackers use Triton Malware to Shut Down Plant Industrial Systems: https://www.zdnet.com/article/hackers-use-triton-malware-to-shut-down-plant-industrial-systems/

[3] US Treasury Sanctions Research Institution Connected to Triton Malware: https://home.treasury.gov/news/press-releases/sm1162

[4] Triton is the World's Most Murderous Malware: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

THE FUTURE IS WHAT WE MAKE IT

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.becybersecure.com

Case Study | Rev 1 | 09/2021

Honeywell