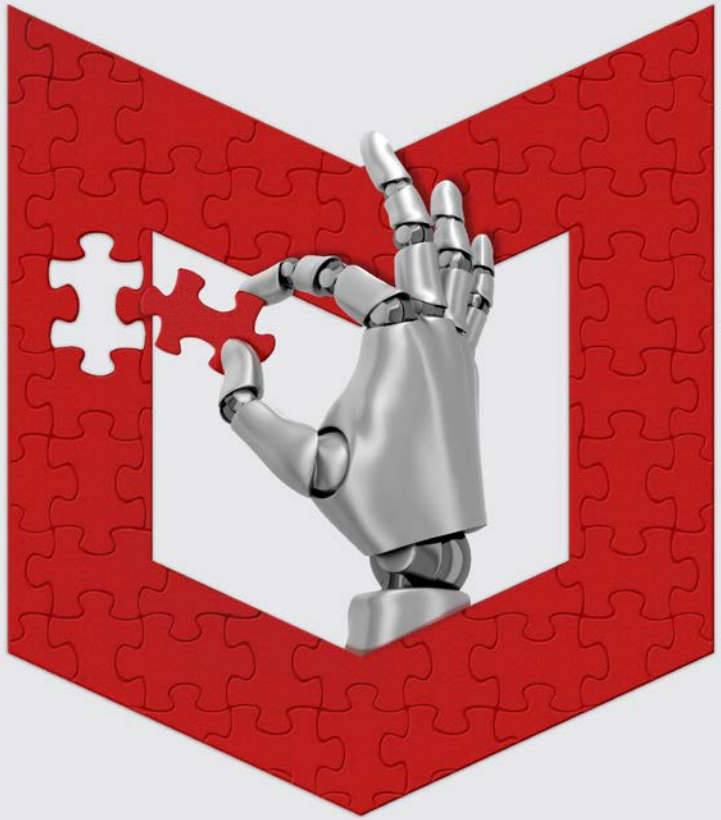
McAfee
Together is power.

Disrupting the Disruptors

Threat Hunting and the Evolution of SOC Survey

www.mcafee.com/soc-evolution



Report: *Disrupting the Disruptors, Art or Science?*

Research objective

What are the current and predicted best practices for threat hunting for different maturity levels of organizations?

- *Impact of automation, artificial intelligence, and machine learning*
- *Specific tactics of hunters sedimenting into core SOC operations*
- *Role of sandbox technology*
- *Key tools to perform threat hunting*
- *Role of threat intelligence*

Research objective & study specifications

Study specifications

- **727 interviews**
- Data was collected via online interviews
- Interviews took place in May 2017

Sample source

- McAfee customers, comprised from the Security Product Advisory Council (SPAC)
  - ✓ Worldwide, English speaking customers
- General Market sample
  - ✓ US, Canada, UK, Germany, Australia, New Zealand, Singapore

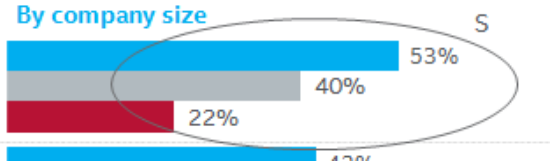
Target audience

- Organizations must have more than 1000 employees
- Respondents must spend at least 20% of their time performing Threat Hunting
- And must have Sandbox and SIEM in order to qualify

Significance test

- Differences between segments (either company size or country, etc.) as indicated in this report are based on two-sided tests with a significance level of 95%
- If findings of a certain segment are significantly higher than an other segment this has been indicated

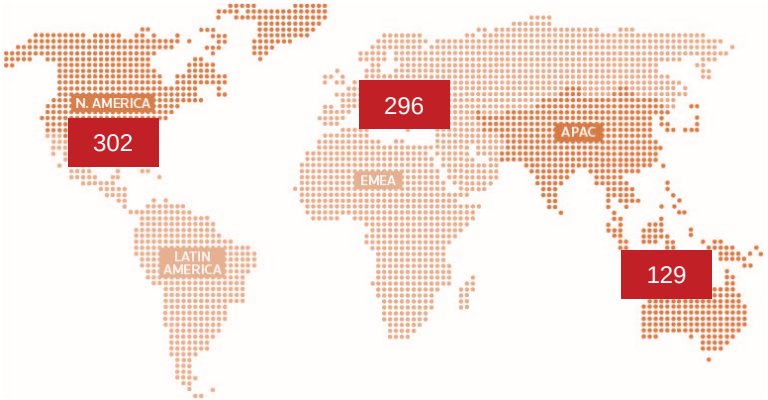
example



Audience

Large enough bases for north America, Europe and Asia

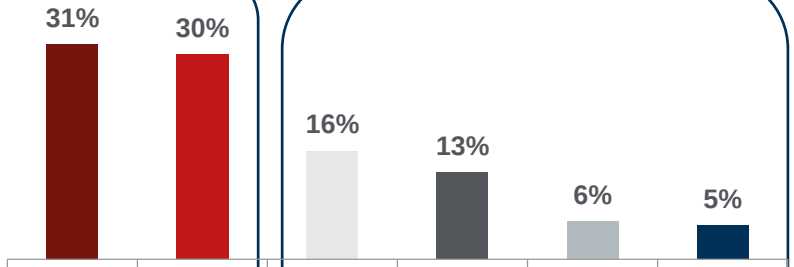
interviews per region



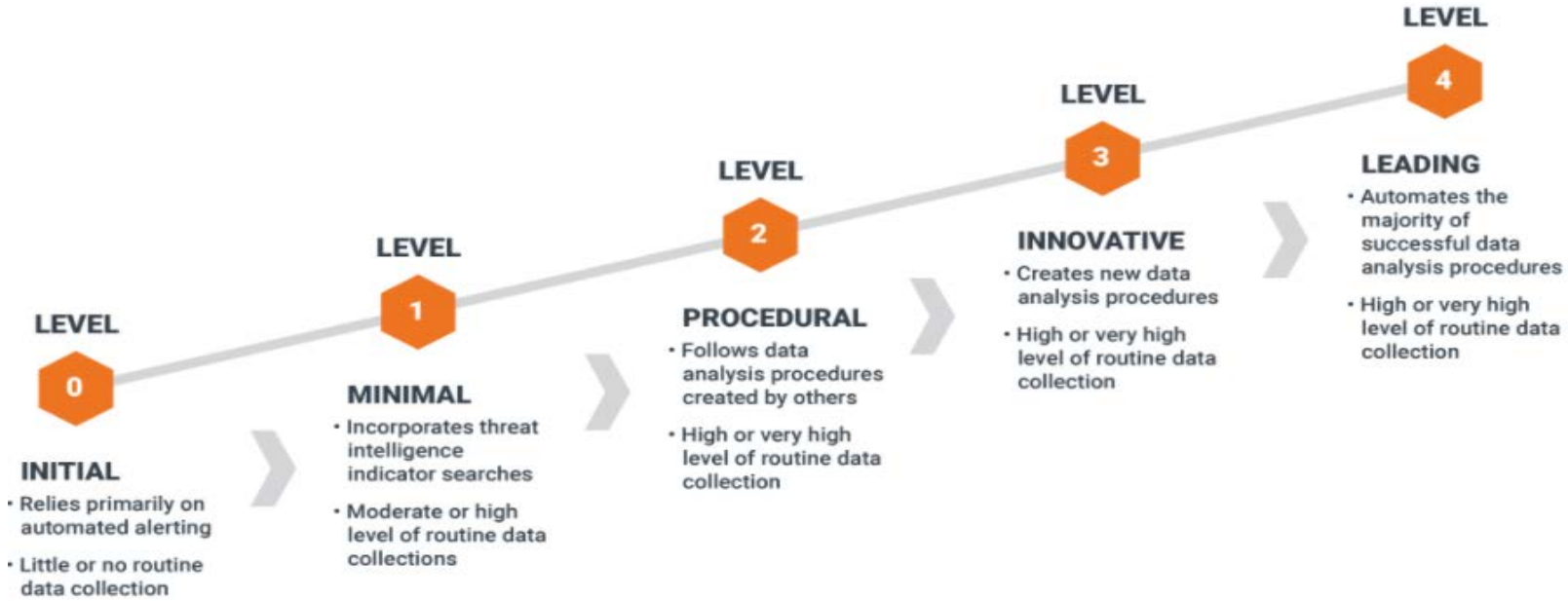
Country

US	CA	UK	AU	GE	IN	NZ	SG	Other
34%	8%	21%	4%	19%	1%	2%	10%	-

Company size (based on number of employees)



Respondents were asked to place their organization into one of 5 levels

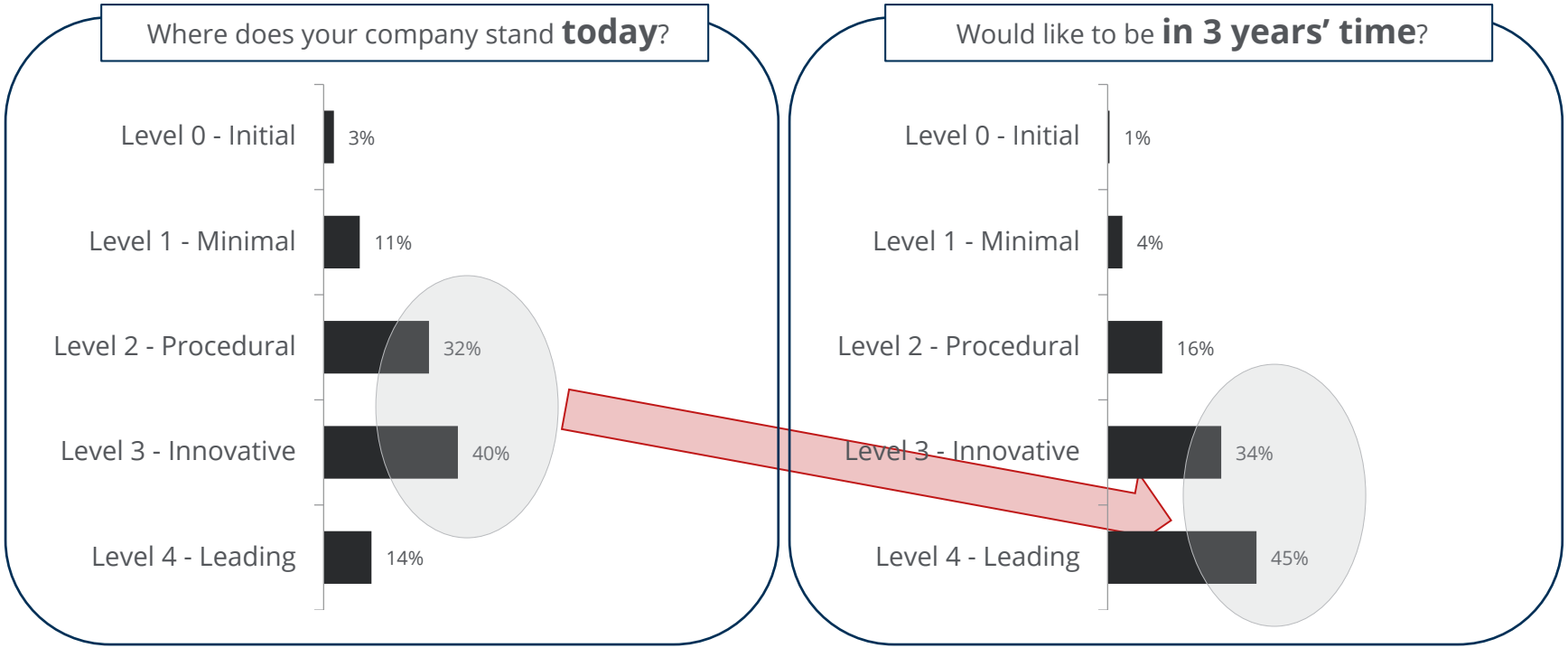


The Hunting Maturity Model (HMM)

The Hunting Maturity Model, developed by Sqrrl's security technologist and hunter David Bianco

Maturity Model – Companies WANT to improve

Nearly half of the organizations (45%) surveyed would like to be at level 4, three years from now.



Key findings: advanced SOCs get measurably better results

Improve speed and depth of investigations

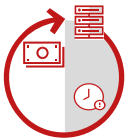
71% closed in under one week

- 71% of the most advanced SOCs closed incident investigations in less than a week and 37% closed threat investigations in less than 24 hours

4.5X as many root causes found

- Threat hunters in more advanced organizations verify root cause 4.5X (90% over 20%) more than threat hunters at the lower levels of the maturity curve

45% more value from advanced sandbox use

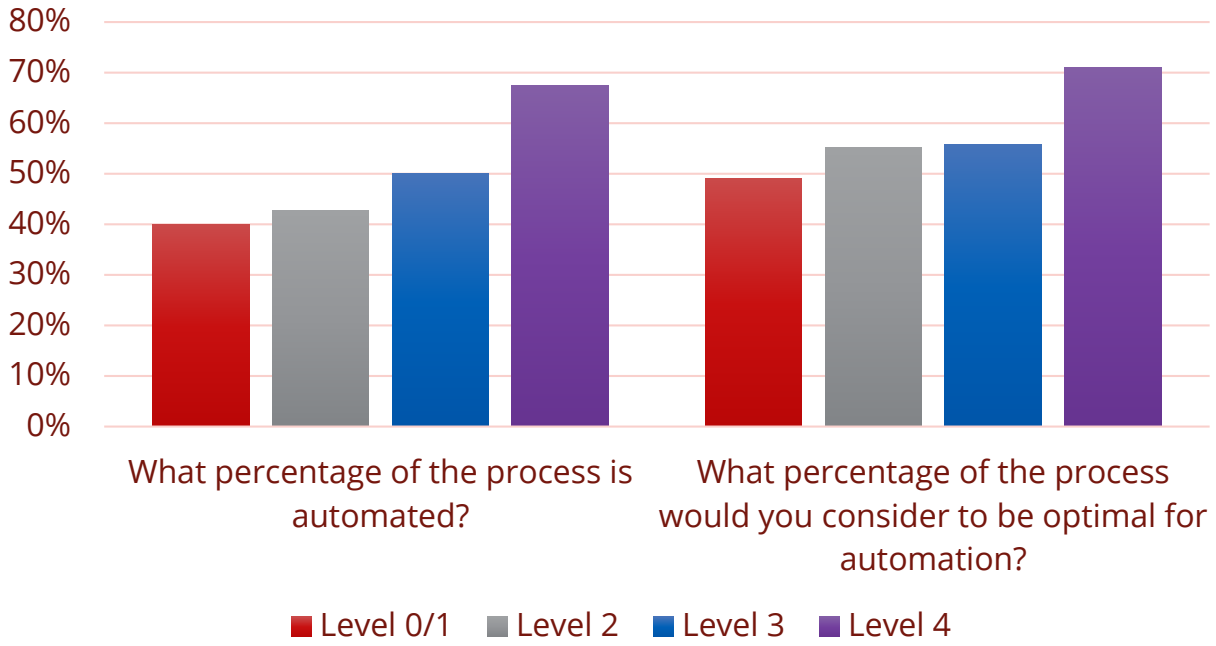


- Advanced SOCs get as much as 45% more value across the board when using sandboxes, saving costs and time, improving workflows, and revealing information otherwise not available

So how do advanced SOCs get these results?

Figure out what works, and automate it: human-machine teaming

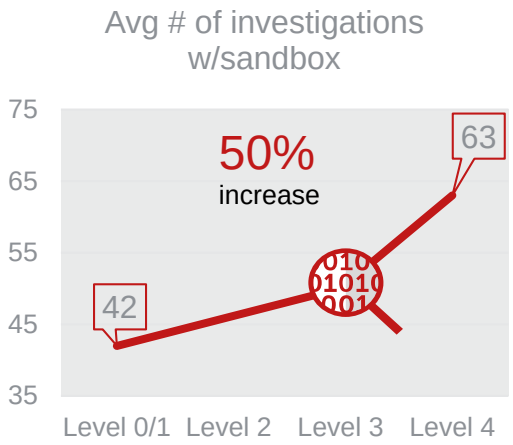
- 68% say they will improve through better automation and threat hunting procedures
- More mature SOCs are 2X more likely to automate
- Maturity leads to a better, but still mixed, balance of ad hoc and organized processes – the right weapon for the job



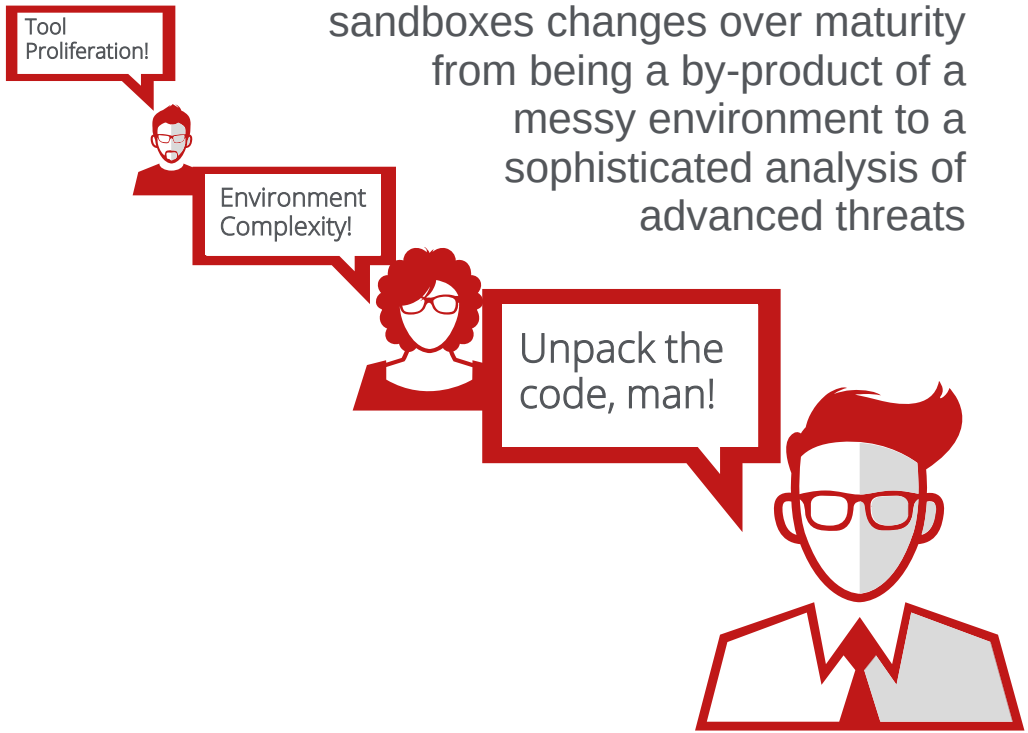
They use sandboxes to dig deeper

"The best is when you can do vulnerability testing and foreclose the threat before it happens. Sandboxing is useful here."

interviewed threat hunter, qualitative sessions, McAfee threat hunter survey, May 2017



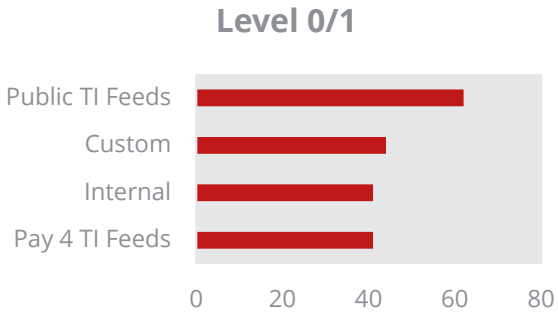
Reasons for using multiple sandboxes changes over maturity from being a by-product of a messy environment to a sophisticated analysis of advanced threats

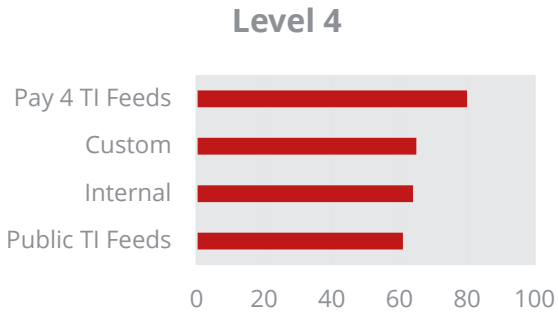


They curate threat intelligence feeds for purpose and buy to fill gaps

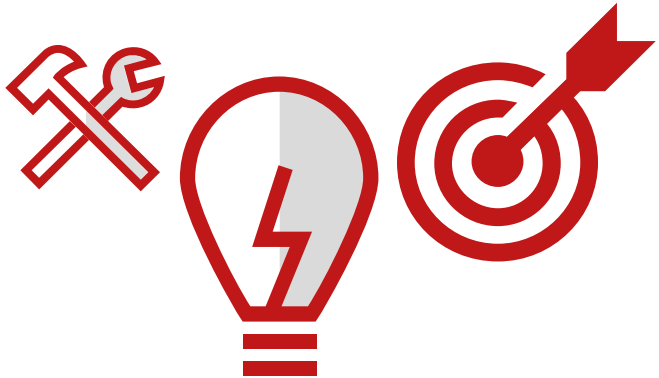
SOCs at levels 0/1 rely on public threat intelligence feeds **50%** more than any other type of threat feed

In comparison, SOCs at level 4 are **2x** more likely to pay for specialist threat intelligence and nearly **50%** more likely to use custom feeds.

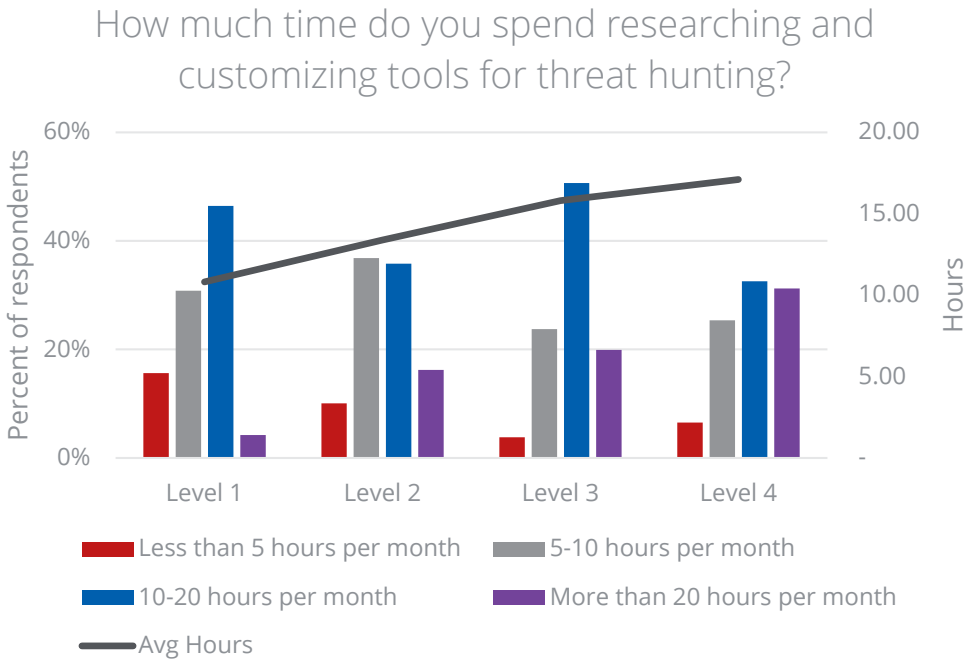




They do more customization



Mature SOCs spend **70%** more time on customization, using scripts and open source more heavily



Good hunting is hard work that pays real results

Mature threat hunting organizations sustain the good habits of:

- Identifying which processes can be automated
- Use the tools at hand to dig deeper
- Curate intelligence for purpose
- Customize and tinker for richer insights


McAfee™
Together is power.