
TRIDENT
SEARCH
THE CYBER SECURITY
INNOVATION FORUM
HOW TO BREAK A BLUE TEAM
Sponsored by
wavenet

HOW TO BREAK A BLUE TEAM

The Cyber Security Innovation Forum brings together leaders from across the cybersecurity industry to discuss the biggest topics affecting our businesses. We've covered the rise of AI, the red flags that will derail your security posture and the importance of bridging the divide between vendors and end users, all resulting in actionable takeaways to drive change in the market. We've seen so many events that merely operate as a vacuum, so the purpose of the Innovation Forum has always been to ensure leaders are held accountable for delivering change across the sector.

In this latest Forum, Trident was joined by executives and decision-makers from the financial services industry to debate "How to Break a Blue Team." Over the course of the evening, we discussed the threats to security, the challenges blue teams are facing and the importance of constant vigilance and regular testing in an evolving threat landscape. Thank you to all our guests who provided their insights into the issues raised.

Our Sponsor

Thanks go out to our event sponsor, Wavenet, a market leader in unified communications, business telephony, and cybersecurity solutions.

OUR EXPERTS

Paul Colwell, CTO, **Wavenet**

Craig Edwards, CISO, **Schillings**

Simon Fowler, CISO, **Trading 212**

Paul Colnan, CISO, **ION Markets**

Kushal Dave, Head of Security Operations, **Deliveroo**

Munawar Valiji, CISO, **Trainline**

Jon Dapre, Ex-Gobal CISO, **Arqit**

Daniel Jones, CISO, **Elwood Technologies**

Philip Bennett, VCISO, **Nownet Ltd**

Stefan Dieni, Director of Cyber Engineering and Architecture, **Capital One**

Alex Barnett, Director of Business Development, **Wavenet**

Mark Stevens, Head of CERT, **Santander**

Katarina Vetrakova, Head of Privacy and Security, **GoCardless**

Emili Evripidou, Senior ICT & Security Risk Manager, **Klarna**

Diana Moldovan, Security Operations Manager, **GoCardless**

Charlee Ryman, COO, **Trident Search**

Lottie MacCallum, Head of Marketing, **Trident Search**

KEY THEMES

So what will break your blue team, and as a leader what can you do to safeguard your business and people? We'll cover some of the key discussions that came out of the Forum, including:

What are the critical issues that will make your blue team fail, and how can you proactively mitigate their effect on your security function?

The importance of regular red teaming and stress testing for improved incident preparedness.

Why, in an increasingly sophisticated threat landscape, without effective incident response your business will fail.

How do we collaborate, both within our own businesses and with the wider industry, to ensure collective success?

BREAKING THE BLUE TEAM

The blue team in any organisation are always under considerable pressure, and unfortunately with the rising intensity and sophistication of threats, we have to accept that this situation shows no sign of abating any time soon.

With challenges including **burnout, lack of appropriate tooling, technical debt, advanced persistent threat (APT) groups, inefficient incident response processes and a shortage of people power**, is it any surprise that blue teams are stressed?

One of the most significant challenges however is that APTs and other threat actors are evolving at a faster rate than defensive functions can keep up with, necessitating constant adaptation. It was Diana Moldovan who mentioned the unfortunate reality that security team decisions are often based on **cost rather than need** as budget cuts are made across the sector, meaning SOC teams have to achieve more with less. **New regulations** such as **DORA**, of critical importance in the financial services sector, will further redirect resources from the front line of defence as more effort has to be put into ensuring compliance, says Alex Barnett.

At the head of security, the role of the CISO has also become increasingly difficult. CISOs face **personal liability** for crises and breaches and must navigate an environment of **strict and often escalating regulations**. Charlee Ryman pointed out that without the board and leadership's buy-in regarding the importance of cybersecurity, we'll expect see many professionals leaving the industry. Yet strong leadership is essential; without it, defensive teams can quickly become directionless and that compromises the whole security posture.

Put simply, there's a lot of factors that will break your blue team, and an awful lot at stake if they do! But the situation doesn't have to be so bleak – there are plenty of ways to safeguard and protect your business, which our experts delved into over the course of the evening.

"The biggest threat to your blue team is still internal - when we're seeing 95% of all incidents caused by human error and 43% of breaches attributed to insider threats, it's no wonder stretched security teams are struggling. Worryingly, this is often exacerbated by constrained IT budgets causing the postponement or cancellation of planned blue team IT security training."

Jon Dapre, Security Leader

YOU DONT KNOW WHAT YOU DONT KNOW

What's the issue: Without regular testing, you run the risk of being complacent and thinking your security posture is at a level it's not.

The key to proactive defence is **effective preparation**, and the best way to do so is to use a red team to test out your capabilities. By simulating real-world attacks, pen testers allow security teams to uncover weaknesses in their systems, applications and networks that they may not have been aware of.

Mark tells us that "a proper red team will give you visibility into what your blue team can do", but as Stefan Dieni added, the real point **"is to find the things you don't know about"**. Your security team need to know where the critical vulnerabilities are in their architecture, and drawing on the skills of an outsider with no pre-conceptions or biases is an important way to do this. By putting themselves into the mindset of an attacker, pen testers help you to mitigate risks and prepare for challenges before you hit crisis point.

You may think that you already have robust security processes, but what came out of the discussions was that it's easy to forget **you don't know what you don't know.**

The objections to pen testing are often framed around **budget capacity, buy-in from leadership and the Board and the time commitment of taking security teams away from their front-line roles** to take part in exercises. However, as Mark Stevens says, bringing in an external red team is "not a luxury, but an essential" if you want to identify gaps in your security posture, remediate issues in the architecture and ultimately improve resilience.

For larger organisations, Munawar Valiji floated the idea of **bringing red teams in house,** helping your blue team to continuously improve as they are repeatedly tested. The aim is that as they become more aware of their own vulnerabilities, they also get better at pre-empting issues and proactively defending against threats. Yet we must be cautious of the **bias-risk** here, as the key benefit of using external parties is to get around any preconceptions of where your weaknesses are.

Despite the objections leaders may have to pen testing, it's essential to get buy in. By simulating real-world attack scenarios, a red team can reveal blind spots in your security posture, **ensuring that unknown risks are identified and addressed before they can be leveraged in an actual attack** - surely a priceless asset?

SOLUTIONS - OVERCOMING OBJECTIONS

Get the Board on board: Our experts suggested the best way to ensure buy in is to highlight that proactive testing helps the organisation to align with industry best practice and compliance requirements, helping you to meet regulatory obligations and avoid costly penalties.

Test out your vendors: In a straw poll led by Paul Colwell of "how many of us stress test vendors", only 12% of all attendees did. If the CrowdStrike incident has shown us anything, it's that we put a lot of trust into third parties and give them unprecedented access to our assets and systems. To maximise the benefits from pen testing should we not be applying the same stringent testing to our partners as we do to our teams? This will likely become more essential as a means to maintain control over the security ecosystem.

Leverage tools and technology: As the industry evolves, its worth exploring which vendors are using emerging or disruptive technology who may be able to use novel tools to plug gaps in your security architecture. You'll only know what's required when you know where the weaknesses are in your systems.

"Regular application of red team learnings helps you to stay ahead of evolving threats, ensuring that your security posture remains adaptive and effective. This proactive stance not only reduces the risk of successful attacks but also builds trust with stakeholders, demonstrating your commitment to safeguarding sensitive data and maintaining operational integrity."

Mark Stevens, Santander

STRENGTHENING INCIDENT RESPONSE

What's the issue: When it's more important than ever to be proactive as well as reactive, why aren't we prioritising incident preparation?

A theme which frequently came up, was the importance of being prepared for critical incidents, especially in financial services industry where the repercussions of failure can be catastrophic for customers. As an industry we are really falling behind on incident response (IR), with **just 21% of UK companies having an IR plan in place**, despite facing over **2.39 million cybercrime incidents** last year.

But we need to look at this as two very distinct categories: incident preparedness and incident response. Most security teams worth their salt will have a solid response plan in place for how to combat critical threats and major attacks. Yet too many businesses are falling down on the preparedness part.

PRE-INCIDENT STRATEGY:

To proactively defend against threats a pre-incident plan is essential, and most effective when used in collaboration with pen testing; allowing organisations to identify and address vulnerabilities before they can be exploited.

Diana and Katerina Vetrakova both referenced times when running drills revealed weaknesses they didn't consider, such as the need for **backup systems**. They encourage organisations to have emergency laptops in all branches which are kept turned off and without the latest updates, ensuring a physical resource is always available.

This kind of **proactive risk management** ensures communication channels are established, responsibilities are established, due diligence is carried out and the necessary tools, personnel and processes are in place before an incident occurs.

Like with pen testing, many of the objections to building up incident preparedness centre around time and cost. Yet with many **third parties and consultancies** including it in their offering, it's worth considering outsourcing the service as a temporary fix whilst you build up in-house capabilities.

Fundamentally, it's of critical importance to build up a pre-incident strategy in line with red team activities. First, uncover the vulnerabilities in your blind spot, then use this information to safeguard your people and systems before an attack. Being proactive helps **maintain customer trust** and **minimizes financial losses** further down the line.

PROACTIVE MANGEMENT:

Rotate your SOC: To prevent burnout, regularly rotate your SOC team shifts so that blue team members are not always operating in first line of defence roles and can take a break from constant high alert.

Take a comprehensive approach: Cyber attacks typically teach us about complete destruction scenarios, which our playbooks are designed to handle. However, unexpected events require planning too. Stefan questioned whether essential tasks like payroll are considered in the event of system failures, emphasizing that IR plans must encompass the broader business, not just IT.

Enhanced security drills: There is an argument for running non-critical scenarios as P1's so that when crises occur your team are better prepared and aware of the processes they need to follow. With the speed of response so fundamental to its success, a well-drilled team is a more effective one.

Prioritize efforts systematically: To keep systems running smoothly, determine the hierarchy of recovery efforts well in advance of an attack. Kushal commented that it's often a case of helping "the loudest first" when security teams are scrambling, but you must have a structured approach to which functions are most important – is the CEO really the top priority?

REACTIVE MANAGEMENT:

Assess the tech stack: IR teams need the proper tools to analyse, detect, manage and report on threats. In light of the CrowdStrike fallout, we may see more companies diversifying the vendors or third parties they work with to provide these tools, but regular analysis of whether the tech stack is effective for the business is essential.

Training and development: Implement additional training for the blue team to improve awareness and readiness for future threats, as well as assessing the tools in your architecture to ensure they are still capable of addressing the latest threats and vulnerabilities.

Continuous development: When any crisis is resolved, take the time to analyse the incident to understand the lessons that can be taken from it and ensure your IR plans and playbooks are always being updated with post-incident reviews. This will help you to be adaptable in the changing threat landscape.

COLLABORATION IS KEY

What's the issue: Internal collaboration - or purple teams in this case - are incredibly useful, but if you're only looking inwards, you're only as good as your team and risk missing crucial intel and support from the wider industry.

In such an interconnected world, partnerships and tools have become essential. As Jon Dapre says, with so many options on the market it's simply not cost-effective for companies to bring all operations in house, not when there are **specialist vendors** who could provide better protection. So as we become more reliant on partners, we have to accept the need to collaborate.

There are significant benefits to this as well. Being able to rely on communication channels and information sharing across the industry means you **access news and intel much faster**. With the speed of response so critical in any incident, the importance of this cannot be underestimated. On the day the CrowdStrike incident occurred, we spoke to one security provider who, 12-hours into the incident, still had no idea what was happening as they were only sharing information internally and no one in the business was aware.

As Alex says, "we are a community of professionals who work best together", a comment supported by Mark who stated that the real USP of the cybersecurity industry is that with the number of **professional communities, peer groups and ISACs** we have access to, we're in the best possible position to share intelligence and work through crises together. In fact, it was the view of some of our experts that these external collaboration channels were in some ways more beneficial for threat intel than having your own CTI team!

From LinkedIn groups to WhatsApp chats, and from general news to niche interest groups, there are a wealth of channels available. Ultimately, if you don't have those external outlets, peer groups and networks that enable information sharing, you're taking a huge risk with your business.

INSIGHTS FROM A CTO

Paul Colwell

CTO, Wavenet

With over 20 years of experience in cybersecurity, Wavenet CTO, Paul Colwell, has been instrumental in positioning the company at the very forefront of the industry. As leaders in unified communications, business telephony and cyber solutions, they are now focussing their efforts on solidifying their place as the go-to supplier for pen testing expertise, a move Paul is spearheading in the drive to attain CBEST.

"**Formed in 2000, Wavenet has grown to become a respected, multi-award-winning provider of telecoms, cybersecurity, IT & technology solutions to thousands of businesses and organisations across the UK**. Its vision is to be the most respected provider of cyber security, cloud and technology solutions to UK customers by investing in the right technologies, partners and people, and maintaining strong and dependable growth.

As a managed service provider, we have long-standing partnerships with top global technology providers including Microsoft, BT, Gamma, Extreme Networks, 8x8, Five9, Darktrace, Cato and Gigamon, and of course we have the relationship with Trident Search for our hiring and personnel needs, which is how our partnership on this Innovation Forum came about.

With pen testing a key focus of the event, myself and Alex Barnett, Director of Business Development, enjoyed hearing the insights and experiences of the leaders around the table. Wavenet's pen testing team is growing quickly; we now have over 50 testers and maintain both CHECK and CREST accreditations. Our testers are highly certified, with over 90% holding SC clearance, and a large number of them possessing Developed Vetting (DV) clearance.

As a business that sees huge value in red team activities and stress testing your security posture, it was certainly beneficial to hear our views echoed by other executives during the Forum. Wavenet continues to invest in our testing teams with new, exciting projects, such as the Pen Testing as a Service portal, which is due to be released in October. We have also made investments in threat intelligence and advanced red teams, and we aim to obtain CBEST accreditation in the next few months.

The key benefit to this kind of roundtable format is to hear from other CISOs and business leaders as to why we may have differing opinions and how we can collaborate on solutions to common problems.

Indeed, my biggest takeaway was that whether you are an MSSP, a global enterprise, or a smaller business, we are all worried about the same issues. Detecting advanced threats, artificial intelligence, and alert fatigue are problems we are all trying to overcome, and with the pace of industry development we're all trying to figure out the best way to utilise some of the new technologies. What this has made me realise is that we can't work on any of these challenges in isolation; working together and learning from one another is vital in the fight against cybercrime."

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

wavenet TRIDENT SEARCH

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