Disrupting the Disruptors, Art or Science?

United Kingdom

Security professionals in the United Kingdom (U.K.) need to increase the resources allocated to threat hunting in order to win more battles against criminals trying to disrupt their organisations. Attackers nearly always have the element of surprise in their favour, but proactive threat hunting can throw the attackers off their footing.

Learn More

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

Connect With Us

EXECUTIVE SUMMARY

Whilst U.K. firms have the necessary tools available, phishing attacks are still the leading root cause, and they are getting below average results in elapsed time from threat discovery to investigation closure. The biggest challenges appear to be a mix of not enough full-time threat hunters, underutilisation of automation, and challenges dealing with the vast amounts of security data being generated.

This analysis of U.K. security operations was extracted from McAfee's 2017 Disrupting the Disruptors, Art or Science? Report. Research participants were IT and security professionals from commercial (1,000 to 5,000 employees) and enterprise (more than 5,000 employees) organisations around the world.

One of the key questions was the level of maturity of the organisation'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 lessons for organisations looking to understand and enhance their threat hunting capabilities.

Key Findings

- On average, threat hunters in the U.K. are operating at Level 2 or Level 3 maturity, or about average. Characteristics of this stage are a shift from process-oriented hunting towards a balance of ad hoc and process, increased emphasis on automating tasks, and more time spent researching and customising tools. However, the vast majority (94%) think that they are as effective as those working at Level 4.
- The most mature threat hunting organisations have automated 68% of their attack investigation process, compared to just 42% of U.K. firms. They are also 20% more likely to have full-time hunters on staff, and as a result are determining root cause 74% of the time, compared to an average of 58% in U.K. organisations.
- Mature threat hunters use a broad mix of tools to achieve their objectives. U.K. firms are progressing towards this practice, but are underutilising important options such as analytics, artificial intelligence, private or public threat feeds, and big data tools like Hadoop.
- U.K. firms have the tools, but not the people. They reported on average that 7 people in the organisation are involved in threat hunting, matching the overall average of 7 but below the 9 threat hunters working at Level 4 organisations.
- On average, 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. U.K. firms reported an over-reliance on user behaviour analytics by Tier 1 analysts, and above average experimentation with custom scripts by Tier 2. However, their Tier 3 and 4 analysts reported below average usage of almost all hunting tools, especially deception technologies by Tier 3s and EDR by Tier 4s.

- Customisation and optimisation are critical. Threat hunters in mature SOCs spend almost 25% more time customising their 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 organisations 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 favour. 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.

Based on the survey results, threat hunters in U.K. firms are generally operating between Level 2 and Level 3 maturity. During this stage, the focus shifts from hunting as an ad hoc activity to one that is heavily process-oriented, before eventually finding an appropriate balance between process and ad hoc in the most mature hunters. U.K. firms are leaving the purely ad hoc behind, as only 14% reported that they mainly hunt that way. As they mature, hunters refine their processes and hunting techniques, adding automation and analytics to help manage the vast amounts of security data. U.K. firms reported average levels of automation across all processes, although the percentage of the process that is automated is well below average, at 42% compared to a global average of 55%.

However, they report that they are not often using the broad set of tools that they have, and are struggling with the vast amounts of data generated. Surprisingly, they were also the lowest users of threat feeds, almost 20% below the global average.

Observe, orient, decide, act cycle

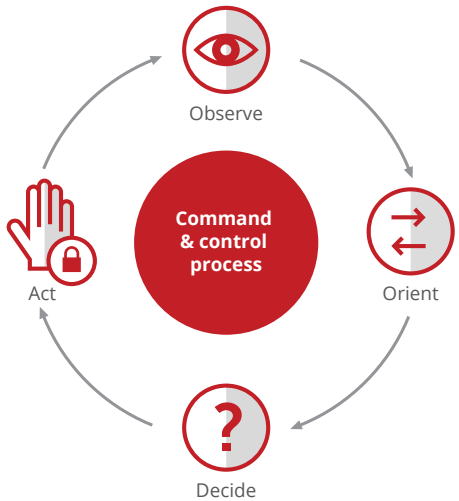

Figure 1: Observe, orient, decide, act cycle.

Level 2 organisations, still hunting mostly part-time, ranked hiring additional experienced people as their top priority. It was notable that U.K. firms ranked more precise diagnostic tools as their primary goal, followed by increased use of data analytics and better employee training. Employee training is especially critical as phishing was the leading cause of identified threats for this group.

Conclusions

As organisations move up the maturity curve, they document the repeatable steps in the attack investigation process, which provides the foundation for further automation. At Level 2, less than 45% 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 behaviour, 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 3 weeks for U.K. organisations, and determined root cause over 70% of the time, compared to 58%. This is a typical scenario in Level 2 organisations, as they discover that adding new tools without changing anything else is unlikely to produce positive results.

"This researches highlights an important point: mature organisations 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

Sandboxing, automation, and analytics can empower these less-experienced hunters, but organisations that have not invested in architecture and defined processes that support that automation will experience diminished results. 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.

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 organisations' 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

McAfee™
Together is power.

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

3885_0418
MAY 2018