sans.org/ics

Industrial Control System Resources

SANS

Oldsmar, FL Water Facility Event

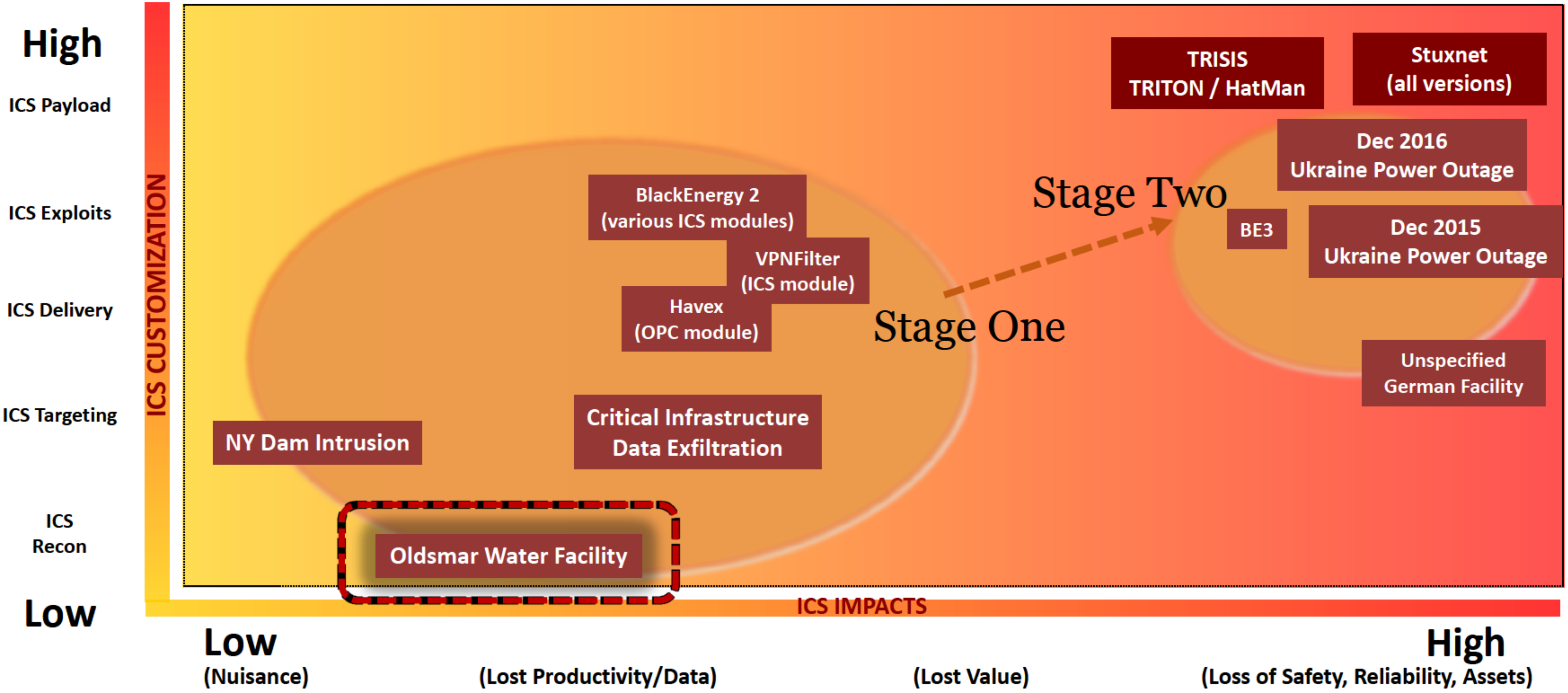
SANS ICS

Industrial
Control
Systems

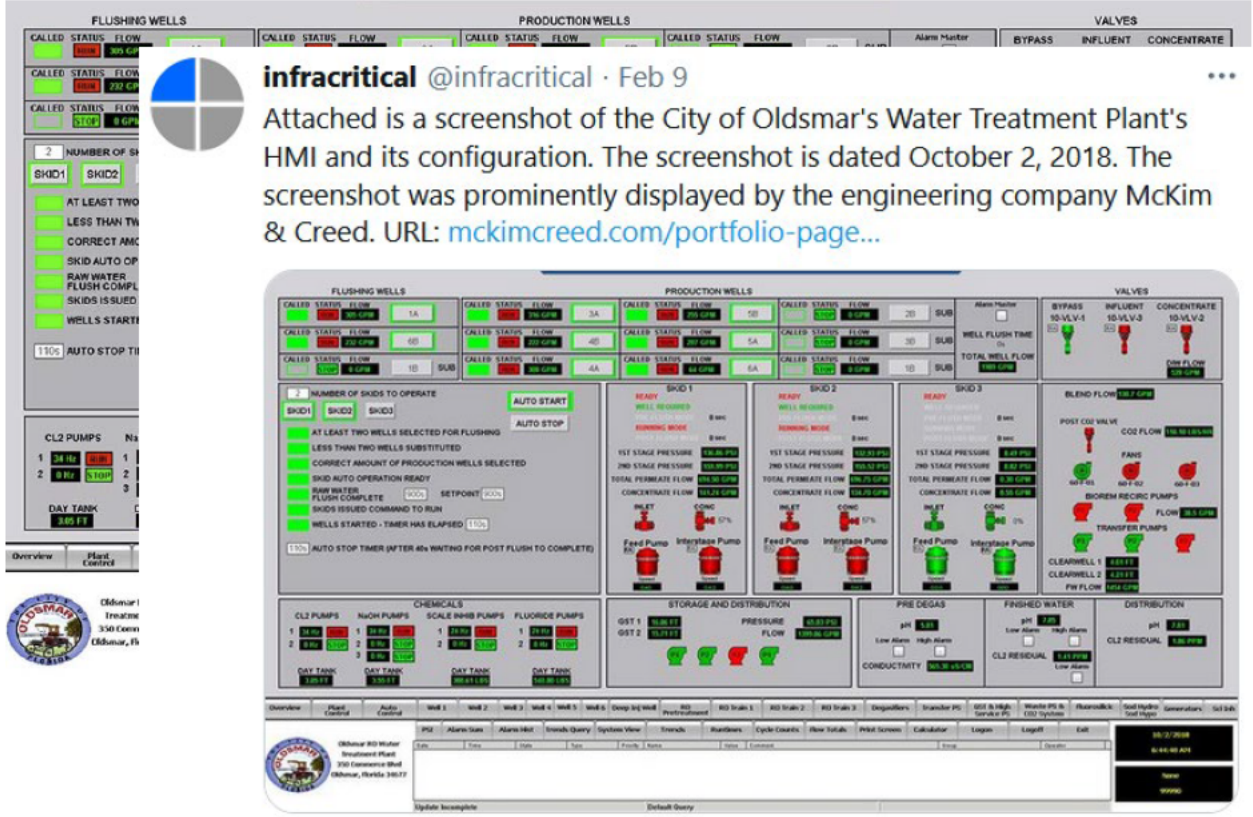
Oldsmar, FL – Water Facility – The Basics

- □ An individual accessed a water treatment system in Oldsmar, Florida on 2/5/21 and increased the levels of sodium hydroxide to potentially dangerous levels
- □ Oldsmar is about 17 miles west of Tampa with a population of 15,000 people
- □ The individual gained access through the TeamViewer remote access software in use
- □ This was not an advanced attack, this is not a new or uncommon problem

Where Does This Fit? - ICS Incidents & Access Campaigns

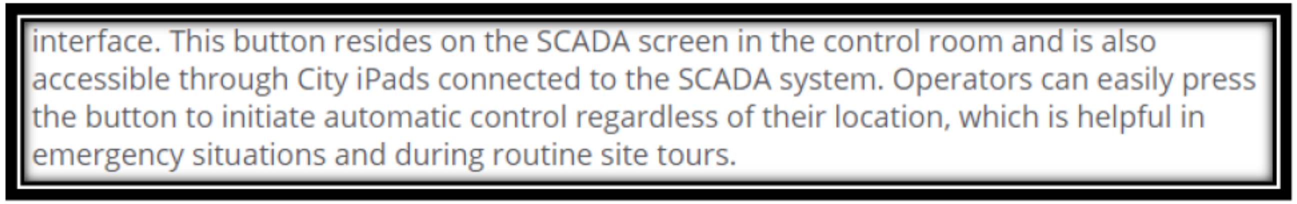


Lessons Learned in Reference to Open-Source Reconnaissance



infracritical @infracritical · Feb 9

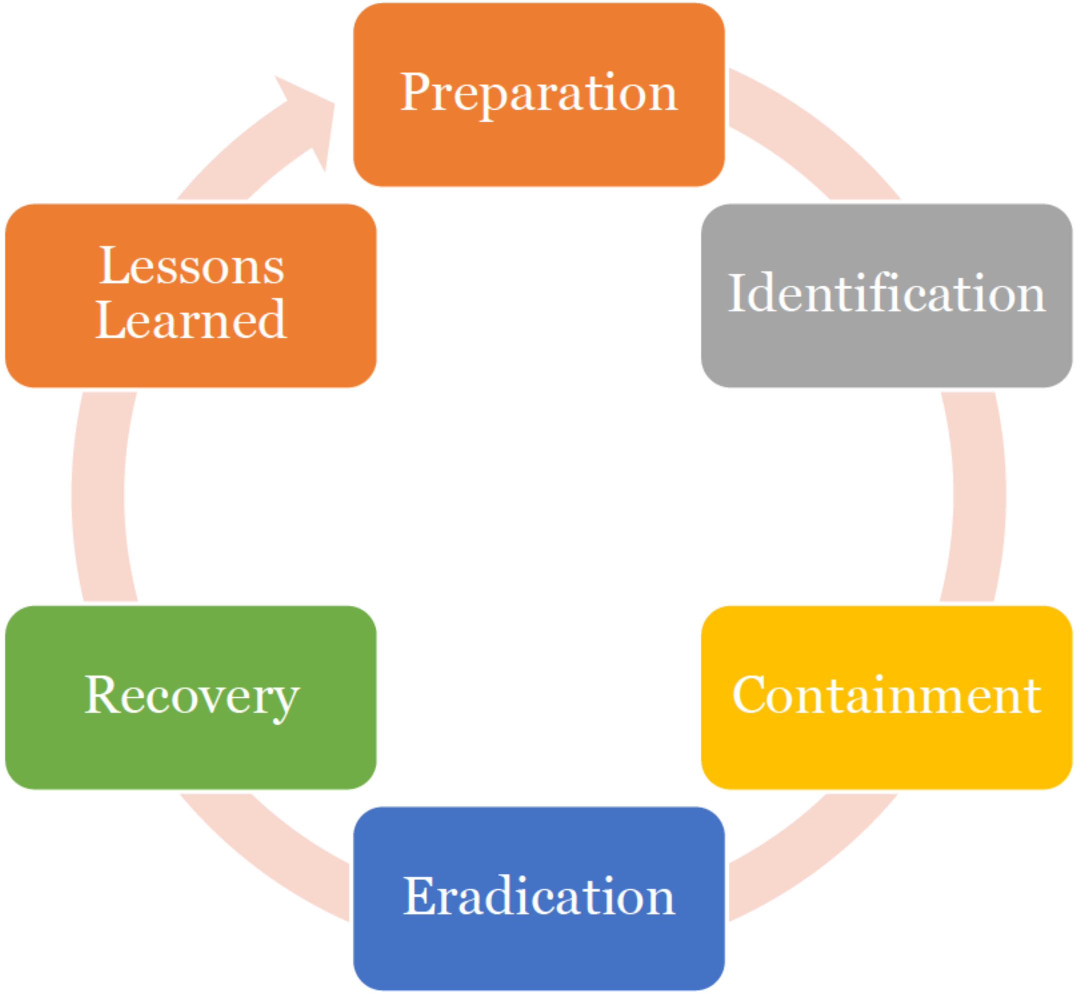
Attached is a screenshot of the City of Oldsmar's Water Treatment Plant's HMI and its configuration. The screenshot is dated October 2, 2018. The screenshot was prominently displayed by the engineering company McKim & Creed. URL: mckimcreed.com/portfolio-page...



interface. This button resides on the SCADA screen in the control room and is also accessible through City iPads connected to the SCADA system. Operators can easily press the button to initiate automatic control regardless of their location, which is helpful in emergency situations and during routine site tours.

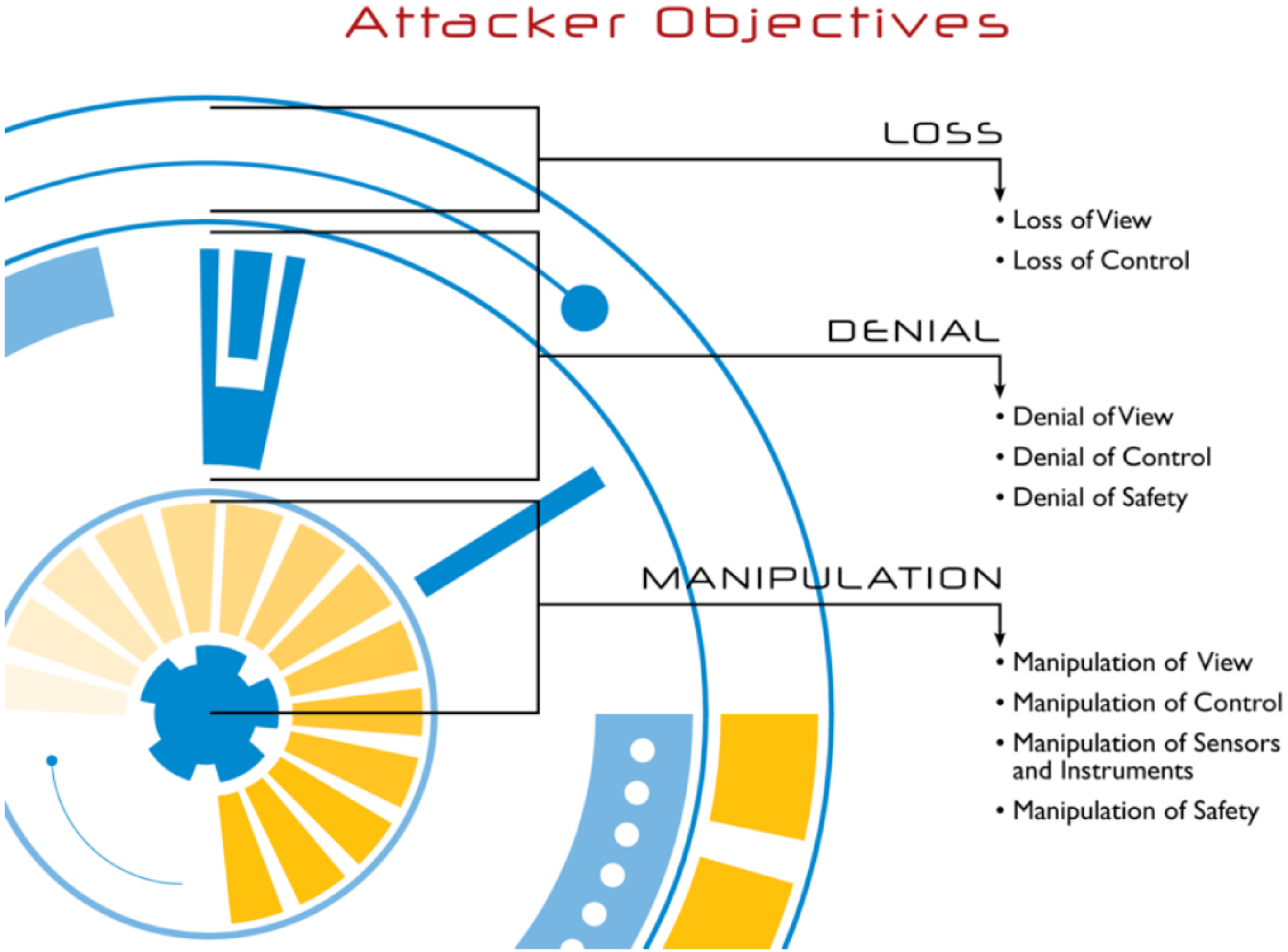
- ❑ If publicly available information about your system is interesting for an adversary, then it should be interesting to you
- ❑ Review agreements with vendors and integrators in relation to protecting your information
- ❑ Provide security awareness training related to information protections

ICS Considerations for Response Actions



- ❑ Response actions can often be IT focused: turning off remote access software, and analysis of remote application connection logs
- ❑ A joint ICS response team would also be working to understand the system design and controls in place, developing lessons learned based on what could have occurred with full access to an operator workstation, ability to manipulate alarm indicators, the potential for leave behind capabilities, ability to operate in a manner that was not operator observable, and identify the potential for additional system modifications
- ❑ ICS incident response focus needs to prioritize a shift to manual controls, manual testing to validate system readings, and ensuring system integrity.
- ❑ After action lessons learned need to look at operational engineering approaches that limits ability for misuse if they are not currently in place

Operations Impacts



Well defined plans for loss of view and loss of control at small scale or for short periods of time

Plans do not completely address events when systems are available, but do not perform the functions required or expected

Plans do not address events when systems are available, but someone else is in control of them

Resources

Overview Stories Various News Media

- Hack exposes vulnerability of cash-strapped US water plants - The Washington Post
- https://www.cbsnews.com/video/hack-in-florida-citys-water-system-reveals-potential-cyber-risks-of-many-local-communities/#app

Sector Guidance WaterISAC Resource

- 15 Cybersecurity Fundamentals (WaterISAC).pdf

FBI PIN Law Enforcement and Intelligence

- Breached water plant employees used the same TeamViewer password and no firewall | Ars Technica

Questions or Follow up

CONTACT
Tim Conway
tconway@sans.org

SANS INSTITUTE
SANS Institute
11200 Rockville Pike, Suite 200
North Bethesda, MD 20852

ICS RESOURCES
ics.sans.org
Twitter: @sansics
Community Forum:
https://ics-community.sans.org/signup

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
PRESS/PR: press@sans.org