

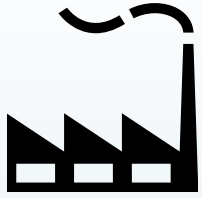


The SCADA Dilemma

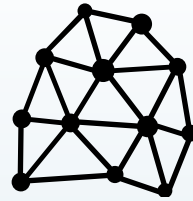
PROTECTING ICS FROM CYBER THREATS

web: www.smokescreen.io
email: info@smokescreen.io

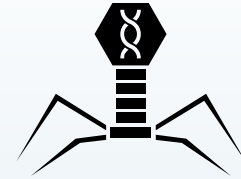




Manufacturers are the **#1 target** for cyber-espionage.



Over **1,000,000** SCADA systems are Internet accessible.



In a study, decoy SCADA systems were attacked in under **18 hours**.

If there was even a remote chance of damage, would you **allow a security scan** of your SCADA / ICS systems?

We thought not.

So we built IllusionBLACK.

THE DILEMMA

Despite being high-value targets for nation-state hackers, SCADA and ICS are the most inherently insecure manufacturing systems.

Worse, you can't conduct traditional I.T. assessments or use regular security products for fear of crashing them and causing catastrophic damage.

THE SOLUTION

Smokescreen's ILLUSIONBLACK does not touch the SCADA network or devices at all.

Using next-generation deception technology, it creates decoy SCADA systems to lure hackers away from your real ICS assets into a virtual world, where their every move is monitored.

ILLUSIONBLACK

DETECT, DEFLECT, DEFEAT.

