ESG Enterprise Strategy Group | Getting to the bigger truth.™

Operationalizing the **MITRE ATT&CK Framework** in Security Operations

Timely detection and response to emerging threats, zero-day vulnerabilities, and targeted attacks depend upon the right security data at the right time, as well as strong collaboration between security and IT operations teams. Integration between security monitoring tools; security orchestration, automation, and response (SOAR) tools; the MITRE ATT&CK knowledge base; and service teams can help organizations contextualize and expedite the lifecycle of security events from detection through remediation.

Primary security analytics and operations objectives.

As they face more subtle threats, security teams are leaning on analytics and improving their operational abilities through automation of tasks and orchestration of workflows. The most targeted processes include vulnerability management and threat intelligence operationalization and how they manage and contextualize data for analysts and executives. Overlaying MITRE ATT&CK TTPs on operational workflows boosts quality, structure, and consistency of security operations and enables organizations to assess their overall cybersecurity strategy and close gaps.

40%
Improve our ability to discover, prioritize, and remediate software vulnerabilities

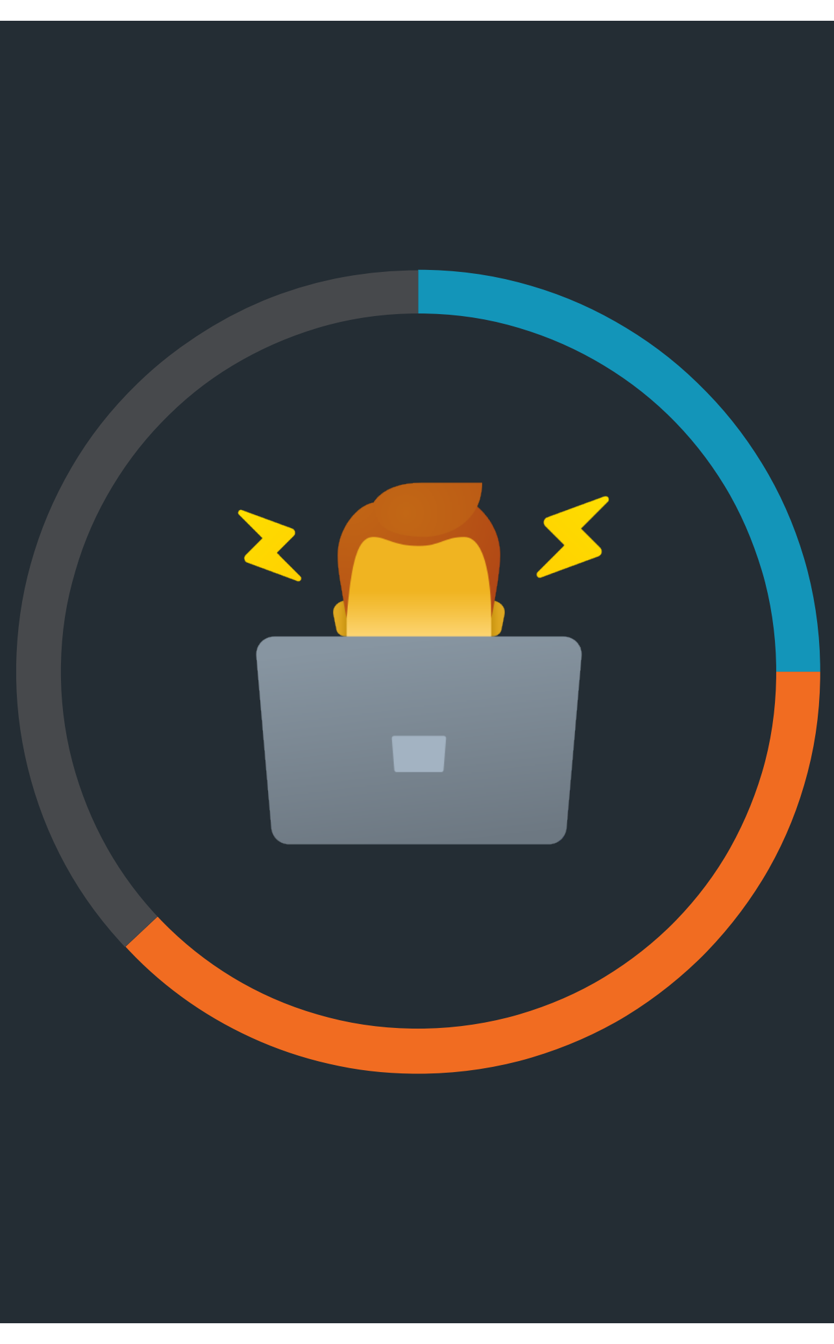
38%
Improve the operationalization of external threat intelligence

38%
Improve the management of our data pipeline to provide more real-time data for security analysis

37%
Improve our ability to combine and enrich multiple security data sources to provide more context around security events

Security analytics and operations landscape grows increasingly complex.

Unfortunately, meeting these objectives won't be easy. 63% of security professionals believe that cybersecurity analytics and operations are more difficult than they were two years ago because of factors like the increasingly dangerous threat landscape, the volume of security data needed for analysis, and an overwhelming number of security alerts that need to be triaged, prioritized, investigated, and acted upon.

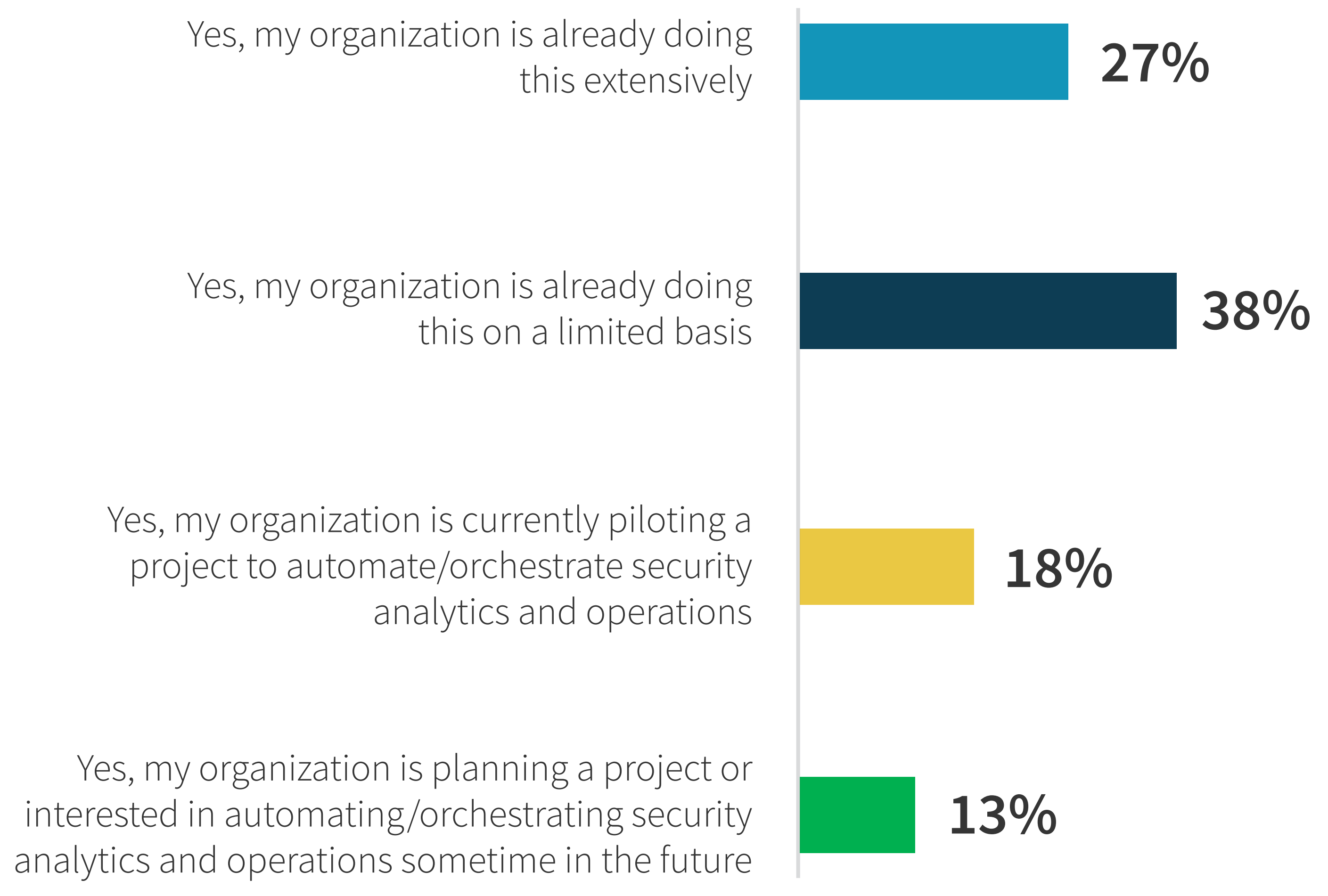


25%
Cybersecurity analytics/ operations is **significantly** more difficult today than it was 2 years ago

38%
Cybersecurity analytics/ operations is **somewhat** more difficult today than it was 2 years ago

Plans for security analytics and operations automation.

To scale security operations, many organizations are implementing SOAR technologies to help them automate security operations processes. Many firms are already using SOAR extensively while others are piloting the technology or plan to do so in the future. The data indicates that SOAR technology and security operations process automation will gain momentum in the future, leading to more extensive utilization and process automation maturity.



Priorities for security analytics and operations automation.

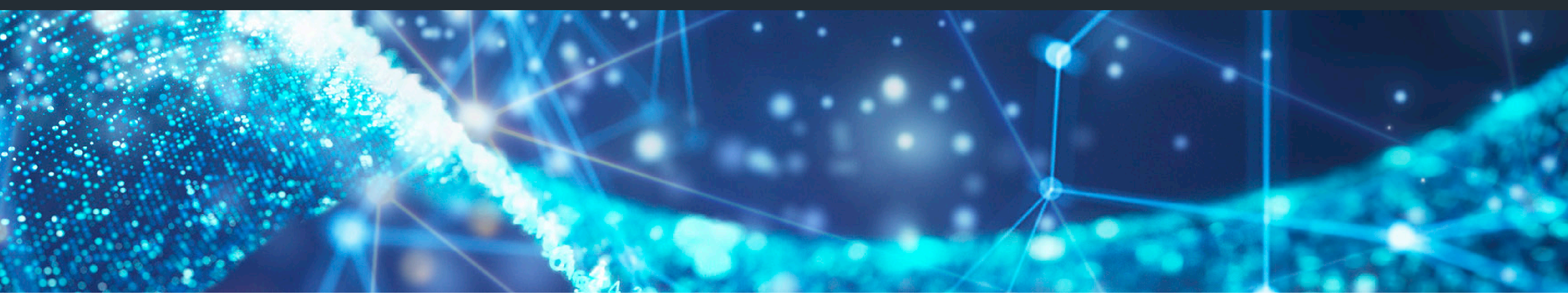
SOC teams have ambitious goals for security automation and orchestration, like integrating security and IT operations leveraging asset intelligence (like CMDBs) and improving collaboration between these two groups. Organizations want flexibility in performing remediation without being dependent on IT operations (for tasks like updating security rule sets and configuration settings). Finally, SOC teams want visibility into the entire security event lifecycle. Many firms will combine SOAR tools with the MITRE ATT&CK framework and IT systems to accomplish this. A security operations platform that acts as a single source of truth will help facilitate this.

35%
Integrate security tools with IT operations systems

34%
Improving collaboration between security and IT operations staff

29%
Automate remediation tasks without involving IT operations

28%
Tracking the security event lifecycle from discovery through remediation



The Bigger Truth

ServiceNow provides a platform that unifies SOAR, risk-driven vulnerability and configuration management, threat Intelligence, asset data, business context, and IT operations with the MITRE ATT&CK framework. This can help organizations address the scale, scope, and sophistication of today's threat landscape.

LEARN MORE

servicenow™

ESG