IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

How Effective is Threat Hunting for Organizations? Learnings from the SANS 2020 Threat Hunting Survey

Anthony Perridge

Anthony Perridge
Vice President, International
ThreatQuotient

Biography

Anthony Perridge is Vice President, International for ThreatQuotient (https://www.threatq.com) where he leads all aspects of international sales, business development and marketing. Anthony leverages significant experience for sales growth and new business development – accelerated through the implementation of strategic partner programs. Anthony is strategically focused on customer success, building long term customer and partner relationships and loyalty.

Prior to joining ThreatQuotient, Anthony served as Sales Director for Cisco Security following its acquisition of Sourcefire, Inc. At Sourcefire, Anthony served as the EMEA Sales and Channel Director and previously held senior leadership roles at AirDefense and McAfee.

Keywords Compliance, Cyber defence, Security, Threat hunting, Regulations, Cyber attacks, Data breaches
Paper type Research

Abstract

Threat hunting is the art of finding the unknown in your environment, going beyond traditional detection technologies with active cyber defence activity. However, as the author of this article explains, threat hunting is now being utilized to tick the compliance box. ThreatQuoteint recently sponsored the SANS 2020 Threat Hunting Survey, to see if this would shed more light on how organizations are using threat hunting and how valuable it is proving to be.

The survey revealed that although Security professionals state that threat hunting has strengthened their company's defences – with 88% of respondents saying they are using it as part of their cybersecurity strategy and that it was proving effective with 86% saying it had strengthened their company's defences – over half of the respondents said that they see no value in hunting for new or unknown threats.

Introduction

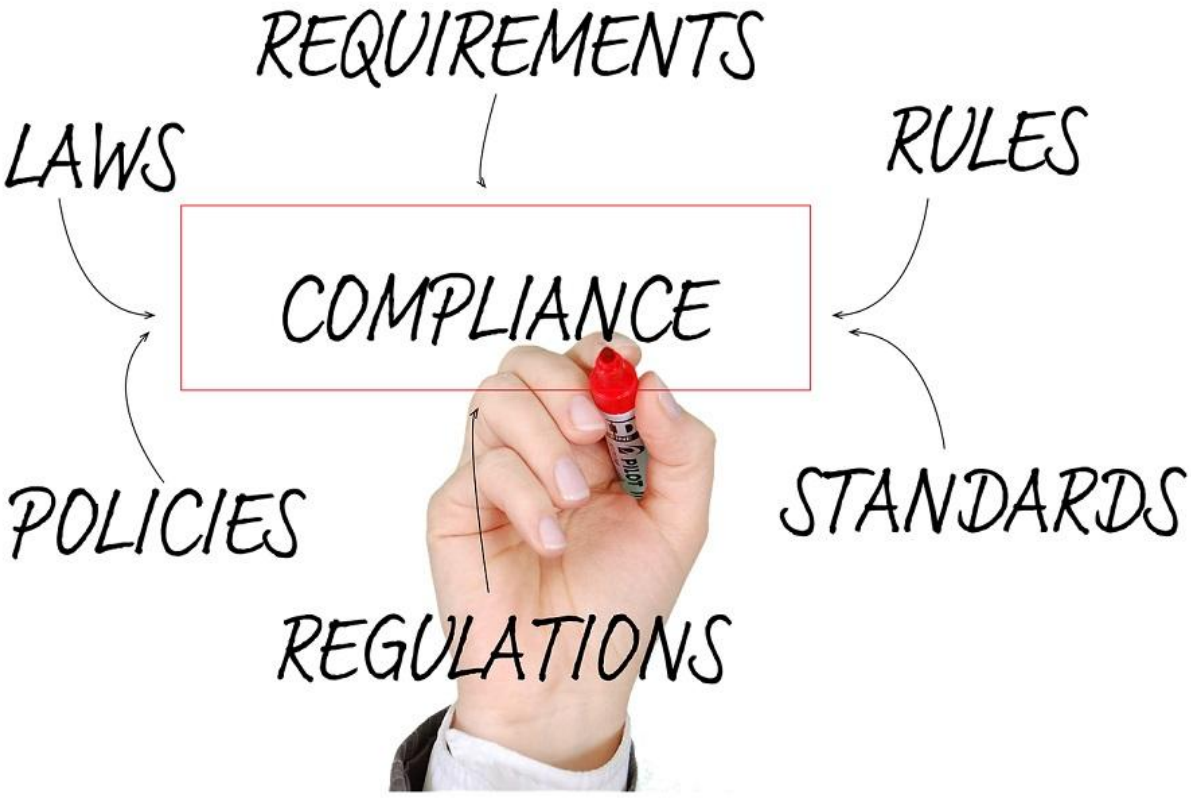
In recent years threat hunting has become much more widely adopted, but today the definition of threat hunting is still quite a controversial topic. Threat hunting is the art of finding the unknown in your environment, going beyond traditional detection technologies, with active cyber defence activity, proactively and iteratively


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

searching through networks to detect and isolate advanced threats that evade existing security solutions.

An essential part of security operations centre (SOC) services, threat hunting should be incorporated at an early stage. However, even though organizations have been threat hunting for a number of years now, with the job of 'threat hunter' being defined about five or six years ago, adoption and use is still quite a hotly debated topic. This is one of the reasons why we recently sponsored the SANS 2020 Threat Hunting Survey[1], to see if this would shed more light on how organizations are using threat hunting and how valuable it is proving to be.



Threat hunting is being utilized to tick the compliance box

Whenever introducing new threat hunting strategies to find malicious activities, there are various methods that organizations can utilize. The SANS survey found that some companies define how their threat hunting operations need to work and build up teams to meet these goals.

Unfortunately, the other still-quite-common approach is to run threat hunting operations with what organizations already have. Instead of defining goals that threat hunting needs to deliver the maximum value to the organization, they define threat hunting as simply having some form of threat hunting in the business, classifying it as an activity for existing teams to adopt.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

While this approach might still render results, these will not be as beneficial to the organization and its security posture as they could be. SANS frequently sees this approach at compliance-driven IT organizations whereby some standards require them to have threat hunting in place, which prompts them to set up a form of threat hunting simply to tick that box.

Security professionals state that threat hunting has strengthened their company's defences

Interestingly, in the recent VMware Carbon Black 2020 Global Threat Report[2] which interviewed over 3,000 IT leaders from 13 different countries, it found that threat hunting teams were starting to formalize their processes and procedures, and that trends were moving in the right direction for the industry overall.

In the report, 80% of respondents stated that attacks had become more sophisticated, however respondents also said unequivocally that threat hunting was paying dividends and increasingly being recognized for its value in identifying malicious actors already in the system.

When asked "In the last 12 months did your company's threat hunting achieve a goal of strengthening its defences against cyberattack and did the threat hunting find malicious cyberattack activity you would not have ordinarily found?" 88% of respondents said they are using it as part of their cybersecurity strategy and that it was proving effective with 86% saying it had strengthened their company's defences.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The difference between threat hunters and incident responders

However, the SANs report found that many organizations were tagging threat hunting activities onto the incident responder's role. Undoubtedly there are commonalities and differences between threat hunting and incident response. While threat hunting comes in various shapes and forms, the most sophisticated way of threat hunting is hypothesis-based hunting. In this case, the hunter envisions an attack scenario that might have happened in the organization. That scenario leads to a hypothesis that subsequently must be tested. Testing that hypothesis usually requires intimate knowledge about the suspected attack path as well as the right toolset and visibility to either accept or reject the hypothesis.

Incident responders usually know that an attack occurred, then start their investigation with limited knowledge about the attack path. This results in incident responders extending their knowledge about the attack and establishing visibility to investigate further. The tools and techniques for this overlap broadly between incident response and threat hunting. For that reason, it tends to be beneficial to use incident responders when building up threat hunting operations. However, over time the incident response-led approach should transform into a dedicated threat hunting team.

A lack of automation and frequently switching applications all impact the hunt

The report also found that there does appears to be a significant gap in the use of automated tools to aid in the curation of useful and applicable threat intelligence. In addition, most threat hunters are not full-time threat hunters but split their time with

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

other responsibilities. The trend to staff threat hunting operations with incident responders and SOC analysts was also very prominent. While incident responders may be very familiar with the task of finding new, unknown threats, SOC analysts might have difficulties deviating from their routine of analyzing alerts to actively searching for signs of a breach.

The report found that what threat hunters struggle most with are frequent context switches, as only a few respondents said that they never need to switch tools while doing their job. So, jumping between applications is one area that has a huge potential for improvement and increased efficiency. What also factors into efficiency is that a high proportion of respondents (36.3%) are manually applying the threat intelligence they have collected. One of the reasons appears to be that almost half of the respondents don't store threat intelligence in a platform but rather they are using traditional file-based methods such as spreadsheets or PDFs.

Finding a common understanding of threat hunting

I found it surprising that half of the respondents said that they see no value in hunting for new or unknown threats because uncovering unknown threats is one of the main arguments for threat hunting, while daily threats can be met by a SOC.

In summary

Moving forward, we need to establish a common understanding of threat hunting, improve tools that reduce context switches, automate the process and make threat hunting more measurable. Low-hanging fruit for many respondents would be to switch their intelligence management from document-based to an open-source or commercial platform to make threat intelligence easier to consume, evolve and apply.

Threat hunting is becoming more pervasive in the industry, but its general value is still not widely understood, nor is there a gold standard for threat hunting today.

Reference

[1] https://www.sans.org/webcasts/2020-threat-hunting-survey-results-114555
[2] https://www.carbonblack.com/resources/global-threat-report-extended-enterprise-under-attack/