ExtraHop

SHIELDS UP

RECLAIM THE CYBER ADVANTAGE

Act quickly to secure the nation's critical infrastructure against foreign cyber threats.

The threat of nation-state actors against critical assets has never been higher. Defend vital infrastructure and focus on your core mission with Shields Up implementation from ExtraHop.

INCREASED CYBER RISK

Our most critical infrastructure systems are vulnerable to malicious foreign cyber activity as global tensions and threats reach a new level. The Cybersecurity and Infrastructure Security Agency (CISA) has issued Shields Up guidance for how to stay secure. Implementing the recommended controls may be difficult for security teams already struggling with staffing shortages and challenges related to remote work, cloud adoption, and legacy systems.

EXTRAHOP ACCELERATES SHIELDS UP IMPLEMENTATION

CISA's Shields Up guidance includes a range of technical and operational recommendations. ExtraHop Reveal(x) network detection and response delivers several crucial technical controls to achieve the four high-level goals recommended by CISA.

1. **Reduce the likelihood of a damaging cyber intrusion.**
2. **Take steps to quickly detect intrusions.**
3. **Ensure your organization is prepared to respond if intrusions occur.**
4. **Maximize your organization's resilience to a destructive cyber incident.**

ExtraHop professional services can also provide much needed help in staying secure without introducing friction to the business.

CISA RECOMMENDATION SUPPORTED BY EXTRAHOP

- Monitor and Secure All Remote Access Paths
- Assure Security Hygiene and Strong Encryption
- Secure Your Entire Asset Inventory
- Quickly Detect and Respond to Destructive Attacks

ExtraHop

INCREASED CYBER RISK

ExtraHop Reveal(x) network detection and response technology supports fast and thorough implementation of the CISA Shields Up guidance.

Secure Your Whole Attack Surface

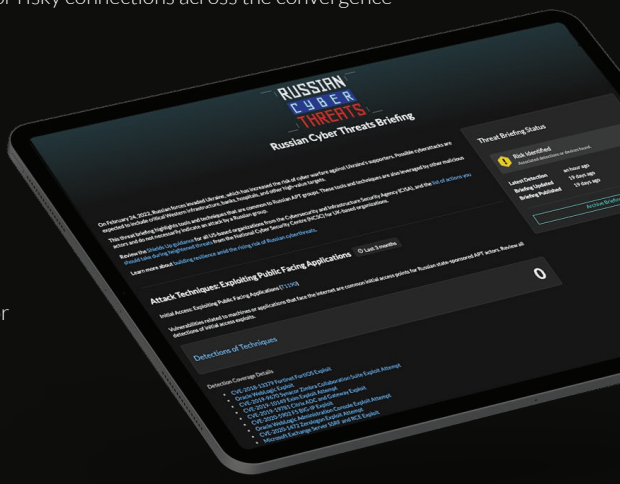
- Monitor all network traffic to, from, and inside your network for suspicious behavior.
- **Identify and secure all assets including IoT devices, critical systems, unmanaged devices, and legacy systems**
- Analyze all communications with cloud and SaaS systems and monitor risky connections across the convergence of IT, IoT, and OT networks

Assure Complete Security Hygiene

- Identify and eliminate insecure ports and protocols.
- Catch weak encryption schemes.
- Confirm and compensate for other hygiene controls.

Detect Advanced Threats Quickly

- Detect stealthy attack behaviors other tools miss.
- Decrypt traffic to catch attackers attempting evasion.
- Discover attack attempts on devices not monitored by EDR, SIEM, or other methods – such as unmanaged devices and legacy systems.



SHIELDS UP ASSURANCE

ExtraHop Advisor Services and ExtraHop Network Assurance Incident Response services are here to help your business implement Shields Up and take back the cyber advantage.

To assess your Shields Up readiness and improve your security posture, reach out to ShieldsUp@ExtraHop.com

LEARN MORE

Get our Practical Guide for Shields Up

Concrete advice for organizations in implementing CISA's cybersecurity doctrine to defend your enterprise.

GET GUIDE NOW

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to advanced threats–before they compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

Request a Free Trial **extrahop.com/request-free-trial**
Take the Demo **extrahop.com/demo/cloud**

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com