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 Mikkel Drucker and Christian Have

Carol Baker

As Logpoint embarks on the next phase of its journey to become a European cybersecurity powerhouse, we talk to the company's new CEO, Mikkel Drucker, and Christian Have, Logpoint's Chief Technology Officer about the cyber challenges which lie ahead.

Mikkel Drucker *is the new Chief Executive Officer (CEO) at Logpoint (https://www.logpoint.com). The nomination of Mikkel marks the next stage in Logpoint's journey to becoming a European cybersecurity powerhouse, providing regional access to outcome-driven security operations and compliance technologies.*

An international technology executive with a strong focus on commercial excellence and a proven track record of successfully scaling software as a service (SaaS) and scale-up companies and driving profitable growth, Mikkel spent three years as CEO at Netigate. He then sold the company to a Private Equity fund and drove its healthy growth performance, reshaping the product into an innovative technology platform organically and through acquisition.

As Chief Growth Officer at Tacton, Mikkel secured the company a Leader position in the Gartner® Magic Quadrant™ for Configure, Price and Quote Applications and spearheaded its growth. Mikkel also has entrepreneurial merits – he co-founded Lindrucker, leading it to a successful exit to a strategic buyer. In addition, Mikkel has held leadership positions at Atea, Trustpilot, and Nokia.

Christian Have *is the Chief Technology Officer (CTO) at Logpoint. Christian creates threat detection and incident response (TDIR) and compliance solutions for organizations and managed security service providers (MSSPs) in the mid-market. He brings many years of cybersecurity experience into play, building the products he would have loved to have as a practitioner.*

After graduating from the IT University of Copenhagen, Christian gained experience as a hospital Security Specialist and Head of Network Security for the Danish National Police before joining Logpoint more than ten years ago.

He is a regular guest lecturer on cybersecurity at some leading Danish universities, and he mentors startups venturing into the cybersecurity space with cutting-edge technology.

Mikkel, tell our readers a little about yourself and what attracted you to Logpoint.

I have over 25 years' experience in the IT technology software service industry and in growing businesses. For several years, I have worked internationally including

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**

spending five years in the EU and Asia, and then the rest of the time in Sweden and Denmark. It is a great privilege to join Logpoint as its new CEO.

What intrigues me about Logpoint is not only the business we are in, but also how our society is influenced by cyber threats and risks. The chance to join Logpoint, a company that cares so much about trying to make the world a safer place, really stood out for me.

Christian, tell our readers a little about yourself and the focus of your work.

As Chief Technology Officer (CTO) for over 12 years, I run Logpoint's technology department and specifically the organization's engineering research. Much of my focus is on threat research and how the use of cutting-edge research activities within artificial intelligence (AI) and machine learning (ML) can make it easier for midsize organizations to protect against advanced threats. A key focus for us is protecting these companies against AI and ML emerging threats and our proactive threat analysis means Logpoint is making a real-world difference to the sector.

Prior to Logpoint, I spent ten years working in IT security on behalf of the Danish National Police, as well as in sectors such as healthcare and manufacturing, where I undertook cybersecurity malware disassembly from small scale all the way up to large policy initiatives on security architecture.

Mikkel, tell our readers some of your plans for Logpoint.

Having been at the company for only a few weeks, it's a little too early to disclose a thorough plan – I'm still meeting a lot of our partners, customers and employees to understand our situation – but there's no doubt, there is huge opportunity.

Our current plan is to continue our excellent work with partners and customers which has seen us win copious awards. Traditionally, we have been working directly with our customers, and we have recently expanded our partnerships especially on the managed security service provider (MSSP) side. So, a big focus in both the short and longer term is to work even closer with our partners expanding our revenue generation further through the channel.

A second priority for us is to continue to grow our market share working with smart companies, and essentially that will revolve around mergers and acquisitions (M&A).

The cybersecurity landscape is a very dynamic market in which we see quite a few activities on the M&A side. I know that you have spoken to our investors some time ago (https://www.itceoscfos.com/jzerlang-melby), and readers will be aware that we are backed by a very well-funded Nordic private equity, so that is of course something that we as a company will be leveraging as we focus on acquisitions, but also in general on strategic alliances.

The third current priority is what everyone else in the world is very preoccupied with, which is talent. So as a company, we will be focusing on attracting, developing and


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**

retaining great talent in Logpoint. Working with talent is as big a part of our agenda as are the topics I mentioned before, and of course will be key to the success of the company.

What have you found to be some of the biggest challenges facing companies during scale up?

Mikkel – For me, the scale up phase comes right after the startup, and right before the grown-up stage. If you will, it can be likened to the teenage period in life where you develop quite a lot and you are very prone to new impressions and everything else. At this time, most companies will face the people and competencies issue. You're moving away from a startup organization and individuals who wear many hats and do many different things, to a period where you are specializing more and where you are to a large extent seeing individuals wear fewer hats as the business develops into a more grown up company. It's also the stage when a company will start layering on quite a few more processes which they hadn't previously required as a startup.

One of the challenges facing startups as they develop and move into the next stage is applying too many processes too fast because they feel it will make them more insightful as a result. But when startups do this it slows down decision-making, impacting innovation and speed to market. The key is to find the balance between establishing the right processes which are needed both now and over the next 12 months while still maintaining your ability and agility to execute and move forward with the market.

There is also something around infrastructure in general: first, how your infrastructure and IT systems are communicating internally; and secondly, is the infrastructure of your technology built for scale? This relates to my point around processes; but if you don't change some of those infrastructure elements fast enough, you won't be able to scale with the current market nor with the new markets which you are entering, or with the many new customers who suddenly need to reside on your platform.

Then the startup needs to deal with the changing culture. As you go through the various growing phases it's important to create a sense of belongingness for the individuals in the organization, especially when you have a lot of people coming and going as part of changing competencies. How do you establish trust, psychological safety and a sense of belongingness in the organization while doing that? It's a challenge that most companies face.

With Logpoint aiming to become a European cybersecurity powerhouse, what impact do you foresee on other players in the cybersecurity market? For example, will you be looking to acquire them?

Mikkel – For us becoming a European cybersecurity powerhouse will also revolve around strategic partnerships, M&A, and working much closer with our customers and partners. It is also about competition and competencies. The cybersecurity market is converging in so many ways. Some of the competitors we have today are


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**

not the same as those we had 12 months ago. So, we are very focused on evolving our product, our technology, and our offering to the market, as quickly as we can and preferably faster than the market – and one of the key components to do that is through acquisitions.

Christian – on a European scale, how is ransomware as a service fragmenting the threat landscape?

The answer to this varies depending on the size of the industry. For example, if a CIO or CSO of a midsize organization sees the company's peers are being breached by ransomware – we see it right here in Denmark where we have just had a hosting company that services the public sector and healthcare go bankrupt because it was unable to restore its backups after a ransomware attack – then as a CEO, CIO or CSO I will be concerned about what that means for the survival of my organization. I am also concerned about what it means for me because there is a liability at the personal level.

When we see ransomware fragmenting and the emergence of ransomware as a service evolving it becomes a problem because essentially much of the classic tech detection strategies are saying everything is OK but we know there are indicators that systems are being attacked and compromised.

Then we see a myriad of operators now existing in a much more distributed economy: there are initial access brokers (IABs) who gain access to these systems, and security researchers selling these really advanced exploit kits; and then you have people who are driving the extortion. All of these players are now fragmented into a disconnected economy instead of a centralized or decentralized economy – and that is worrying, especially when we look at it at the European level.

It is not just at company level, but in a geopolitical context as well where we are seeing an increase in hybrid warfare. It's an area where these ransomware operators are increasingly cooperating with nation state entities. We've seen those relationships built with units of the Russian intelligence, Iranian groups and so on, and we are beginning to see that asymmetric or hybrid pressure against Europe's defenses increasingly hitting the cyber scene and critical infrastructure supply chains, especially in logistics – so it is a big and increasing threat.

Picking up on a couple of points from our previous interview with Jesper when Summa had become an investment partner, can we expect to see Logpoint's messaging change around emerging technology and geographical political developments, and will Logpoint's technology need to change to deal with these?

Christian – When we look at the changes to technology, historically security has been in a bit of a privileged situation where you got excited about the new tools or had a strong relationship with your vendor. But attackers will find a way to circumnavigate your strong point solutions, and customers have gotten exhausted in the constant chase of the newest most advanced technology and are looking for ways to do more with their existing technology.


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**

I know when we go to trade shows we still see a lot of AI hype. AI has a place absolutely but what gets companies breached and what makes them not recover is the lack of basics and hygiene. So, customers are looking for ways to get a better understanding of their risk landscape, and better guidance when something happens and what to do about it. That's where we are seeing a change – there's a move away from hardcore security analytics only, towards putting it closer to some of those people who now have to operate these technologies. Typically SIEM was predominantly used in larger organizations but we're now seeing much more demand for its use to analyze the regulations and pressures experienced in the mid-market. We need to re-envision what that security solution is actually like for those new market buyers.

How do you explain your solutions to non-technical corporate leaders so that they have a greater understanding of the link between cybersecurity, risk and the impact on business performance?

Christian – The biggest sense of urgency when you think about cyber threats and cyber security is that the average cost of downtime for businesses for instance, not having its operations up and running is $300,000 per hour. This is in addition to the risk of the company not being able to serve its customers, partners, employees and the ecosystem.

We are seeing a shift from business-oriented CISOs to technical CISOs as the pendulum continues to swing one way or the other. For the last ten years we've seen a lot of business-oriented entities, now we are seeing the pendulum swinging back and there is a realization that it might be easier to teach a technical CISO how to talk to the board than it is for a business-oriented CISO to talk to the security analysts.

But at the end of the day, what makes it difficult for the board to gain an understanding and oversight is an inability to answer questions such as 'How well are we doing with our security?' 'What is the appropriate investment?' and 'Is the priority of investment versus risk a conversation that can be had at the board level?' This is where we see our solution helps. We have a way at the technical level to model what we see and what that means, and then we can use that to drive and benchmark companies against each other and ascertain whether we are behind or in front in terms of their security posture. It also looks not just at cause but at consequence, which helps drive a more data driven conversation at the board level as opposed to 'we blocked 500 phishing emails yesterday'. Without some context, no one knows if that's good or bad. It sounds scary, but no one has any idea how to connect that back to anything that is business driven or outcome related.

There have been many conversations among the security community about whether cloud forensics is just log analysis – it would be interesting for our readers to get your thoughts on this.

Christian – People need to realize that the exact same problems exists when you move your workloads to the cloud. You still own the responsibility even though someone else runs your infrastructure. We have an example of a large customer


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**

where they had a logical error in the HR system that meant every employee had administrator privileges, and it became a big problem in a GDPR context. Platforms may change through strategic changes but the problem is still the same, and what we are expected to do at the conceptual level is the same. I think in our eagerness to move to the cloud and transform our ways of working to a more cloud-oriented approach, we might – in the industry – collectively have forgotten that a lot of these basics are there for a reason. These guidelines are based on the mistakes and experiences of past generations and still have relevance despite the infrastructure changing.

What drives the passion in your work, and what gets you out of bed in the morning?

Mikkel – I touched on this at the start of this interview – I am humbled and grateful about working at Logpoint – there are so many passionate people who harbour a desire to use technology to help our society. Together we can help our customers become more secure and ultimately more successful. But probably more than anything else is that we can support the critical infrastructure in our society that provides electricity, running water, healthcare, banking on a daily basis – all the things which we are used to in a modern society for everyone that lives there. Ultimately, I think that is what gets me up in the morning.

Christian – That's a tough one to follow. But I think there is a lot of opportunity in improving what and how organizations are doing cybersecurity. The mid-market has just been underserved by a lot of other technology vendors and we can see the impact it has had on our customers. Every single day we go to work, every single feature we produce, every single threat research report that comes out moves the needle forward for these customers, and to me that is enormously rewarding.