Disrupting the Disruptors, Art or Science?

Learn More

To read the full report, please visit **mcafee.com/soc-evolution**

Executive Summary

Security professionals are in a fight every day to track down criminals who would disrupt their organization. Attackers nearly always have the element of surprise in their favor, but threat hunting can throw the attackers off their footing.

McAfee surveyed more than 700 IT and security professionals from commercial (1,000 to 5,000 employees) and enterprise (more than 5,000 employees) organizations around the world to identify insights and lessons for organizations looking to understand and enhance their threat hunting capabilities.

One of the key questions was the level of maturity of the organization's threat hunting activity. Ranging from Level 0 (Minimal) to Level 4 (Leading), these self-reported assessments provide useful insight into the current nature of the threat hunt and reveal some surprises about how organizations are investing for future improvement.

Key Findings

- The most mature threat hunting organizations are twice as likely to automate parts of the investigation process, spend 50% more of their time actually hunting, and as a result 70% of them are closing investigations in less than a week or less, compared to only 50% of the less-mature organizations.
- Mature organizations are three times more likely to consider every level of the identification and investigation processes as viable for automation, especially sandboxing, endpoint detection and response, and user behavior analysis.
- Tool emphasis changes with experience. Sandboxing was the number one tool for Tier 1 and 2 analysts of all sizes and maturity levels, but Tier 3 and 4 analysts use sandboxing as part of a broader mix of tools.
- Immature companies are trying to use the same tools as the most mature companies, but without the same results. Adopting new tools without changing the processes for hunting and incident response is rarely successful, as success requires an upfront investment in architecture and optimized processes.
- Customization and optimization are critical. Threat hunters in mature SOCs spend 70% more time on customization of tools and techniques. Custom scripts and Security Information and Event Management (SIEM) are heavily used to automate manual and ad hoc processes.
- Use of threat intelligence significantly affects results. More mature organizations use IOCs to validate and enhance decision-making at all levels of the security stack. Best practices include development of tactics, techniques, and procedures (TTP), observational skills, and curation of threat intelligence sources.

Observe, Orient, Decide, and Act

Human decision-making can be the critical advantage in many security scenarios, tilting the playing field in your favor. U.S. Air Force Colonel John Boyd first documented the four fundamental parts of this process, which are Observe, Orient, Decide, and Act. Effective security operations teams are leveraging this process to exploit their adversaries' weaknesses, supported by automated processes, machine-driven analytics, and curated threat intelligence. Threat hunters often begin with the assumption of a breach or compromise, following clues and personal intuition, and later turning successful hunts into automated rules. Hunting is a human-centric activity, using a wide range of tools and information to seek out hidden threats to the organization.

Based on the survey results, threat hunting begins as an ad hoc process in the least-mature organizations, then swings strongly towards process development before eventually finding an appropriate balance between process and ad hoc in the most mature hunters. Immature organizations tend to aggressively give their hunters sophisticated tools and data, with limited success. As they mature, hunters refine their processes and hunting techniques, adding automation and analytics to help manage the vast amounts of security data. By Level 4, hunters have significantly increased their effectiveness as they selectively use tools and data appropriate to their environment and likely attack vectors.

Humans working on their own simply do not have the capacity to deal with the volume of security data. Managing that data and leveraging it for threat validation are the top two challenges for most organizations. Less-mature organizations struggle with getting access to data and prioritizing events, while the most mature consider threat validation to be the biggest challenge. It is no surprise that Level 1 and Level 2 organizations, still hunting mostly part-time, ranked hiring additional experienced people as their top priority. In the more mature organizations, better automation becomes the number 1 priority and increased analytics number 2, as organizations shift their focus from building strong hunting and incident response teams to making them more effective.

Observe, orient, decide, act cycle

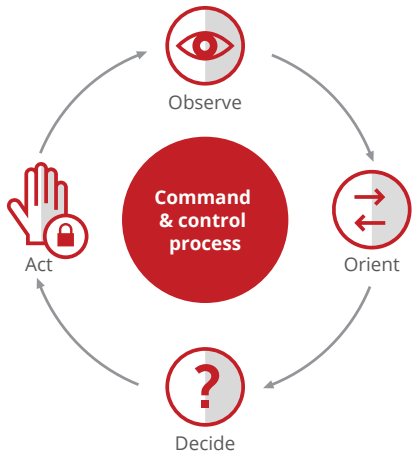

Figure 1: Observe, orient, decide, act cycle.

Conclusions

As organizations move up the maturity curve, they document the repeatable steps in the attack investigation process, which provides the foundation for further automation. At Level 1, only 40% of processes are automated, compared with more than 70% by Level 4. This embrace of automation, combined with effective and skilled identification of patterns of anomalous behavior, results in a synergy between hunting and incident response that delivers faster triage, shorter case closure times, and a much higher percentage of root-cause determination. Our survey showed that more than 70% of mature SOCs closed cases in less than 7 days, compared to 25 days for the least mature ones, and determined root cause 70% of the time, compared to just 43%.

71%

Of SOCs with a level 4 maturity closed incident investigations in less than a week

Threat hunters are using a wide range of tools and techniques to find, contain, and remediate cyberattacks. As they mature in the role, their effectiveness increases as they are augmented by human+machine teaming, combining human judgment and intuition with machine speed and pattern recognition.

For less mature organizations, simply copying the tools and techniques of the leading hunters is not sufficient. Adding new tools without changing anything else is unlikely to produce positive results. Sandboxing, automation, and analytics can empower these less-experienced hunters, but organizations that have not invested in architecture and defined processes that support that automation will experience diminished results.

"This researches highlights an important point: mature organizations think in terms of building capabilities to achieve an outcome and then think of the right technologies and processes to get there. Less mature operations think about acquiring technologies and then the outcome."

Mo Cashman, Enterprise Architect and Principal Engineer, McAfee

Threat hunting is here to stay, and is no longer an esoteric practice limited to a few of the edgier practitioners. Over the next few years, expect to see threat hunting as part of most organizations' analytics-driven security operations, backed by extensive automation and machine analytics.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. www.mcafee.com

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com