FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

A CEO Perspective

Building Smarter Cybersecurity: How AI, Open Collaboration, and Threat-Informed Defense Are Reshaping Resilience

Julien Richard
Co-founder & CTO,
Filigran
in conversation with
Jarad Carleton
Global Research Director,
Cybersecurity, Frost & Sullivan

Building Cybersecurity Around Threat-informed Defense

For years, organizations have strengthened their cybersecurity by adding more tools, collecting more threat intelligence, and generating more security data. Yet despite these investments, many security teams continue to struggle with a fundamental challenge: turning information into timely, informed action.

At the same time, the threat landscape is evolving faster than ever. Artificial intelligence (AI) is compressing the time between vulnerability discovery and exploitation, while increasingly complex technology environments make it harder for security teams to understand which threats matter most and how they should respond.

In this Transformational Growth Leadership conversation, Julien Richard, Co-founder & CTO of Filigran, explains why the future of cybersecurity lies not in accumulating more intelligence, but in building threat-informed defense, an approach that connects threat intelligence, exposure validation, risk management, and operational workflows into a continuous decision-making process. He also discusses the role of open-source innovation, the responsible use of AI, and why empowering defenders, not replacing them, will define the next generation of cybersecurity

> “It’s not about the number of tools. It’s about how quickly you can validate and take the right action.”
>
> — Julien Richard, Co-founder & CTO, Filigran

Why More Security Tools Aren't Solving the Problem

Jarad Carleton: *Organizations have invested heavily in cybersecurity over the past decade, yet many still struggle to reduce cyber risk. Why do you think organizations continue to face that challenge despite having more security technologies than ever before?*

Julien Richard: One of the biggest challenges is that organizations have accumulated an incredible number of security tools, but those tools often operate independently. Every solution produces valuable information, yet much of that intelligence remains fragmented across different systems and teams.

Threat intelligence is a good example. Many organizations have become very effective at collecting indicators of compromise, adversary techniques, and vulnerability information. The challenge begins after that information has been gathered. Security teams still need to determine which threats are relevant to their environment, validate potential exposures, understand business impact, prioritize remediation, and coordinate action across multiple stakeholders.

That process is often far more difficult than collecting the intelligence itself. Our philosophy has always been that threat intelligence should never be viewed as the final objective. It's the starting point. Intelligence becomes valuable only when it helps organizations understand their actual level of exposure and supports faster, more informed action.

Ultimately, cybersecurity is not measured by the amount of information an organization collects. It is measured by how effectively organizations can translate that information into action and reduce risk.

Frost & Sullivan's **Transformational Growth Leadership Program** aims to honor visionary business leaders who possess the foresight and leadership acumen to drive positive change within their organizations. The leaders we celebrate hail from diverse sectors and company sizes, yet they all share an unwavering commitment to innovation and excellence.

AI Is Compressing the Time Between Discovery and Exploitation

Jarad Carleton: *You touched on how quickly the threat landscape is changing. Artificial intelligence is accelerating that change on both sides of cybersecurity. How do you see AI reshaping the security landscape?*

Julien Richard: AI is accelerating change on both sides of cybersecurity. Attackers can automate activities that previously required significant time and expertise. As a result, the window between discovering a vulnerability and attempting to exploit it continues to shrink. Security teams have less time to assess exposure, validate risk, and implement effective mitigation.

Defenders, however, also have new opportunities. AI can help security teams analyze large volumes of information, identify patterns more quickly, summarize intelligence, and automate repetitive tasks that would otherwise consume valuable analyst time.

The important point is that AI should enhance human expertise rather than replace it. Cybersecurity decisions often require context, judgment, and an understanding of business priorities. AI can dramatically improve the speed at which analysts process information, but accountability and decision-making must remain with experienced security professionals. That balance will become increasingly important as AI adoption accelerates across both offensive and defensive cybersecurity.

From Information to Action

Jarad Carleton: ***Throughout our conversation, you have emphasized that collecting threat intelligence isn't enough; it has to lead to action. Was that the conventional thinking you set out to challenge when you founded Filigran?***

Julien Richard: One assumption we questioned very early was the idea that threat intelligence alone creates security value.

For years, organizations invested heavily in collecting intelligence feeds, indicators of compromise, malware reports, and threat actor information. That work remains extremely important, but we believed the industry had become too focused on gathering information rather than using it effectively.

Threat intelligence should never exist in isolation. Its real value comes from helping organizations understand how threats relate to their own environment, whether they are actually exposed, what the business impact could be, and which actions should be prioritized. That realization shaped our thinking from the very beginning.

Rather than building another intelligence repository, we wanted to connect threat intelligence with exposure management, validation, and operational decision-making so organizations could move beyond simply collecting information and start acting on it. That's what ultimately led us to build around the concept of threat-informed defense.

From Threat Intelligence to Threat-informed Defense

Jarad Carleton: ***That naturally brings us to a term you have mentioned several times throughout our discussion: threat-informed defense. For readers who may be hearing it for the first time, what does it actually mean in practice?***

Julien Richard: Threat-informed defense is about bringing together information that has traditionally remained disconnected. Security teams often have threat intelligence platforms, exposure management tools, vulnerability scanners, attack simulation capabilities, and risk management systems operating independently. Each provides valuable insight, but each represents only one part of the overall picture.

Threat-informed defense connects those different perspectives. It starts with understanding how adversaries operate, but it doesn't stop there. Organizations also need to understand whether they are vulnerable to those techniques, how likely an attack is, which business assets are affected, and which remediation activities will reduce risk most effectively.

When those elements are connected, security becomes much more proactive. Rather than reacting to individual alerts, organizations begin making informed decisions based on their own environment, priorities, and risk profile. Ultimately, the goal isn't simply to know more. It's to understand what matters most and act on it.

Connecting Intelligence, Exposure, and Risk

Jarad Carleton: ***Threat-informed defense clearly requires more than a single technology. How does Filigran bring those different capabilities together into one operational view?***

Julien Richard: We have always believed security shouldn't be managed as a collection of disconnected products. Each capability contributes a different piece of the overall security picture. Threat intelligence explains how adversaries operate. Exposure management identifies weaknesses within the environment. Validation technologies help determine whether those weaknesses can actually be exploited. Risk management provides business context and helps organizations prioritize remediation. When these capabilities operate independently, security teams spend enormous amounts of time manually connecting information across different systems.

Our focus has always been to simplify that process. By connecting these different sources of information through an open platform, organizations gain a much clearer understanding of where they are exposed, what requires immediate attention, and how they should respond. That creates a far more operational approach to cybersecurity than simply producing reports or collecting indicators.

Building an Open Platform for Security Collaboration

Jarad Carleton: ***Listening to you, it sounds like collaboration is just as important as technology itself. Why has openness remained such a central part of Filigran's strategy?***

Julien Richard: Cybersecurity has always been a collaborative discipline. No single organization, vendor, or community possesses complete visibility into every threat. Progress happens when information can be shared, validated, and improved across the broader ecosystem.

That's one of the reasons we have invested so heavily in open source. Open-source communities allow organizations to collaborate around common challenges while accelerating innovation. They also provide transparency, giving users greater confidence in how technologies evolve and how information is managed. For us, openness isn't simply a development model. It's fundamental to the way we believe cybersecurity should evolve. The more effectively organizations can collaborate, integrate different sources of intelligence, and build on shared knowledge, the stronger the entire security ecosystem becomes.

AI Should Strengthen Human Judgment, Not Replace It

Jarad Carleton: *One technology has come up repeatedly throughout our conversation, artificial intelligence. It's changing the way both attackers and defenders operate. As organizations increasingly embed AI into their security operations, how do you see the relationship between AI and human expertise evolving?*

Julien Richard: AI has enormous potential to improve cybersecurity, particularly by helping analysts process information more efficiently. Security teams deal with vast amounts of threat intelligence, technical reports, vulnerabilities, and operational data every day. AI can summarize information, identify patterns, recommend possible actions, and automate repetitive tasks that would otherwise consume significant time. Those capabilities can dramatically improve productivity.

However, cybersecurity is ultimately about managing risk. Decisions often require context, business understanding, and human judgment. AI can assist those decisions, but it should not become the decision-maker.

Transparency is equally important. Security professionals need to understand why a recommendation has been made and be able to validate it before taking action. AI should increase confidence in decision-making rather than becoming a black box that analysts simply trust without question. Our philosophy has always been that AI should empower defenders by helping them work faster and more effectively while keeping humans firmly in control of critical decisions.

Turning Technology into Measurable Outcomes

Jarad Carleton: *Ultimately, organizations don't invest in cybersecurity platforms simply to deploy another technology. How do your customers define success once these capabilities are in place?*

Julien Richard: It's never been about deploying another platform. Customers want to understand whether they're responding faster, prioritizing more effectively, and ultimately reducing cyber risk. One of the biggest improvements comes from giving security teams a more complete view of their environment. Instead of working across disconnected tools and isolated datasets, they can bring intelligence, exposure information, and operational priorities together in a single workflow. That helps teams spend less time manually correlating information and more time focusing on remediation and risk reduction.

Ultimately, success isn't measured by the number of alerts processed or reports generated. It's measured by whether organizations can consistently prioritize the right actions, respond more effectively, and strengthen their overall security posture.

Building an Ecosystem Through Open Collaboration

Jarad Carleton: *Throughout our discussion, one message has come through very clearly, cybersecurity isn't something any organization can solve alone. How important are partnerships and the broader security ecosystem to Filigran's long-term vision?*

Julien Richard: Cybersecurity has always been a collaborative discipline. No single organization, vendor, or community possesses complete visibility into every threat. Progress happens when information can be shared, validated, and improved across the broader ecosystem. That's one of the reasons we have invested so heavily in open source.

Open-source communities allow organizations to collaborate around common challenges while accelerating innovation. They also provide transparency, giving users greater confidence in how technologies evolve and how information is managed. For us, openness isn't simply a development model. It's fundamental to the way we believe cybersecurity should evolve. The more effectively organizations can collaborate, integrate different sources of intelligence, and build on shared knowledge, the stronger the entire security ecosystem becomes.

Balancing Innovation with Enterprise Reliability

Jarad Carleton: *As Filigran continues to grow, how do you balance the speed of innovation with the stability and trust that enterprise customers expect?*

Julien Richard: That's one of the most important responsibilities for any technology company. Innovation is essential because the threat landscape changes constantly. We need to move quickly, respond to customer feedback, and continuously evolve our platform.

At the same time, our customers depend on these technologies to support critical security operations. They expect stability, transparency, and reliability. Balancing those priorities requires discipline. It means listening carefully to customers, maintaining a strong engineering culture, and ensuring that every new capability strengthens the overall platform rather than adding unnecessary complexity.

Ultimately, innovation isn't about releasing more features. It's about delivering innovation that customers can trust and adopt with confidence while helping them solve increasingly complex security challenges.

Leading the Next Evolution of Cybersecurity

Jarad Carleton: *As you look ahead, what do you see as the next chapter in Filigran's journey? Where will your focus be over the next few years?*

Julien Richard: Our ambition has always extended beyond building individual security products. We are working toward a platform that helps organizations connect intelligence, exposure management, validation, risk, and operational workflows into a single operational view of cybersecurity. As the threat landscape becomes more complex, that ability to connect information and provide meaningful context will become increasingly important.

At the same time, we remain deeply committed to open source. Open-source innovation has played a significant role in our growth, and we believe it will continue to shape the future of cybersecurity. It encourages collaboration, transparency, and faster innovation while allowing organizations to adapt technologies to their own environments. Looking ahead, we are focused on continuing to expand that ecosystem, while helping customers build a more operational and collaborative approach to cybersecurity.

Ultimately, success isn't defined by how many products we develop. It's defined by whether we help organizations become more resilient by turning intelligence into meaningful action.

Looking Ahead: The Future of Threat-informed Defense

Jarad Carleton: *If we look three to five years ahead, what do you think will define the next generation of cybersecurity?*

Julien Richard: I believe cybersecurity will become far more connected over the next few years. Organizations are moving beyond managing isolated technologies toward building security programs where intelligence, exposure, validation, automation, and risk management work together as part of a continuous process.

AI will accelerate that transformation by helping organizations process information more quickly and automate many routine activities. The goal shouldn't be to remove people from the process. Instead, AI should help security professionals make more confident and informed decisions.

I also believe collaboration will become even more important. No organization has complete visibility into every threat or every technology. Open standards, ecosystem partnerships, and community-driven innovation will continue to play a critical role in helping organizations strengthen their security posture.

Ultimately, the organizations that succeed will be those that can transform intelligence into action quickly, consistently, and intelligently.

Closing Reflections: Turning Intelligence into Action

Throughout the conversation, Julien Richard consistently returned to one central idea: cybersecurity is no longer constrained by a lack of information. The real challenge is helping organizations transform intelligence into action.

Threat intelligence, exposure management, validation, risk assessment, and artificial intelligence each provide valuable insights. Individually, they offer only part of the picture. Together, they enable organizations to understand their exposure, prioritize what matters most, and respond with greater confidence.

For Filigran, this philosophy extends well beyond technology. Open-source collaboration, ecosystem partnerships, and responsible AI all contribute to a cybersecurity model where transparency, shared knowledge, and human expertise remain central to every decision.

As cyber threats continue to evolve, success will depend less on deploying additional security tools and more on connecting intelligence, context, and operational workflows into a unified approach that enables faster, more confident action. At the same time, Julien believes the future of cybersecurity depends on making these capabilities accessible to organizations of every size, not just those with large security teams or deep technical expertise.

Threat-informed defense, as Julien describes it, is ultimately about making cybersecurity more connected, more collaborative, and more operational, while lowering the barriers that prevent organizations from strengthening their security posture.

As Julien concluded:

> “Filigran will be able to change global cybersecurity if we can lower the entry fee, in terms of knowledge and teams, and automation, about bringing this value to every company, even if they don’t really have a strong practitioner in their organization.”

— Julien Richard, Co-founder & CTO, Filigran

Julien Richard | Co-founder & CTO, Filigran

With over 20 years of experience in product and engineering management, Julien Richard is the CTO and co-founder of Filigran. He brings extensive expertise in developing complex software solutions, specializing in data and artificial intelligence, to drive innovation in threat exposure management. Prior to co-founding Filigran, he held engineering leadership roles, including Vice President of Engineering at YOOI and Director of Engineering at Axway. At Filigran, he has been instrumental in developing the company's open-source eXtended Threat Management (XTM) platforms, OpenCTI and OpenBAS, helping organizations strengthen threat-informed defense while accelerating Filigran's growth as a leading cybersecurity innovator.

Jared Carleton | Global Research Director, Cybersecurity, Frost & Sullivan

Carleton brings 25+ years of experience in the USA and Europe to his role. He works with organizations in Israel, North America, Europe, and Asia, focusing on various security domains such as Active Directory, zero-trust enterprise browsers, managed security services, digital risk protection, digital trust, Internet of Things (IoT) security and privacy, encrypted voice and text messaging, automated security validation, vulnerability management, IT/OT security convergence, fraud detection and prevention, and cloud service provider (CSP) security services. His quantitative research on security trends, maturity, services, and products informs legislators, regulatory bodies, and CXOs, helping them make data-driven decisions that enhance growth.

Ready to Lead the Transformation?

- **Schedule a Growth Strategy Dialog:** Align your growth roadmap with Frost & Sullivan's Visionary Growth Pipeline™ Dialog.
- **Engage with Growth Experts:** Co-design AI-enabled, data-driven operating models that scale industry-specific and commercial impact.
- **Showcase Your Transformational Leadership:** Position your organization as a transformation leader through Frost & Sullivan's Transformational Growth Leadership platform.
- **Join the Growth Council:** Collaborate with industry leaders shaping the future of your ecosystem.
- **Explore Best Practices Recognition:** Be recognized for excellence in growth strategy, execution, and customer impact.
- **Benchmark Your Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Tell Your Story:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.

Appendix: Advancing Threat-informed Cyber Defense

As cyber threats become more dynamic and AI accelerates attack cycles, organizations are adopting threat-informed defense to turn intelligence into faster, more effective action. By connecting threat intelligence, exposure management, validation, and risk, enterprises are building more resilient and adaptive security operations.

To help organizations strengthen cyber resilience, Frost & Sullivan provides strategic insights across threat intelligence, AI-driven cybersecurity, exposure management, security operations, and Zero Trust, including:

- Global Cyber Threat Intelligence and Threat Intelligence Platform Growth Opportunities
- Mobile Threat Defense, Global, 2025–2029
- Frost Radar™: Risk Intelligence Solutions, 2026
- External Risk Mitigation and Management (ERMM) Solutions, Global, 2025–2030

Together, these perspectives highlight the shift toward intelligence-driven security, where connected ecosystems, AI, and threat-informed decision-making enable stronger cyber resilience.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN