

State of SecOps

2021

Between the global pandemic, a widespread surge in remote work, and substantial supply-chain attacks, it has been a significant year for security operations. We surveyed 500+ global SecOps decision-makers to learn what's changed, how they're adapting, and their foremost challenges.

Here are some highlights of what we discovered:

Growth of SOC teams during COVID-19:

**85%**

increased budgets

**79%**

increased adoption of advanced technologies

**73%**

increased staffing

The Essential Cloud

99%

of organizations use the cloud for IT security operations.

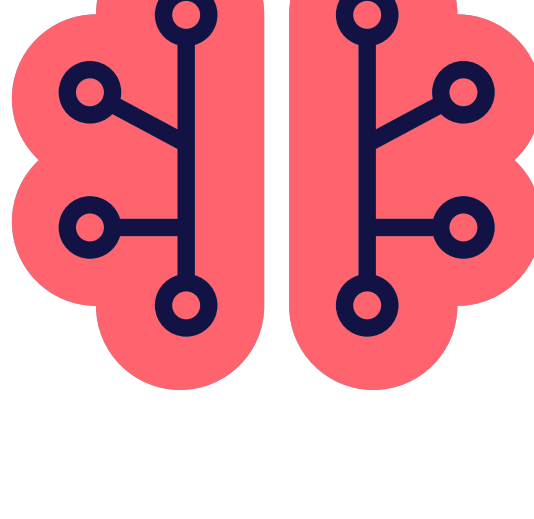
On average, these companies have two-thirds of their SecOps solutions deployed in the cloud.

85%

of companies have increased their adoption of cloud security technologies.

AI vs. Advanced Threats

59% of respondents say improving detection of advanced threats is the top use case for **AI, ML, and automation.**



Threat Intelligence

82% of companies have increased their adoption of threat intelligence.

Top two priority investments:



Setting up a threat intelligence platform (TIP).



Building a repeatable process backed by PIRs.

The Talent War

97%

of respondents report the need for additional skilled staff on their SecOps teams.



The greatest need for skills is in attack detection and analysis.

Outsourcing for Support:



92% of organizations outsource some of their SecOps functions.

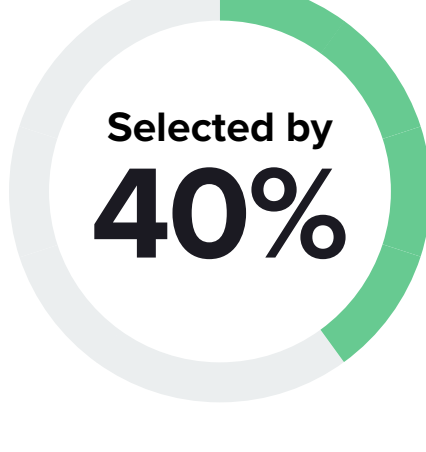
6-7

On average, 6-7 functions are outsourced to some degree.

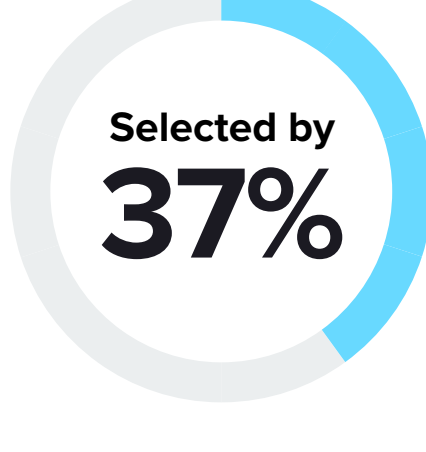
3 Top Challenges in 2021

1

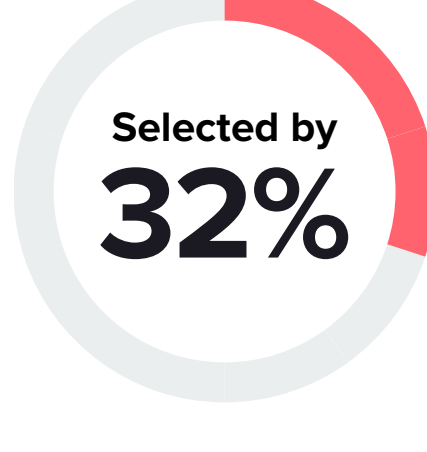
Monitoring security across a growing attack surface

**2**

Expanding workloads to cloud/hybrid environments

**3**

Pre-emptively detecting threats to reduce exposure



Read the Report

To learn more, download the 2021 State of Security Operations report. Other topics include:

- C-Level Insights
- Advanced Threat Analysis
- Digital Twin Technologies
- Defense Evaluation
- SOC Automation

[View now](#)