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**

In Conversation

In Conversation with Leon Ward

Carol Baker

Research by ThreatQuotient shows that whilst there are signs that cybersecurity automation adoption is advancing, 98% of those surveyed say they have experienced problems during implementation. We asked Leon Ward, Vice President of Product Management at ThreatQuotient, for his views on why cybersecurity automation is so challenging for many organizations.

***Leon Ward** is the Vice President of Product Management at ThreatQuotient (https://www.threatq.com/) and leverages his 15+ years of experience in information and network security to lead product aspects of ThreatQuotient's innovative threat intelligence platform, ThreatQ. In this role, Leon drives the ThreatQ product roadmap aimed at improving the efficiency of analysts, security teams, and threat operations.*

Prior to ThreatQuotient, Leon was Cisco's Group Product Manager of Security Innovation, contributing to a number of exciting product launches that were aimed at changing the infosecurity world.

Leon was previously a Director of Product Management at Sourcefire, where he managed the detection capabilities in the company's line of network products (SNORT).

Tell our readers a little about yourself.

I'm the Vice President of Product Management, rather than 'Product Marketing'. People often confuse the two, but the biggest difference is that my role is defining the product definition for ThreatQuotient – that is the products and services we sell, their roadmap, and then aligning the creation of our products to the businesses of our customers, rather than positioning and selling a product. We put our customers at the centre of everything we do.

I've been involved in cybersecurity since the early 2000s – it's pretty much the only thing that I've ever really done. I fell into the world of product management because I enjoyed making something rather than chasing down incidents or selling technology. I have a real passion about building things, and that has led to work in product management.

At ThreatQuotient, we describe our ThreatQ product as a 'security operations platform'. Normally, when I speak to industry analysts or people who aren't really close to what we do, they ask the question, "Well, what is a security operations platform? Is it merely a threat intelligence platform, or is it an incident response platform? Where does it fit in?"


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**

We call it a security operations platform because ThreatQuotient has a leg in two or three different markets. First, we are known in the threat intelligence management market as it helps organizations to understand the risks they are facing, and secondly, we are involved in the security operations world because a lot of things impact on security in organizations. Gartner defined the term 'security, orchestration, automation and response' – it's a term that describes us very well and has led to the development of our product ThreatQ, and our first automation product TDR Orchestrator.

The third market we are involved with is the XDR extended detection and response market. This is an evolving market where sophisticated organizations are investing in best of breed tools, such as ThreatQuotient technology, and making sure all those tools work together to provide a single source of truth. This allows organizations to truly understand the impact on the organization and its users and allows them to prioritize the most important things. This could be risk, vulnerability or threat, an adversary campaign, or an incident that's taking place. With knowledge of the threat environment out there, you can put things into context, and understand what it means for the organization.

Can you tell us more about ThreatQuotient's research findings?

In 2021, we did our first research in the UK market. This year, we have expanded that research to include North America plus Australia. One of our goals was to understand more about how cybersecurity automation was taking hold, how organizations were using cybersecurity automation, and whether they were struggling with its adoption.

We targeted senior job titles in information risk, security operations, and C-suite, and divided the research into different verticals. The results were very interesting and are getting more interesting as trends change. Significantly, budgets for cybersecurity automation are increasing. The driving force behind this is that the role of the analyst or practitioner in security operations is really, really hard. Security teams are under constant pressure to do more. But the thing they can't control is how many tickets there are in their work queue; how many events are happening; or how much bad stuff is going out on the internet, especially with this changing geopolitical situation that we find ourselves in at the moment. This constant pressure, together with the lack of availability of skills in the cybersecurity workforce, continues to cause a major pain for organizations.

Another interesting statistic that came out of the research is that, when it comes to cybersecurity automation, 98% of those surveyed say that they have experienced problems during implementation. So, whilst it's great to get increasing budget, when these projects are rolled out, it is almost guaranteed that the organization is going to be faced with challenges in deploying automation technology.

Let's think about why those problems exist. What types of problems they are, and how is that linking back to the soft skills gap? One of the most common problems facing organizations is founded in trusting the outcome of that automation. Our research found that organizations were having a trust issue.


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**

Last year's research showed that 41% of respondents stated that trust was an issue. This year, it is only 12%. We believe this is because organizations are beginning to change their perception of what automation can, and cannot, achieve.

A lot of security automation tools and products have been born out of a strong legacy of automation technology, so why is this presenting a challenge for organizations?

This presents a challenge for organizations because once they commit to a bunch of code, a whole bunch of tests need to kick off to identify whether the things that worked yesterday, still work today. Is the thing that broke yesterday, and was fixed, still working today? For instance, you need to provide provision for a new user who needs to have access to certain parts of the system. The goal is to get them up and running as quickly as possible, but you may need to reset a password on ten different systems each with their own security, detection, and response, so when an analyst is handed a ticket event or incident, they don't necessarily know what the end goal needs to be.

For instance, there could be a ticket saying "here's a potential spear phishing message". Was the target the CEO, was it somebody in shipping? Is the attachment in it potentially malicious? Is that attachment related to an adversary group who are well known, or have been known to target your organization in the past?

When that ticket lands on the analyst's desk, he doesn't know what the outcome is going to be. To combat this, we've developed an approach that we call data-driven automation – and that's the approach that ThreatQ and TDR Orchestrator uses.

What's so different about data-driven automation?

First, with data driven automation, the data itself will tell you which actions need to be taken. For instance, the more you learn about that spear phishing email that has entered your organization's network, the more it will automatically trigger something. If it relates to an adversary that targets your geography, that can automatically trigger a series of actions. If we take that data driven approach, as long as you keep the single source of truth of what the threats, events and incidents are that you care about in your environments, and keep things up-to-date via automation – you can achieve very sophisticated outcomes, without the complicated development of super complex playbook processes that try to deal with all possible inputs, which happens simply because you don't know what the end result is when you start your investigation.

Can you tell us more about the new ThreatQ TDR Orchestrator?

Our new ThreatQ TDR Orchestrator is the industry's first solution for a simplified, data-driven approach to security operations. Built on the ThreatQ Platform, the latest version of TDR Orchestrator includes enhanced automation, analysis, and reporting capabilities to accelerate threat detection and response across disparate systems. This allows more efficient and effective operations that can be directly


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**

measured by timing savings and FTEs gained, improved risk management, and greater confidence when detecting and responding to an event.

In particular, the new version prioritizes automation on the most important events and alerts with context from threat intelligence and other internal and external sources. A feedback loop captures results to improve the automation flow over time.

Also, playbooks are easier to maintain as a result of Smart Collections, which are used to abstract automation logic. Atomic Automation allows for immediate action when a complex response is not needed; and Automation Packs for vulnerability prioritization, indicator enrichment, XDR, and more use cases help users get started with common use cases quickly.

As there is a no-code user interface, less training is required up front. This helps deliver a lower total cost of ownership over time and enables users to rely less on their organization's technical resources, which can be a bottleneck - especially when waiting for internal developers to work through their backlog and write the playbook automation requested.

Leveraging automation to do the heavy lifting and cut through the noise is vital to helping cybersecurity teams thrive under pressure. ThreatQuotient continues to innovate in a way that drives meaningful operational benefits to customers. Many process-based SOAR platforms are designed such that only security engineers and analysts have the skills necessary to use them directly; making these traditional platforms hard to implement and maintain, which drives higher costs over time.

The latest version of Threat TDR Orchestrator reinforces the need for no-code solutions that empower operators to adapt to dynamic threat landscapes faster, and focus their energy on security operations workflows that provide critical business context.

ThreatQ TDR Orchestrator has been a long time in the making. It takes the data-driven cybersecurity automation approach, and makes things easier, cheaper, and faster to automate without the complexity normally associated with playbooks.

There is so much demand for skilled staff that people who build playbooks frequently jump from one organization to another. You find that once they have built their version of a Frankenstein's monster of automation, they leave the organization and something changes, or something breaks because vendors change their APIs, and the system needs constant fixing. Even when a new person comes in to try and unpick and unpack the playbooks and processes, they find it very hard to understand.

How do we address that? Well, we simplify them the right at the start. Through data-driven automation you can build a large number of much more simplified, triggered actions to take place. This means that as soon as a threat, a vulnerability, a security event, whatever it may be, meets your defined characteristics of the stuff that you should be caring about happens, then a single action can be taken. By

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**

taking that action, perhaps it moves that incident to the next kind of state you're interested in. Previously, you may have only cared about, let's say spear-phish events related to a specific adversary, maybe an analyst identified them after doing some research associated with the adversary, but that analyst may not know that they need to trigger a whole response process. But the fact that associations have been made means the system can automatically trigger those actions. The result is a situation where your analysts need only to focus on the higher-value tasks that they have, whilst all your tools and systems automatically communicate and trigger the right responses.

So, what can we expect when it comes to cybersecurity automation in the future?

We are still in a world where a lot of security metrics are required, and we will see more security teams and vendors take a triage approach. At the moment, analysts are finding they have ticket queues of 100 deep to get through. The reality is teams cannot and will not address all of these, so triage becomes much more important.

This is the ability just to explicitly say, "I'm not going to do anything with this event, threat vulnerability", whatever it may be – not because teams are lazy, or because they are absent minded, or not diligent – it is because the economics of cybersecurity operations has shifted to a world of 'you'. 'You' have only got a finite number of resources, and you must choose where you apply them.

You can't magically ramp up your resources when there is a spike in events or threats because there is no one to bring in. Therefore, optimizing how you can triage security events, objects, whatever it may be, is going to be the future – and that's where ThreatQuotient is leading the race.