EXECUTIVE SUMMARY

Together is power.

Disrupting the Disruptors, Art or Science?

Financial Services

REPORT

Together is power.

Disrupting the Disruptors, Art or Science?

Understanding the role of threat hunters and continuing evolution of the SOC in cybersecurity

Learn More

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

Security professionals in financial services firms are in a fight every day to track down attacks that are trying to disrupt or steal from their organization. Attackers nearly always have the element of surprise in their favor, but threat hunting can throw the attackers off their footing. While financial services firms have the necessary tools available, they do not appear to be getting optimal results, due to a mix of not enough full-time threat hunters, underutilization of the tools, and too much focus on process over human intuition.

This analysis of financial services threat hunting was extracted from McAfee 2017 Threat Hunting research, *Disrupting the Disruptors: Art or Science?* Research participants were IT and security professionals from commercial (1,000 to 5,000 employees) and enterprise (more than 5,000 employees) organizations around the world.

Connect With Us

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 lessons for organizations looking to understand and enhance their threat hunting capabilities.

Key Findings

- On average, threat hunters at financial services firms are operating at Level 2 maturity, or slightly below average. Characteristics of this stage are an over-emphasis on process, lower usage of important hunting tools, and challenges dealing with the vast amounts of security data being generated.
- The most mature threat hunting organizations are twice as likely to automate parts of the investigation process as financial services firms; are 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 financial services.
- Mature threat hunters use a broad mix of tools to achieve their objectives. Financial services firms use a subset of the tools they have available, underutilizing sandboxes, deception tools, custom scripts, and user behavior analysis.
- Financial services firms have the tools, but not the people. They reported on average that six people in the organization are involved in threat hunting, just under the overall average of seven and well below the nine threat hunters working at Level 4 organizations.
- 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. Financial services firms reported an over-reliance on endpoint detection and response (EDR) 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 sandboxing by Tier 3s and EDR by Tier 4s.
- Customization and optimization are critical. Threat hunters in mature security operations centers (SOCs) spend 30% 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 indicators of compromise (IoCs) to validate and enhance decision-making at all levels of the security stack. Best practices include development of tactics, techniques, and procedures (TTPs), 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. US 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 financial services firms are generally operating at Level 2 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. As they mature, hunters refine their processes and hunting techniques, adding automation and analytics to help manage the vast amounts of security data. Financial services firms tend to have an above-average level of automation in most areas, remediation being the primary exception. 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 big data management tool Hadoop—more than 25% below average.

Observe, orient, decide, act cycle

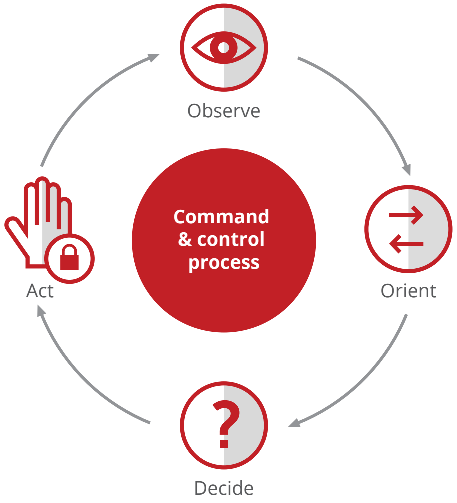

Figure 1: Observe, orient, decide, act cycle.

Level 2 organizations, still hunting mostly part-time, ranked hiring additional experienced people as their top priority. It was notable that financial services firms ranked greater integration of threat hunting capabilities with the SOC as their primary goal, followed by better automation and better employee training. Employee training is especially critical, as phishing was the leading cause of identified threats for this group.

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 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 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 seven days, compared to three weeks for Level 2 organizations, and determined root cause over 70% of the time, compared to 58% in financial services.

Threat hunters have a wide range of tools and techniques to find, contain, and remediate cyberattacks, but in financial services they are underusing them. This is a typical scenario in Level 2 organizations, as they discover that adding new tools without changing anything else is unlikely to produce positive results.

"This research 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

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. 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 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

McAfee™
Together is power.

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

McAfee and the McAfee logo, are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the US and other countries.
Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee LLC

3741_0118
JANUARY 2018