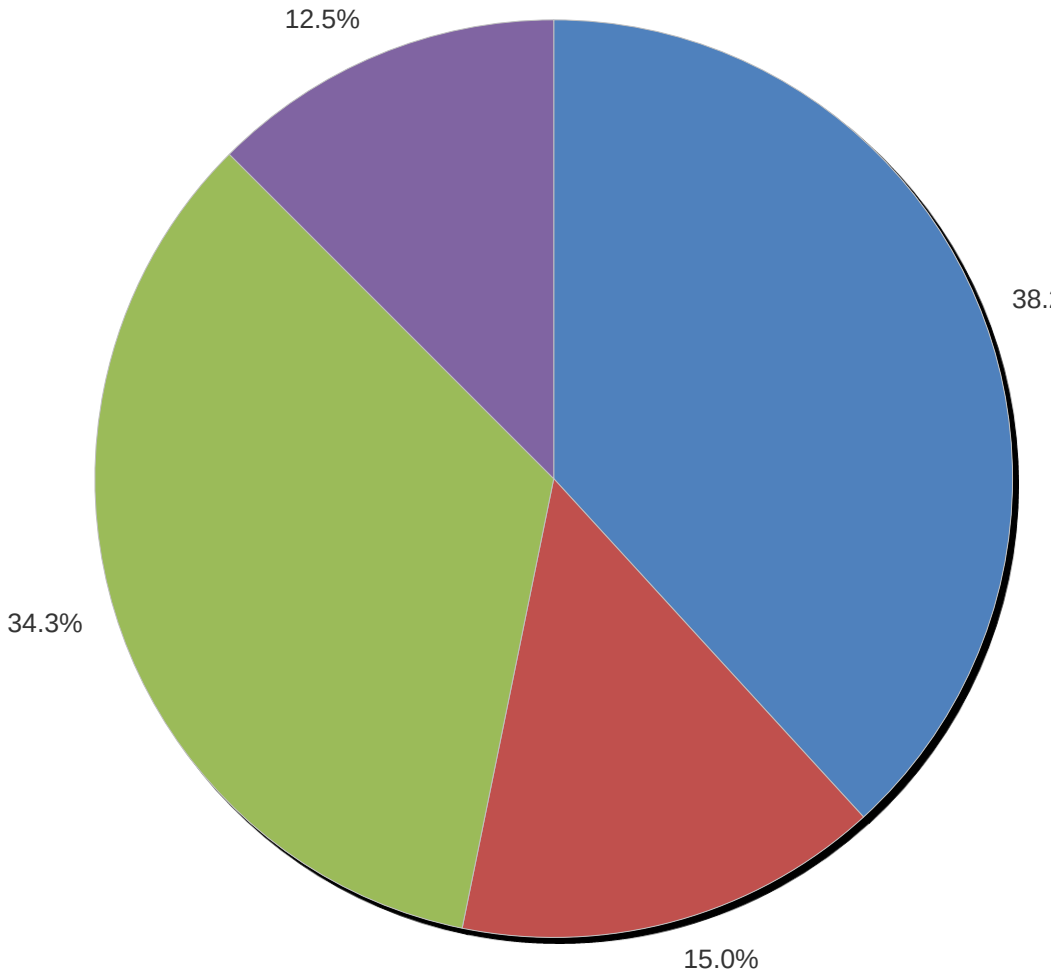
Threat Hunting Survey Results Preview

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

© 2016 SANS| All Rights Reserved

Frequency of Threat Hunting

How often does your organization perform threat hunting?

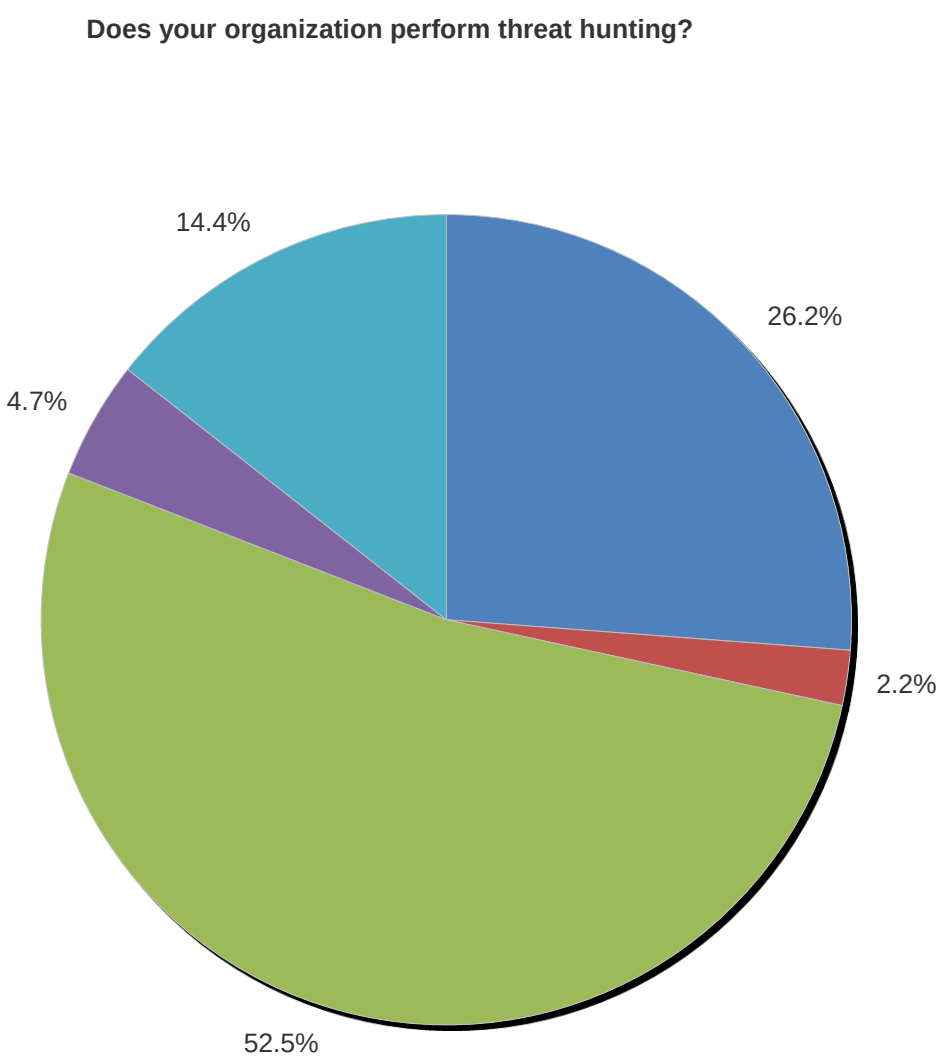


- Continuously. Our tools and analysts are always on the search for new hidden threats that apply to our enterprise risk profile.
- On a regular schedule. We schedule hunts for new hidden threats at regular intervals (such as once a week).
- On-demand. We assign analysts to hunt for the underlying problems when the need is triggered by an event or "hunch" that something isn't quite right.
- Infrequently. We only perform hunts when we know what we're looking for.

Current State of Threat Hunting

- 86% of organizations are involved in threat hunting today, albeit informally
- 40% do not have a formal threat-hunting program in place
- 86% of respondents believe anomalies are the biggest trigger driving threat hunting
- 41% who hunted based on hypotheses
- 51% of respondents say hunts are also triggered by third-party sources, including threat intelligence

Current State of Threat Hunting

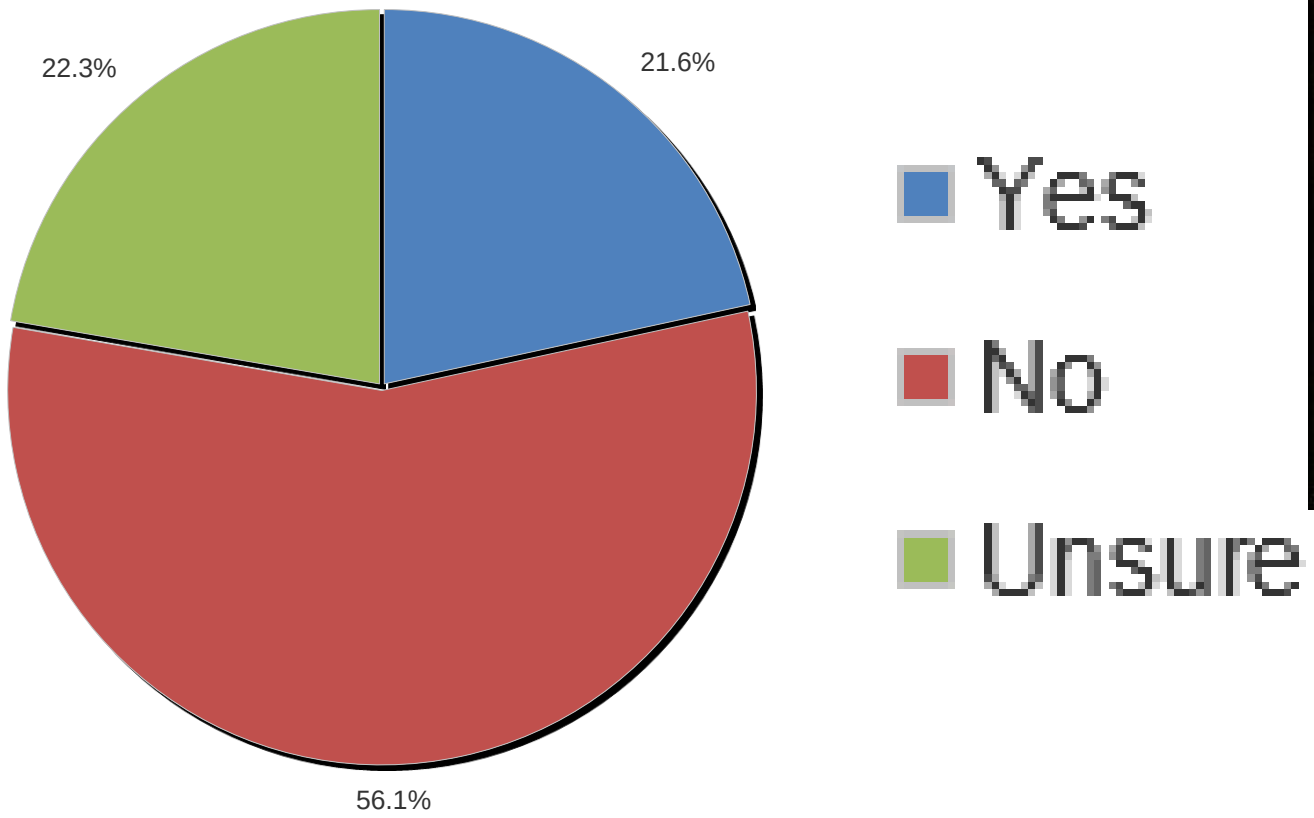


- Yes, we have defined our own hunting methodology and follow it.
- Yes, we follow a published external methodology.
- Yes, our hunting process is largely ad hoc and dependent on what we need.
- Yes, we outsource to a third party that uses its own methodology.
- No, we don't do any threat hunting.

Threat Hunting Skills Needed

Does Hunting Take Too Long?

Are you satisfied with how long it takes you to hunt for threats?

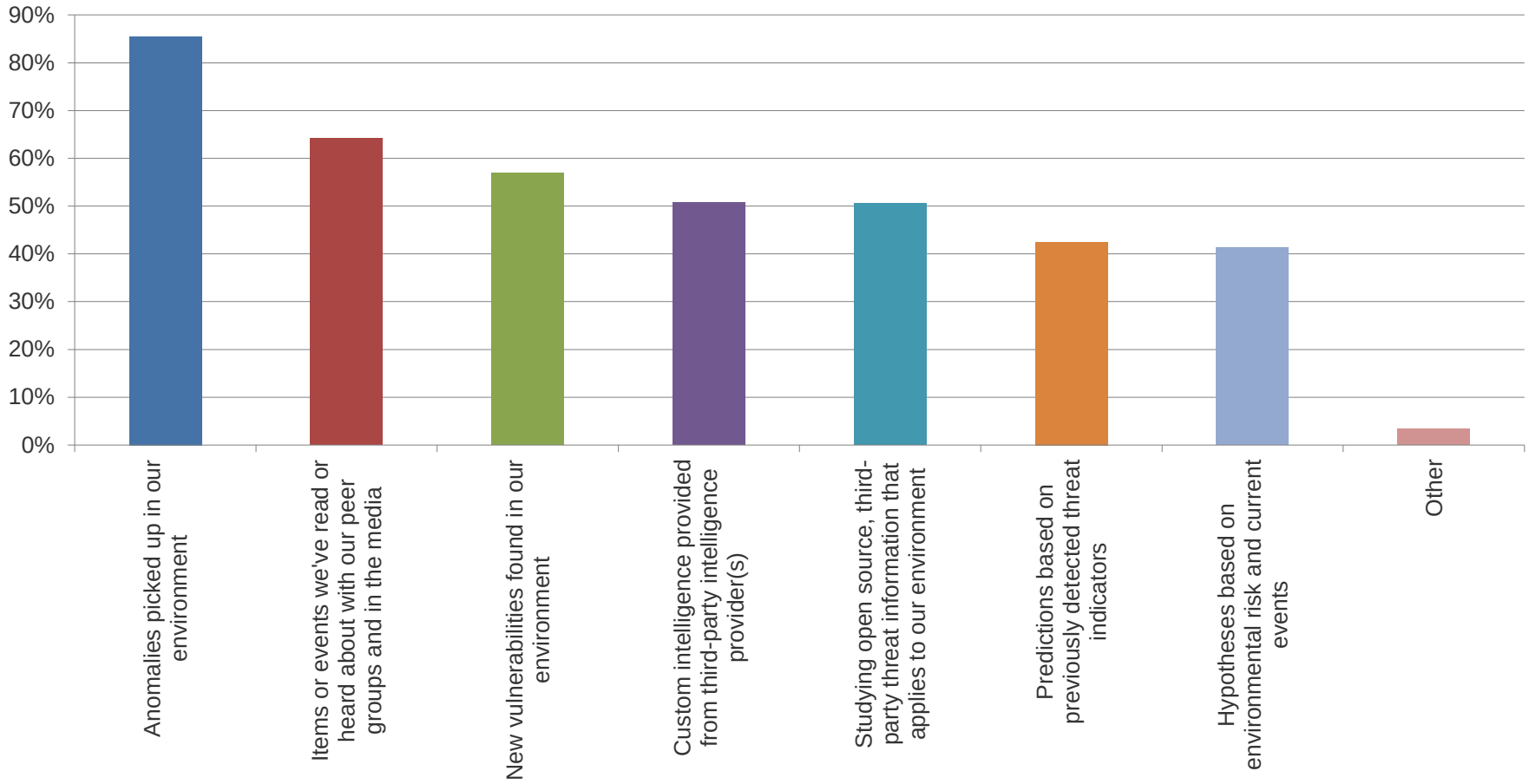


© 2016 The SANS™ Institute – www.sans.org

One Down – A Billion Left To Scan

Triggers for Hunting

What triggers active threat hunting on your network and endpoints? Select all that apply.



© 2016 The SANS™ Institute – www.sans.org

Survey Results Availability

Thursday, April 14 at 1:00 PM Eastern time
Open Season on Cyber Threats
Part 1: Threat Hunting 101
Register today at:

- www.sans.org/webcasts/open-season-cyberthreats-survey-threat-hunting-practices-101097

Friday, April 15 at 1:00 PM Eastern time
Open Season on Cyber Threats
Part 2: Threat-Hunting Methodologies and Tools
Register today at:

- www.sans.org/webcasts/101092