



Implement the SingCERT Guidance to Strengthen Your Security Posture

Take Back the Cyber Advantage with ExtraHop

The threat of nation-state actors against critical assets has never been higher. Defend your cyber territory and focus on your core mission with implementation of SingCERT guidance from ExtraHop.

SINGCERT RECOMMENDATIONS
SUPPORTED BY EXTRAHOP

INCREASED CYBER RISK

Companies large and small are at increased risk of attack from nation-state actors. The Singapore Computer Emergency Response Team (SingCERT) has issued guidance for how to stay secure. Implementing the recommended controls may be difficult for security teams already struggling with staffing shortages.



Identify and disable all non-essential ports and protocols



Closely monitor inbound and outbound network traffic for suspicious communications



Review Active Directory behavior and logs for unusual activity

EXTRAHOP ACCELERATES SHIELDS UP IMPLEMENTATION

The SingCERT Advisory includes a range of technical and operational recommendations. ExtraHop Reveal(x) network detection and response delivers several vital technical controls to achieve the high level goals recommended by SingCERT.

1. Secure your systems and network infrastructure.
2. Monitor network connections to quickly detect a potential intrusion.
3. Prepare for ransomware attacks.
4. Prepare for incident response.



HOW IT WORKS

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

Secure Your Whole Attack Surface

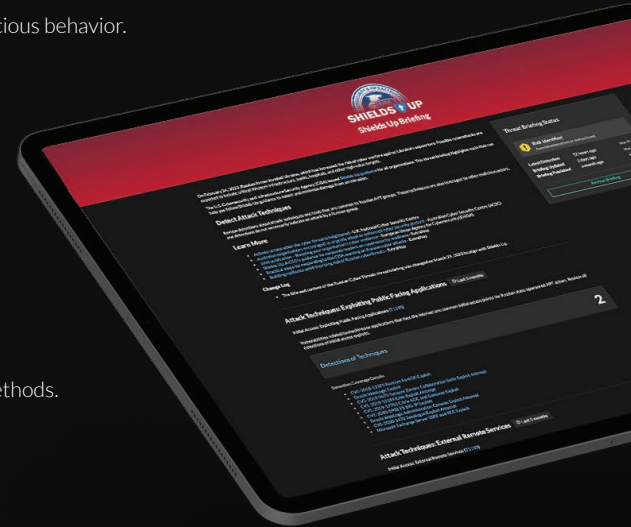
- Monitor network traffic to, from, and inside your network for suspicious behavior.
- Identify and secure all assets including unmanaged devices.
- Analyze all communications with cloud and SaaS systems.

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 not monitored by EDR, SIEM, or other methods.



SINGCERT ADVISORY READINESS

ExtraHop Advisor Services and ExtraHop Network Assurance Incident Response services are here to help your business implement SingCERT recommendations 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 a complimentary assessment of your cyber risk and readiness from ExtraHop

[REQUEST ASSESSMENT](#)

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



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