ExtraHop Urges Organizations to Adopt Shields Up Guidance, Offers Complimentary Readiness Assessment

Submitted by: Positive Marketing
Tuesday, 5 April 2022

The invasion of Ukraine has the cybersecurity community on high alert; ExtraHop puts AI-backed network intelligence to work to assess security controls and detect attack activity

SEATTLE – April 5, 2022 – ExtraHop, the leader in cloud-native network detection and response, today announced that it will offer a complimentary Shields Up assessment (https://www.extrahop.com/lp/free-shields-up-assessment/) for qualified organizations. The Russian invasion of Ukraine has put the world on high alert for retaliatory cyberattacks. Government agencies around the world have issued cybersecurity guidance to help organizations stay secure. The assessment will help enterprises align with and effectively implement the guidance from organizations such as CISA, ENISA, CERT-EU, ACSC, and SingCERT, providing real-time insight into readiness gaps such as insecure protocols, vulnerable devices, and cloud misconfigurations, as well as AI and behavior-based detection of attack patterns and lateral movement. Armed with this intelligence, security teams can zero in on, investigate, and respond to malicious activity before it results in significant impact for their organization.

The use of outdated protocols is still rampant even within sophisticated organizations. A recent ExtraHop survey (https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/) revealed that 64% of organizations admit that half (or more) of their cybersecurity incidents are the result of their own outdated IT security postures while 68% are still running SMBv1, the protocol exploited in major attacks like WannaCry and NotPetya. At the same time, adversaries are actively avoiding detection with the use of increasingly sophisticated attack tactics, including hiding within encrypted protocols, to mask the exploitation of known but unpatched vulnerabilities such as Spring4Shell.

The Shields Up assessment will allow organizations to:
- Discover all ports and protocols in use and identify insecure protocols and weak encryption,
- Find all internet-facing assets inside firewalls accepting external connections,
- Identify all cloud and SaaS services sending and receiving traffic,
- Locate instances of unpatched devices with known vulnerabilities, including Spring4Shell, Log4Shell, and PrintNightmare.

Interested organizations are invited to sign up (https://www.extrahop.com/lp/free-shields-up-assessment/) for their complimentary assessment today.

Additional Resources:

ExtraHop also released two companion pieces that provide practical recommendations on how to implement CISA’s Shields Up guidance:

- One for security organizations (https://www.extrahop.com/resources/papers/shields-up-guidance-for-organizations/), and
- One for corporate leaders (https://www.extrahop.com/resources/papers/shields-up-guidance-for-leaders/)

About ExtraHop

Cyberattackers have the advantage. ExtraHop is on a mission to help you take it back with security that can’t be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, enterprises can detect malicious behavior, hunt advanced threats, and forensically investigate any incident with confidence. ExtraHop has been recognized as a market leader in network detection and response by IDC, Gartner, Forbes, SC Media, and numerous others. Learn more at www.extrahop.com.

Press Contact
Ashley Stewart
ExtraHop
pr@extrahop.com

Jake Galland
Positive
jgalland@positivemarketing.com
+447780866874