# S&P Global
Market Intelligence

Cyberthreats targeting OT: Are organizations prepared?

Where operational technology (OT) is critical, security teams recognize the threat — but can they manage it in-house?

Which type of cybersecurity 'bad actor' — if any — has attacked, or do you expect are most likely to attack, your operational technology (OT) and/or IoT implementations?

Base: All respondents (n=302)
Source: 451 Research's Voice of the Enterprise: Internet of Things, Connectivity & Security 2023

32%

Nation state/ state sponsored hackers

47%

Criminal hackers

31%

Insider threats
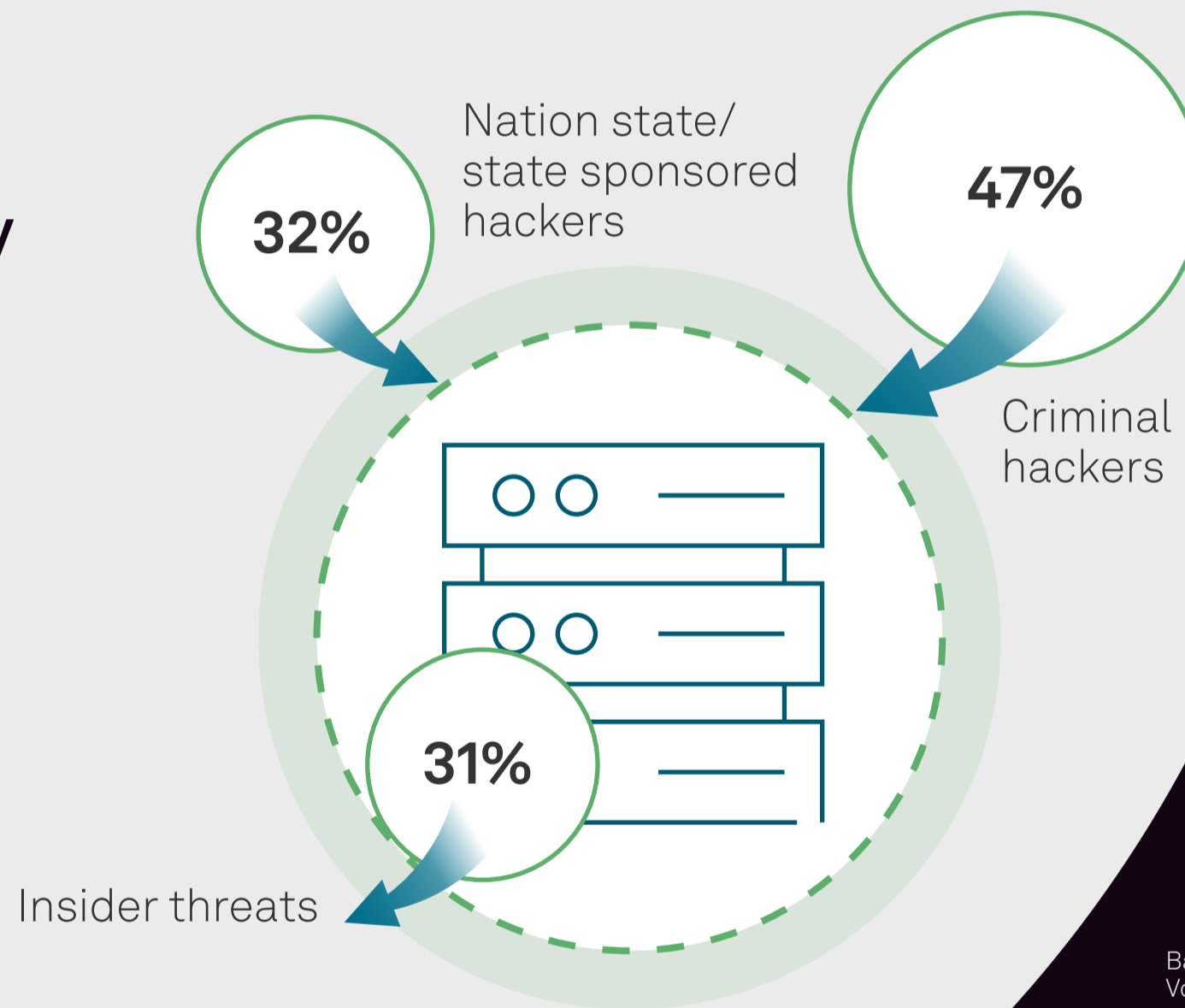
"Let's be clear. Cyber threats to our critical infrastructure represent real world threats to our physical safety."

Christopher Wray, Director, FBI (January 2023)

More than a third think their cybersecurity is inadequate.

13% believe the situation is serious.

Base: All respondents, abbreviated fielding (n=107). Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Behavior 2023.

The No.1 priority for infosec team change? Adding managed response.

37% Intend to add managed security services to specifically augment person power/staff or handle event-based responses.

Base: All respondents, abbreviated fielding (n=107).
Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Behavior 2023.

Practitioners recognize the difference managed detection and response (MDR) for OT security can make. **What can it do for you? Watch our virtual roundtable of OT security experts to learn more.**