Attack Simulation FAQ

Published: 2024-11-02

Here are some answers to frequently asked questions about detecting attack simulations with the ExtraHop system.

What is an attack simulator?

An attack simulator is also known as a breach and attack simulation (BAS). These tools enable analysts to build a threat campaign that emulates attack techniques to evaluate security tool coverage.

How does the ExtraHop system identify attack simulators?

The ExtraHop system can automatically discover and classify some attack simulators based on software or protocol activity, and then assign an attack simulator role to the device. You can also manually assign the attack simulator device role to any device.

Learn more about device roles.

How does the ExtraHop system detect attack simulations?

The ExtraHop system applies machine learning techniques and rule-based monitoring to wire data to detect both real-world and simulated attacks.

Learn more about detections.

What can I expect after running an attack simulation?

Each detection has a detection card that identifies the cause of the detection, the detection category, when the detection occurred, the risk score, and participants, such as the device running the attack simulator. A detection card appears for simulated attack techniques that were generated by an attack simulator, such as Mandiant Security Validation.

Detection cards describe how the ExtraHop system detects real-world attack techniques and behaviors. Attack simulators often simulate real-world attack traffic, but constraints might make simulated traffic different from real-world traffic. Depending on the simulation, a detection card might not exactly describe how the simulated technique was detected. In these cases, a detection card will include [Simulation] in the title. For example, the number of failed login attempts associated with a simulated brute force attack over the Remote Desktop Protocol (RDP) might be significantly lower than the number of failed login attempts during a real-world brute force attack. A **[Simulation] RDP Brute Force** detection appears, because this simulation was detected with increased sensitivity.