Nailing It!

How to win with the NIST cybersecurity Framework

Thank you for downloading this Absolute Security datasheet. Carahsoft is the distributor for Absolute security cybersecurity solutions available via NASA SEWP V, ITES-SW2, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring Absolute's solutions, please check out the following resources and information:

For additional resources:
carah.io/absoluteresources

For upcoming events:
carah.io/absoluteevents

For additional Absolute solutions:
carah.io/absolutesolutions

For additional cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
absolutesecurity@carahsoft.com
833-372-8468

To purchase, check out the contract vehicles available for procurement:
carah.io/absolutecontracts

NAILING IT! HOW TO WIN

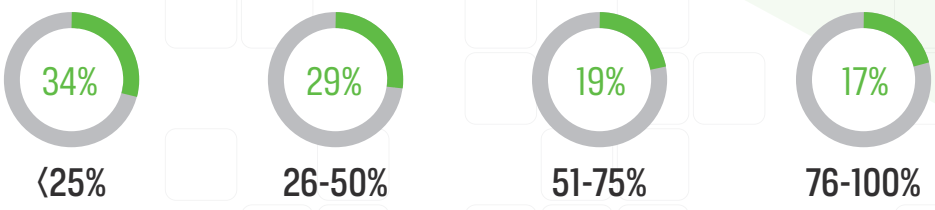
with the NIST Cybersecurity Framework

In a 2018 Absolute survey, IT and compliance professionals weighed in on their efforts to implement the five pillars of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. **How do you stack up?**

1

IDENTIFY

% of IT resources with asset intelligence:



See everything. Asset intelligence means having detailed awareness of an asset, of all its defining attributes and the behavior of the machine, along with the users interacting with it.

2

PROTECT

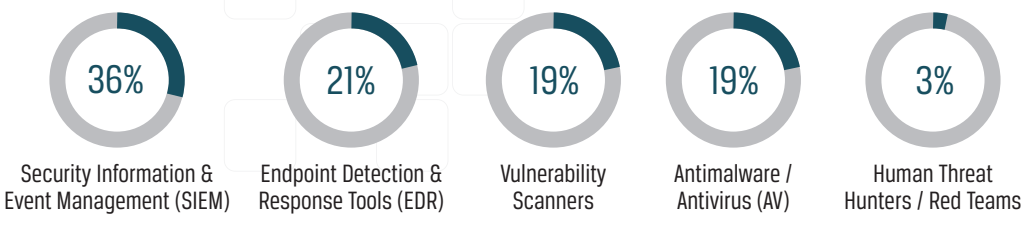
Average number of security apps and/or agents on each machine:

Build a moat. Keep security apps and/or agents to a minimum and ensure that those tools are performing as intended.

3

DETECT

Types of tools used for detecting threats and exposures:

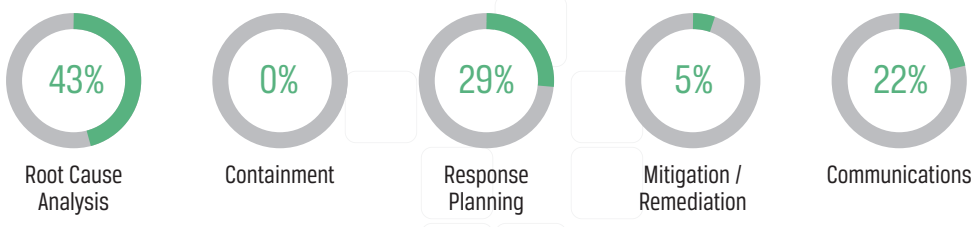


Go looking for trouble. Proactively focus on weaknesses and potential hazards to significantly mitigate risk before a compromise ever occurs.

4

RESPOND

The most neglected aspect of incident response:

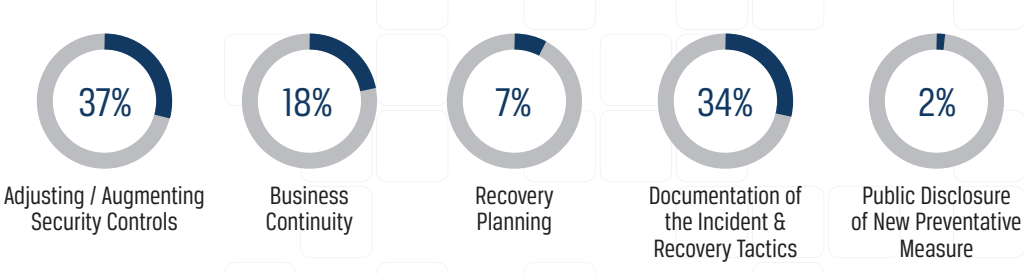


Adopt a bias to action. Analyze what went wrong after an incident, before getting back to business.

5

RECOVER

The most important action after a security incident:



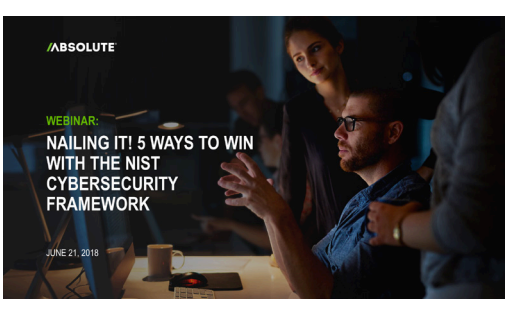
Iterate and adapt. Understand how an incident occurred, learn from it, and create a plan to avoid the same mistakes again.

WIN!

By 2020, more than half of all organizations plan to implement the NIST Cybersecurity Framework (CSF).[1] And for good reason. NIST CSF gives IT and security teams the ability to formalize their disciplines, scale their organizational groups, and push toward the shared goal of cyber resilience.

Hear the whole story by watching this recorded webinar, "Nailing it! 5 Ways to Win with the NIST Cybersecurity Framework."

You will drop in on the vibrant conversation between Forrester Research Analyst Renee Murphy and Absolute's own Josh Mayfield defining how organizations can adopt NIST CSF and achieve cyber resilience.



Source: Polls conducted during a 2018 Absolute webinar, "Nailing it! 5 Ways to Win with the NIST Cybersecurity Framework." Based on the answers of an average of 90 IT, cybersecurity and compliance professionals.

[1] Gartner webinar: Using the NIST Cybersecurity Framework.

ABSOLUTE®

absolute.com