IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Critical Infrastructure S.O.S.

Get your Stuff Off Search.

KNOW WHAT YOUR ADVERSARIES KNOW!

Attackers are increasingly working to compromise cyber and physical security – Don't get caught off guard – Get your Stuff Off Search – S.O.S.!

While zero-day attacks draw the most attention, frequently less-complex exposures to both cyber and physical security are missed. Get your Stuff Off Search - S.O.S. - and reduce Internet attack surfaces that are visible to anyone on web-based search platforms.

Exposures increasingly include Industrial Internet of Things (IIoT), Supervisory Control and Data Acquisition systems (SCADA), industrial control systems (ICS), remote access technologies, and other critical assets – which may impact public safety, human life, and national security. CISA can help you:

#1 ASSESS YOUR POSTURE

You have probably done a lot to secure your facilities. However, without visibility into your assets that are accessible across the Internet, you may not fully understand your potential for being attacked. While many people use search engines to find cat pictures, cyber attackers commonly use similar tools to locate Internet-connected IIoT devices. In fact, once a device is identified, hacking is not even required in many cases – for example, if default and maintenance passwords are in-use, the adversaries' job is easy as they just flip a switch to exploit.

#2 EVALUATE AND REDUCE YOUR EXPOSURE

After you know which assets are exposed, decide which need to be open to the Internet. Once you evaluate necessary exposure, assess how changes will affect your assets and any potential impacts to your operations. This step is important to ensure actions associated with vulnerability remediation are performed with full knowledge of safety risk and unintended consequences are avoided based on the specific implementation plan. Also, consult with your utilities, business partners, and asset owners you do business with to ensure interdependencies are considered.

#3 HARDEN AND MITIGATE YOUR RESIDUAL EXPOSURE

Protect and reduce your risk of business interruptions from cyber-attacks; get your **Stuff Off Search (S.O.S.)!** CISA has developed a How-to Guide to help you assess your IoT/IIOT – all of your Internet connected computers and industrial devices – and take risk mitigation steps. This can include changing default passwords, implementing robust patch management, installing a virtual private network (VPN), and, using multi-factor authentication. Secure your assets where possible!

#4 ESTABLISH ROUTINE ASSESSMENTS

While it's important to get your Stuff Off Search, it's equally important to make these practices routine. As IT and business needs change, continuously monitor your IoT/IIoT and other critical assets to ensure that you always know when they are exposed on the Internet.

Remain vigilant in keeping your assets protected– regular cyber hygiene is important.

Our globally connected society means we will always be vulnerable – but, through regular cyber hygiene, you don't have to be exposed!

Please visit Stop Ransomware | CISA for more information. Victims of cyber and physical attacks should report it immediately to CISA at Central@CISA.DHS.GOV, your local FBI Field Office or Secret Service Field Office. Federal and state assistance is also available through State Homeland Security Advisors and Emergency Management agencies, or the CISA Regional Offices, Protective Security Advisors (PSAs), and Cyber Security Advisors (CSAs).

* Examples are Shodan, Censys, and other full spectrum search