McAfee
Together is power.

Secrets of Successful Threat Hunters

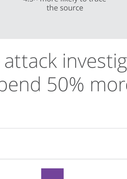
Advanced threat hunting teams excel at...

37%

Investigating Efficiently

37% close in <24 hours

4.5×



Finding Root Causes

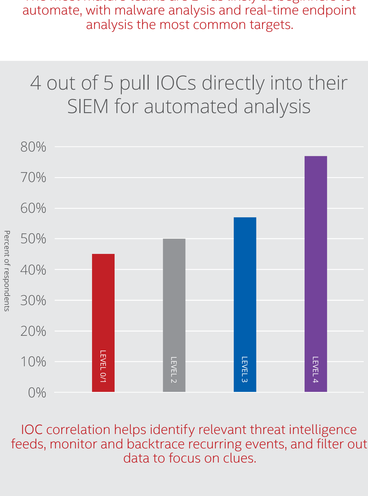
4.5× more likely to trace the source

45%

Improving Workflows

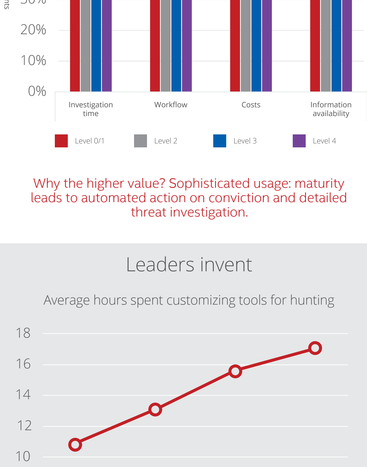
45% more value from sandbox use

75% automate attack investigation—so their experts can spend 50% more time hunting



The most mature teams are 2× as likely as beginners to automate, with malware analysis and real-time endpoint analysis the most common targets.

4 out of 5 pull IOCs directly into their SIEM for automated analysis



IOC correlation helps identify relevant threat intelligence feeds, monitor and backtrace recurring events, and filter out data to focus on clues.

Smart SOCs use sandboxes to cut costs, time, effort, and blind spots

Major improvements due to using sandbox to support investigations?

Why the higher value? Sophisticated usage: maturity leads to automated action on conviction and detailed threat investigation.

Leaders invent

Average hours spent customizing tools for hunting

Mature SOCs gain an edge by investing 70% more time creating processes and tools, relying on scripts and open source.

This is the right time to follow the leaders. Learn their metrics, strategies, and tactics in this report.

Disrupting the Disruptors, Art or Science?

Visit www.mcafee.com/soc-evolution for the full report.

McAfee
Together is power.

MGA_0717_info-disrupting-disruptors-art-science_FWR