TRIDENT SEARCH

CRISIS TO CONTROL

Sponsored by

W/TH® secure

CRISIS TO CONTROL

The Innovation Forum brings together leaders from across the cyber security industry to discuss the most pressing issues affecting our sector. It’s designed to be a space for open, honest conversation - encouraging accountability and collaboration to help drive meaningful progress.

In this forum, we were joined by executives and decision-makers from across the cyber landscape to explore the challenges around incident response (IR). With a discussion focused on how organizations can better prepare for and manage incidents as they unfold, the importance of having robust business processes in place and the role leaders can play in supporting the wider security community, this forum generated valuable insights and clear, actionable takeaways that can be applied directly within your business.

OUR EXPERTS

James Dyson, VP of Global Services, WithSecure
Laure Lydon, VP of Security, Flo Health
Craig Aitchison, CISO, Verian Group
Ben Trethowan, CISO, Brit Insurance
Stefan Treloar, Ex-Group CISO, IG Group
Lauren Wilson, Cyber Incident Manager, EDF
Tobias Puschmann, Group Cyber Security Incident Manager, Sky
Andrew Connor, Director of Product Security & GRC, PG Forsta
Jack Wright, Head of Cyber Incident Management, Allianz
Ross Baker, Head of Cyber Delivery, International Airlines Group
Simon Harris, Head of Global SecOps Centre, IAG GBS
Yoshi Hemzal, Security Operations Lead, Capital.com
Simon Goldsmith, Enterprise Security and Platforms Lead, OVO
Diana Moldovan, SecOps Manager, GoCardless
Diego Fuschini Camargo, Director of Detection and Response, WithSecure
Connor Shannon, Senior IR Investigator, WithSecure
Jyri Karppinen, Incident Response Manager, WithSecure
Waldemar Woch, Senior Incident Response Consultant, WithSecure
Charlee Ryman, COO, Trident Search
Lottie MacCallum, Head of Marketing and Operations, Trident Search

Our Sponsors

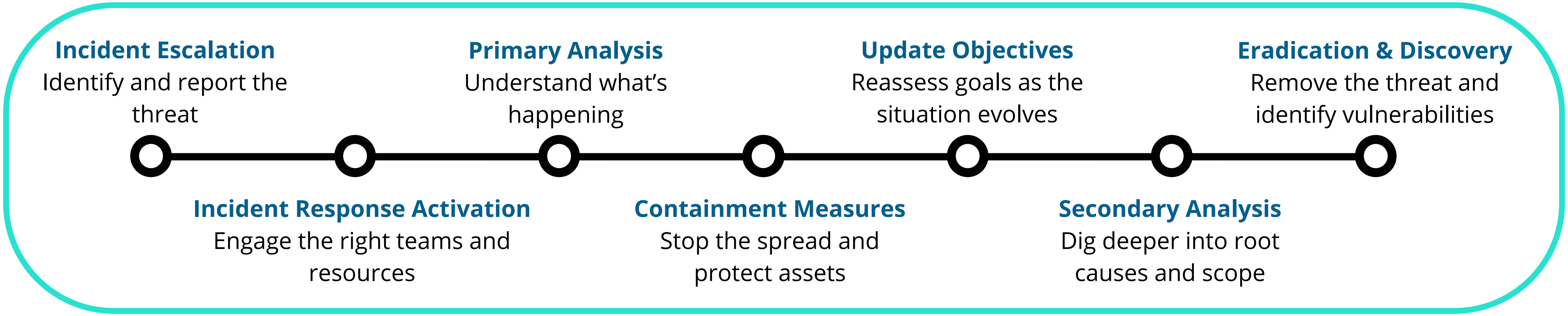
Thank you to all our guests who provided their insights into the issues raised during the evening, and to our sponsors WithSecure, the market leaders in incident response and cyber security solutions.

WITH®
secure

METHODOLOGY

When disaster strikes, the first few hours are critical. We all agree that identifying the attack and raising the alarm for your SOC team must happen immediately. But beyond that, alignment quickly breaks down. At our roundtable, it became clear that there’s no consistent standard for what good incident response looks like, and that inconsistency is dangerous. How and when you escalate, who you inform, and the actions you take vary dramatically depending on your business size, sector, maturity and risk appetite.

In a recent tabletop exercise delivered by WithSecure, we explored a data breach and extortion scenario involving a global charity. Participants from a range of sectors - healthcare, insurance, energy, finance and more - came together to walk through their responses. The key takeaway? There’s no one-size-fits-all approach. To support better preparedness, we broke down the high-level timeline of a typical IR process - bringing structure to chaos:



Incident Escalation
Identify and report the threat

Incident Response Activation
Engage the right teams and resources

Primary Analysis
Understand what’s happening

Containment Measures
Stop the spread and protect assets

Update Objectives
Reassess goals as the situation evolves

Secondary Analysis
Dig deeper into root causes and scope

Eradication & Discovery
Remove the threat and identify vulnerabilities

This timeline provides a critical anchor, but it’s not a silver bullet. What our roundtable exposed was a real and urgent problem: if leaders across the industry can’t align on how to approach a crisis, we risk confusion, delays and poor outcomes when it matters most. In the following pages, we’ll unpack the key decisions and dilemmas that emerged – shedding some light on the blind spots and unexpected challenges that could derail even the most well-prepared teams.

STAGE 1 - THE INITIAL RESPONSE

The bottom line? Have your plan in place, know your data, and don't get distracted by red herrings when time is everything

Have you prepared for the worst?

The moment you're made aware of a breach, your SOC team should be scrambling into action. We discussed how leaders need to have a clear process in place to use the data available – it's all too easy to jump to conclusions when you have limited intel to go off. As Andy put it, "preparation is just as important as response"; without that groundwork and foundation of preparedness you're constantly on the back foot.

Can you validate the data?

During our tabletop exercise, participants tackled a simulated data breach and extortion attack on a global charity. Early on, Stefan highlighted that before anything else you've got to validate and classify the data – you need to know what's been affected and how much of it is out there.

If it's data that causes legitimate harm, some would argue that the breach needs to be taken more seriously and resolved faster, compared to something that causes less tangible damage, like email leaks. Ross added clarity to this view, saying that you need to think about the impact on your stakeholders and how it will impact them financially, reputationally and personally, not just how it will affect your business.

There was also a discussion around verifying the legitimacy of the data being used to drive the response. "How do we fact-check our intelligence in the middle of an attack?" was a common question. Diego pointed out that in some cases, teams spent too long debating the credibility of compromised data when more urgent actions were needed, opening the room up to vulnerabilities.

> *"Preparation is just as important as the response itself. You're only ever as good as your training and without clear processes and policies in place, your team will be thrown into chaos when an incident hits."*
>
> **Andrew Connor, PG Forsta**

Do you understand your capabilities and limits?

Responders need immediate oversight: is the right severity level assigned? Are the necessary people and resources available? If you work with a third-party provider, do you know exactly when to bring them in? One useful approach discussed was for MSSP or MDR partners to be more transparent in their SOPs, e.g. clearly stating that if "X, Y or Z happens, you need to give us a call". Otherwise, small businesses or inexperienced teams (such as a junior colleague on-call during an incident) might waste contracted hours on lesser threats or, even worse, could let a situation get out of control before partners are brought in. This move ensures partners are used efficiently, building transparency, trust and credibility into the partnership.

Do you know your organizations' risk appetite?

If you don't know how much risk your executive team is willing to tolerate, you'll struggle to build an effective response strategy. Teams need to weigh the risk appetite of leadership against the potential impact on stakeholders, especially when sensitive or high-value data is involved, e.g. financial or medical information. Without this clarity, decision-making becomes slow, fragmented and misaligned.

KEY ACTIONS

Preparedness is key: The speed and effectiveness of your initial response relies on planning ahead. Regularly run response drills, assign clear roles and ensure your team knows how to act when the alarm sounds. Without this foundation, you'll always be reactive rather than proactive.

Build in flexibility: No two incidents are the same, and there isn't a set playbook for all attacks. In your preparation stages, build contingency plans for multiple different scenarios so your team know how and why to diverge from standard plans.

Learn from the industry: Insights from tabletop exercises and peer forums highlight blind spots that rarely appear in playbooks. Leaders should regularly review and adapt their processes based on lessons from real incidents and cross-industry collaboration.

Know when to bring in partners: Relying on an MSSP or MDR provider only works if you can establish clear, documented criteria for escalation. This avoids delays, prevents wasted resources and ensures external support is used efficiently and effectively.

STAGE 2 - PLAN OF ATTACK

When a breach hits, don’t just react - pause, assess, and build your plan with precision, because one wrong move can turn an incident into a crisis

Have you got a clear picture of how this happened?

Your first question should be: what kind of data sources and visibility do you have? If your tech stack gives you enough confidence, you may not need to push for aggressive containment right away. But when visibility is limited, it's easy to make assumptions too early. In our attack simulation, a major sticking point was what to do with the SOC team member who had introduced malware into IT systems:

- Craig raised the importance of determining whether you're dealing with an insider threat or a compromised account. If the source of the breach is identifiable, one option is to immediately block access, treating the individual as guilty until proven otherwise.
- However, Yoshi cautioned against moving too quickly, suggesting investigating behind the scenes, as the individual could have multiple accounts or a harmful motive.
- Others highlighted the need to bring HR into the loop early, but only to follow proper process - too much haste could open the business to liability.

The consensus was to dig into the information available and build a clear operational picture of the incident: what data could the individual access, where could it have been leaked from, and what technical permissions or controls are in place? Diego noted that many in the industry still believe ransomware can be handled purely by playbook, but in reality, things rarely go as planned. While some documentation is useful for pre- and post-encryption actions, flexibility and situational awareness are just as important in determining whether you're responding to human error, targeted malicious behaviour or a broader compromise.

How are you going to manage the story?

Ross made a critical point: “it’s all about managing the narrative.” One of the biggest challenges IR teams face is knowing when to escalate an incident - it all depends on the type of data involved, the potential risk to stakeholders and the credibility of the information available. Lauren argued that incidents should stay within the technical team until there’s full validation of what has happened. But Stefan countered that early comms preparation is essential. Indeed, in one case brought up during the forum, failure to prep the service desk led to widespread confusion and false information circulating, making the situation so much worse.

KEY ACTIONS

Establish a clear operational picture: Situational awareness is everything. Document the facts, validate your intelligence and don't assume intent without evidence. This clarity will shape your containment, investigation and communications strategies.

Tailor your response: Adapt your response based on the nature, scale and intent of the threat. Each scenario demands a different blend of technical, legal and communication strategies. Avoid a one-size-fits-all approach.

Plan layered comms: Every business will have a different escalation strategy, risk appetite and confidence in their blue team's capabilities. Layering your crisis comms is the best way to navigate this - escalate internally in phases, draft external holding statements and bring in business stakeholders when appropriate within your IR strategy.

Involve the business: Yoshi pointed out that in today's digital age, stories often break via employees sharing news on WhatsApp or social media. You can't monitor these unofficial channels, so having clear guidance for staff can help to keep control of the narrative.

Jack suggested a middle ground - keep the incident internal, but make sure key business stakeholders are aware early so they can begin forming contingency plans. Depending on your sector, there may also be additional requirements, for example Laure pointed out that legal counsel may need to be informed in healthcare settings, and Simon flagged the importance of considering when to notify regulators like the NCSC. While some feared "crying wolf" if you're updating these bodies with every potential incident, others felt early notification rarely caused harm and could support insurance or regulatory obligations later.

A key takeaway is that it's ok to pause – you aren't legally compelled to reveal all information immediately. For external comms, holding statements are your best friend: you don't need the full story straight away, but you do need a prepared, clear message. As Simon put it, transparency is often your strongest asset when dealing with the media and public - if you trust your stakeholders to back you, being open can help protect reputation, maintain trust and keep you compliant.

STAGE 3 - REMEDIATION CONCERNS

When the dust starts to settle, your next move matters most - remediation is a high-stakes balancing act where clarity, coordination and calm decision-making can make or break your recovery

How are you going to balance financial risk with reputational risk?

In some sectors, such as healthcare or charities, public perception often leans toward sympathy when breaches hit the headlines, which allows you a bit more flexibility and leeway in how you respond. In contrast, large corporations are frequently painted as negligent, especially when it comes to data protection. This context shapes whether businesses prioritise financial loss mitigation or reputational damage control.

A key action point that came out of the discussion was whether small businesses need to take on both business and cyber insurance. Craig flagged the rising trend of ransomware claims being made through business insurance, but as there's still uncertainty over what's covered under cyber insurance versus broader business liability, you need a full understanding of your coverage before an attack happens.

The crucial question – do you pay the ransom?

It's the central consideration all security teams and Boards are going to face – to pay or not to pay? Interestingly, Laure pointed out that payment is never a guarantee: "you might pay, and it might still do you no good." Legal jurisdiction also plays a key role, with some regions - particularly the EU and US - prohibiting payments to sanctioned groups, and in certain states like North Carolina and Florida, ransomware payments are outright illegal for public entities. The UK is also debating similar restrictions for public companies and critical national infrastructure. Even when allowed, logistical hurdles like cryptocurrency requirements can slow the process. There are vendors who specialise in facilitating this, but it's an area many businesses aren't prepared for. Then there's the issue of reserves:

- Stefan argued that organizations should have war chests in reserve in case of ransom requests
- Yet Lauren argued that this simply isn't feasible for every company, especially startups and SMEs
- **Finally, Craig argued that instead of setting aside reserves to pay attackers, companies should reinvest those resources internally - strengthening cyber teams and defences**

It's clear that many companies still don't understand whether paying a ransom is even legal, or financially viable, leaving executives in a state of uncertainty.

As the CISO, are there wider considerations you need to be aware of?

In the aftermath of a breach, CISOs are often asked whether they're protecting the business or themselves. With growing scrutiny and the risk of being scapegoated, many are turning to legal counsel and personal risk planning to protect their own positions. Having a law firm on retainer is becoming more common practice, especially as the boundaries of personal liability in the wake of cyber incidents become increasingly blurred.

> *"Incident Management isn't just about the technical restoration of impacted systems or services, it's about preparing and learning from each situation. When it comes to a live incident, you have to make informed decisions under pressure, and the best way to do that is ensuring you have the right knowledge in the room to articulate the risks and understand the technical complexities so you can fully appreciate your response options."*
>
> **Lauren Wilson, EDF**

KEY ACTIONS

Weigh up the risks: Your remediation strategy should reflect your industry context: what's more damaging: downtime, fines or public trust? Align with leadership early and prepare for media fallout in fast-moving digital spaces.

Clarify insurance coverage: Understand exactly what your cyber and business insurance policies cover before an incident. Don't wait until a breach to discover gaps in liability or ransomware claim eligibility.

Know payment decisions in advance: Establish your payment policy now, considering legal constraints, operational impact and ethical implications. Know your jurisdiction, build response partnerships and don't assume paying equals recovery.

Post-incident review: After containment, conduct a thorough post-incident review involving technical teams, leadership and key business units. Identify root causes, assess response effectiveness and turn lessons learned into actionable improvements to strengthen resilience.

WHAT DOES THE INDUSTRY NEED?

If we don't invest in collaboration, education and shared responsibility now, we'll keep fighting tomorrow's threats with yesterday's mindset, and that's a risk we can't afford to take

Are you doing enough in your own business?

Much of the IR function is reactive by nature, but the real value comes from proactive engagement. It's time we asked how we can help others before the crisis hits and show them that security is a shared responsibility.

Our experts referenced how traditional mandatory training often misses the mark. Instead, we need to focus on preparedness, real-world relevance and clear, jargon-free communication. Yoshi suggested holding open meetings where the entire organization can see how the security team operates and why it matters.

The aim is to solve real problems for the business. Ask: how can we help the CFO avoid fines? What can we give the sales team to strengthen their pitch? How do we help the broader team work more efficiently and safely online? As Stefan put it, "we have to be better at demonstrating our value" and that means changing our approach.

What can we do for the wider industry?

Leaders in cyber, especially those with the experience and perspective to make an impact, should be seeking out pro-bono and NED roles to support less mature organizations. Ideas like a CISO-led pro-bono advisory board could provide huge value across sectors – and this was a key insight that came out of the event. At Trident, we are now building out this board and actively looking for CISOs to join us. Get in touch to join the movement!

As attackers become bolder, targeting vulnerable sectors like healthcare in their attempts to bypass hardened enterprise defences, the need for a united front is clear. There simply isn't enough expertise in the industry to meet the growing challenge. If you're in a position to help, now is the time to contribute. More roundtables, open discussions and real collaboration will help cut through the noise and equip decision-makers with the clarity they need to act.

INSIGHTS FROM THE FRONT LINE

James Dyson

VP Global Services, WithSecure

With over 17 years of experience in cyber security, James has played a pivotal role in positioning WithSecure at the forefront of the global security landscape. His strategic focus on deepening collaboration with partners and clients has helped shape the company's reputation for delivering outcome-driven solutions, proving that the best results come when we face security challenges together.

"Boasting more than 35 years of industry experience, WithSecure offers a comprehensive suite of cyber security solutions, including endpoint and cloud protection, threat detection and response and exposure management. As market leaders in the sector, we work with over 7,000 partners and serve more than 100,000 customers worldwide, always focused on delivering measurable security outcomes through customized tools and solutions.

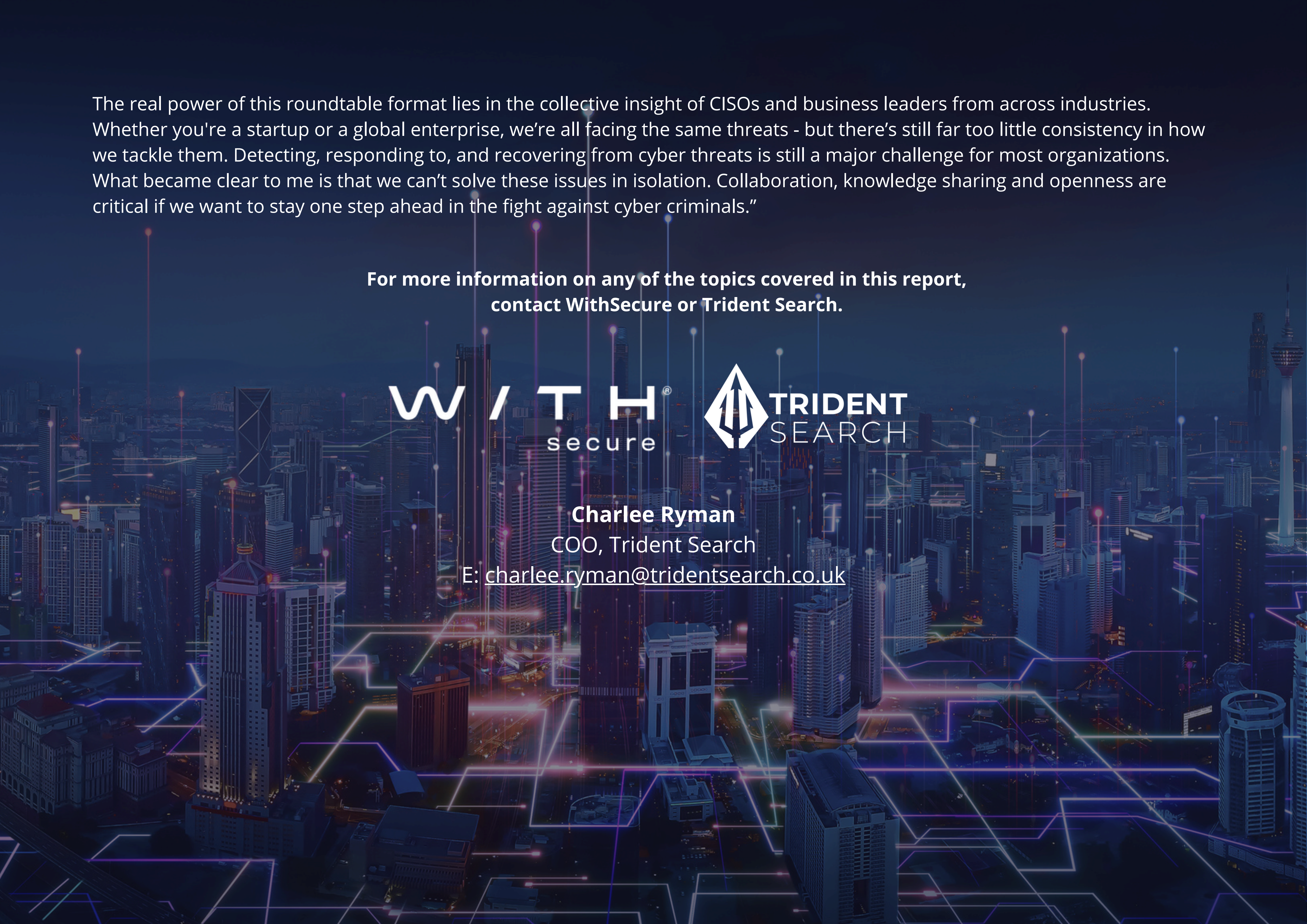
With our incident response experience, we've supported global organizations to make fundamental changes to their people and processes, which was why I found the sheer range of views expressed at this event so striking. In today's threat landscape, consistency in how we respond to major attacks is more critical than ever. A fragmented approach across the industry only increases vulnerability. Threat actors are evolving rapidly, supercharged by AI and automation. To stay ahead, businesses must evolve too - adopting best practices and acting with urgency.

Recent industry reports show that global ransomware attacks surged by over 95% between 2023 and 2024, with malware, DDoS attacks and credential theft following closely behind. In this environment, simply reacting is no longer enough, organizations must proactively strengthen their defences from the ground up. That starts with knowing your environment: maintaining an up-to-date inventory, using gold images, enforcing secure remote management tools and ensuring administrators understand how to manage credentials securely. Service accounts should never allow interactive login, and network segmentation can limit the impact of a breach - sometimes isolating a zone is far less disruptive than taking down an entire data centre.

Patch management remains one of the most critical yet overlooked defences, and frequent exercises - from tactical run-throughs to full-on simulations – are essential to keep your team sharp. Crucially, containment must be tailored to the threat: historical compromises may need a slower, forensic approach, while active ransomware scenarios demand swift, aggressive action. To summarise all of that, cyber resilience is not just about tools, it's about readiness, agility and the discipline to apply the right response at the right time.

Our approach supports best practice while recognising that incident response must flex to business context. **Still, a few lessons have proven true across every client engagement:**

- Even simple tasks become complex under pressure. Practise **isolation procedures** and **access control** in advance.
- **Centralise key documentation** like Incident Response Plans and make sure they're accessible and actionable to all employees.
- For significant incidents, **assign set workstreams and an Incident Commander** to maintain oversight. Even for minor attacks, having a clear chain of command can save you precious time when working under pressure.
- Always **assess the full business impact** before containing - sometimes that means looping in senior stakeholders early.
- The right tools are only as effective as the people using them! **Invest in training and development** regularly to keep your processes watertight.
- Stay compliant by **managing regulatory communications** with care; fines post-breach can be just as damaging as the initial attack, such as Advanced Computer Software Group who were charged £3.07m by the ICO for failing to implement MFA before they were attacked.
- And finally, remember: a major incident is a marathon, not a sprint. **Pace, structure and coordination matter**.



The real power of this roundtable format lies in the collective insight of CISOs and business leaders from across industries. Whether you're a startup or a global enterprise, we're all facing the same threats - but there's still far too little consistency in how we tackle them. Detecting, responding to, and recovering from cyber threats is still a major challenge for most organizations. What became clear to me is that we can't solve these issues in isolation. Collaboration, knowledge sharing and openness are critical if we want to stay one step ahead in the fight against cyber criminals."

For more information on any of the topics covered in this report, contact WithSecure or Trident Search.

Charlee Ryman
COO, Trident Search
E: charlee.ryman@tridentsearch.co.uk