McAfee
Together is power.

Disrupting the Disruptors, Art or Science?

Manufacturing

Learn More

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

Security professionals in manufacturing firms face a significant challenge defending their organizations from threats across a wide attack surface of connected machines. Attackers nearly always have the element of surprise in their favor, but threat hunting can throw the attackers off their footing. Manufacturing firms have the necessary tools available, but are getting below average results in root cause analysis and elapsed time from threat discovery to investigation closure. The biggest challenges appear to be people related, as they had the lowest number of people hunting and ranked training threat hunters as their number one issue.

Connect With Us

EXECUTIVE SUMMARY

This analysis of manufacturing 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.

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 manufacturers 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 customizing tools.
- The most mature threat hunting organizations are twice as likely to automate parts of the investigation process as manufacturing 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 just 52% in manufacturing.
- Mature threat hunters use a broad mix of tools to achieve their objectives. Manufacturing firms are progressing toward this practice, underutilizing a couple of options such as open source tools and advanced analytics, and perhaps relying too heavily on big data tools like Hadoop.
- Manufacturing 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. Manufacturing firms reported below average usage of security information and event management (SIEM) and endpoint detection and response (EDR) by Tier 1 analysts and below average usage of sandboxes and user behavior analysis by Tier 4 analysts.
- Customization and optimization are critical. Threat hunters in mature security operations centers (SOCs) spend 20% more time on customization of tools and techniques than those in manufacturing firms. Custom scripts and 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 manufacturing firms are generally operating at Level 2 or Level 3 maturity. During these stages, 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. Manufacturing firms tend to have an average level of automation in most areas, but

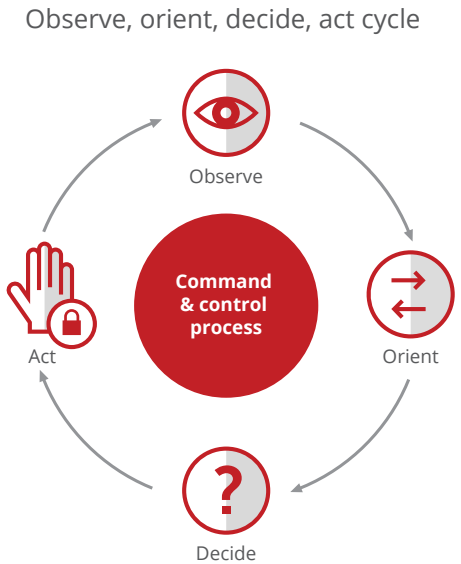

Figure 1: Observe, orient, decide, act cycle.

are below average automating remediation tasks. They reported that they are struggling with training threat hunters, followed closely by threat validation and dealing with the volume of IoCs. It was notable that lack of operating system (OS) patches was a significantly above-average root cause of attacks—53% versus just 39% for the overall group.

Level 2 and 3 organizations, shifting from part-time to full-time hunting, ranked hiring additional experienced people as their top priority. Manufacturing firms ranked more precise diagnostic tools as their top priority, followed by hiring of additional people and better automation.

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 15 days for the average manufacturing firm. The mature group also determined root cause more than 70% of the time, compared to 52% in manufacturing.

Threat hunters have a wide range of tools and techniques to find, contain, and remediate cyberattacks, and in manufacturing firms they are growing into full usage. 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

3742_0118
JANUARY 2018