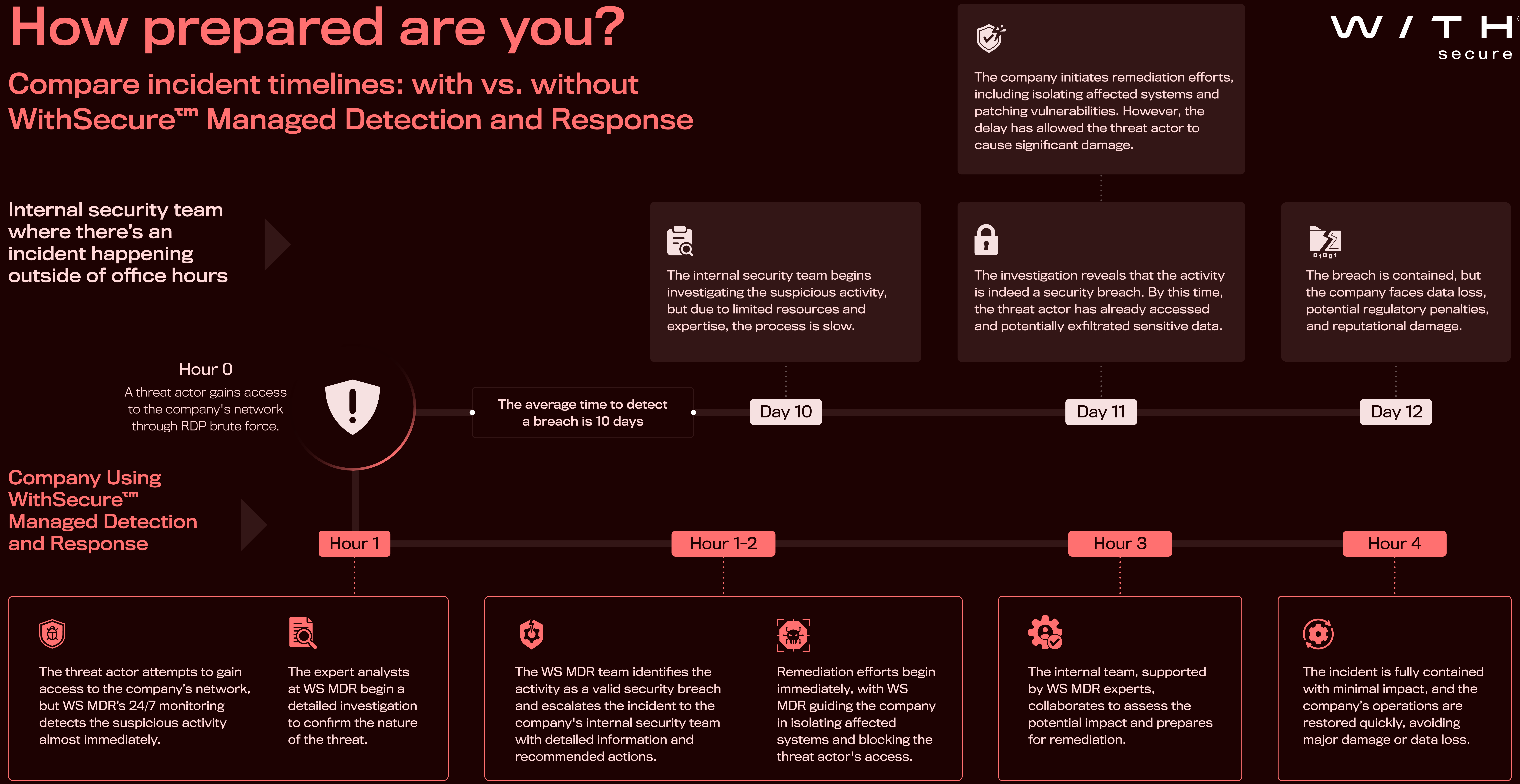
How prepared are you?

Compare incident timelines: with vs. without WithSecure™ Managed Detection and Response



Internal security team where there's an incident happening outside of office hours

Hour 0

A threat actor gains access to the company's network through RDP brute force.

The average time to detect a breach is 10 days

Day 10

The internal security team begins investigating the suspicious activity, but due to limited resources and expertise, the process is slow.

Day 11

The investigation reveals that the activity is indeed a security breach. By this time, the threat actor has already accessed and potentially exfiltrated sensitive data.

The company initiates remediation efforts, including isolating affected systems and patching vulnerabilities. However, the delay has allowed the threat actor to cause significant damage.

Day 12

The breach is contained, but the company faces data loss, potential regulatory penalties, and reputational damage.

Company Using WithSecure™ Managed Detection and Response

Hour 1

The threat actor attempts to gain access to the company's network, but WS MDR's 24/7 monitoring detects the suspicious activity almost immediately.

The expert analysts at WS MDR begin a detailed investigation to confirm the nature of the threat.

Hour 1-2

The WS MDR team identifies the activity as a valid security breach and escalates the incident to the company's internal security team with detailed information and recommended actions.

Remediation efforts begin immediately, with WS MDR guiding the company in isolating affected systems and blocking the threat actor's access.

Hour 3

The internal team, supported by WS MDR experts, collaborates to assess the potential impact and prepares for remediation.

Hour 4

The incident is fully contained with minimal impact, and the company's operations are restored quickly, avoiding major damage or data loss.

Discover WithSecure™ MDR: withsecure.com/mdr