



# BOOST CYBER RESILIENCE

## Implementing ENISA and CERT-EU Guidance

**ExtraHop helps you take action quickly to implement cyber guidance from the European Union Agency for Cybersecurity (ENISA) and CERT-EU.**

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

EXTRAHOP CAPABILITIES THAT SUPPORT ENISA GUIDANCE

### INCREASED CYBER RISK

Companies large and small are at increased risk of attack from nation-state actors. ENISA and CERT-EU have issued joint guidance for boosting your organisation's cyber resilience. 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 organisation.

### EXTRAHOP ACCELERATES ENISA CYBER RESILIENCE IMPLEMENTATION

[ENISA & CERT-EU's guidance](#) includes a range of technical and operational recommendations. ExtraHop Reveal(x) network detection and response delivers vital technical controls to achieve faster implementation of these major ENISA recommendations:

- **Ensure all software is up to date.**
- **Control third party access to your internal networks and systems.**
- **Pay special attention to hardening your cloud environments.**
- **Employ appropriate network segmentation.**

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



**Monitor and Secure Remote Access Tools and Protocols**



**Automatically Inventory all Devices and Network Connected Applications**



**Monitor Behavioural Anomalies Across Assets and Network Segments**



**Proactively Detect and Respond to Attacks**



**Monitor Cloud and On Premises Traffic for Attack Tactics and Procedures**



## HOW IT WORKS

ExtraHop Reveal(x) network detection and response technology supports fast and thorough implementation of the ENISA/CERT-EU guidance

### Secure Your Whole Attack Surface

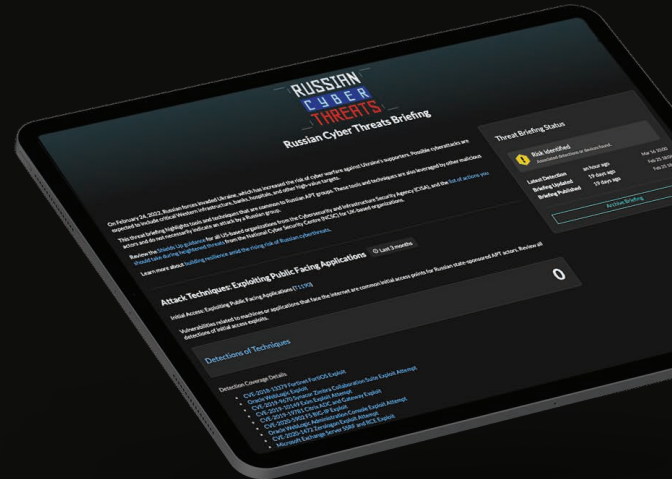
- Monitor all network traffic to, from, and inside your network for suspicious behaviour.
- Identify and secure all assets including unmanaged devices.
- Analyse all communications with cloud and SaaS systems.

### 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.



## ENISA/CERT-EU ASSURANCE

ExtraHop Advisor Services and ExtraHop Network Assurance Incident Response services are here to help your business implement ENISA/CERT-EU guidance and take back the cyber advantage.

To assess your readiness and improve your security posture, reach out to: [ShieldsUp@ExtraHop.com](mailto:ShieldsUp@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](https://extrahop.com/request-free-trial)  
 Take the Demo [extrahop.com/demo/cloud](https://extrahop.com/demo/cloud)



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