ExtraHop

Implementing Australian Cyber Security Centre (ACSC) Enhanced Security Posture Guidance

ExtraHop helps accelerate your adoption of ACSC guidance to take back the cyber advantage against heightened risk from nation-state threats.

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

INCREASED CYBER RISK

Companies large and small are at increased risk of attack from nation-state actors. The Australian Cyber Security Centre (ACSC) has issued guidance for how to stay secure. Implementing the recommended controls may be difficult for security teams already struggling with staffing. Remote work and cloud adoption, driven by the COVID-19 pandemic, further increase that challenge for your organization.

EXTRAHOP ACCELERATES ACSC IMPLEMENTATION

ACSC guidance includes a range of technical and operational recommendations. ExtraHop Reveal(x) network detection and response delivers vital technical capabilities to achieve several high-priority actions as advised by ACSC, including:

- **Patch applications and devices. Monitor for relevant vulnerabilities.**
- **Ensure that logging and detection systems are functioning.**
- **Prioritise internet facing and critical network services.**
- **Beware of ongoing state-sponsored targeting of network devices.**
- **Maintain vigilance against the threat of ransomware.**

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

ACSC RECOMMENDATIONS SUPPORTED BY EXTRAHOP

Monitor for vulnerabilities in your environment

Prioritise monitoring of internet-facing and critical network services.

Secure Your Entire Asset Inventory

Quickly Detect and Respond to Destructive Attacks

Discover MITRE ATT&CK TTPs being used in your environment

ExtraHop

HOW IT WORKS

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

Secure Your Whole Attack Surface

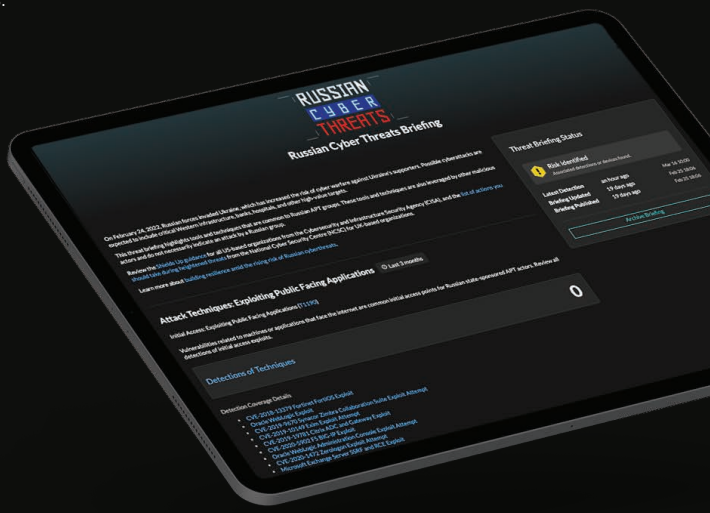
- Monitor network traffic to, from, and inside your network for suspicious behavior.
- Identify and secure all assets including unmanaged devices.
- Analyze all communications with cloud and SaaS systems.

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 behaviours other tools miss.
- Decrypt traffic to catch attackers attempting evasion.
- Discover attack attempts on devices not monitored by EDR, SIEM, or other methods



ACSC IMPLEMENTATION

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

To assess your readiness and improve your security posture, reach out to: ACSC@ExtraHop.com

LEARN MORE

Get the SANS and ExtraHop Guide to MITRE ATT&CK and D3FEND

Practical guidance for how to use ATT&CK and D3FEND frameworks to boost your resilience against advanced threats.

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**

© 2022 ExtraHop Networks, Inc. All rights reserved. ExtraHop is a registered trademark of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners.

ExtraHop

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