

# FRED BRET-MOUNET

CISO

Accela



**Headquarters:** San Ramon, CA

**Employees:** 500+

**Annual Revenue:** Private Company

Fred Bret-Mounet leads security at Accela with a perspective shaped by decades of experience building and evolving security programs across fast-moving technology environments.

His leadership reflects a broader shift in the role of the CISO. The challenge is no longer just about managing risk, but about keeping pace with a level of technological acceleration that is fundamentally changing how software is built and secured.

## AI HAS CHANGED THE PACE OF EVERYTHING

For Fred, the biggest shift in cybersecurity today is not subtle. “Right now, the panic moment is AI,” he says.

In a matter of months, the landscape has transformed. What once required specialized skills is now widely accessible. “It used to be that you needed to have skills and expertise to build software. You do not need that anymore,” he explains.

At Accela, that shift is already visible. “We now have 500 software developers. Everybody has their Claude license and they go at it,” Fred says.

While this unlocks innovation, it also introduces scale challenges that security teams are not traditionally built to handle. “We are getting flooded with new business ideas, new solutions, new internal tools,” he explains. “And we just barely have time to react if we ever find out about it.”

For Fred, this is the defining tension of the moment. The business is accelerating, and security must find a way to keep up.

## REINVENTING THE ROLE OF SECURITY

Rather than resisting that change, Fred sees it as an opportunity to rethink how security operates.

“For the last 25 years, my job has been to get in the way of things,” he says. He describes a traditional model where security reviews happen late, often forcing teams to go back and fix issues after the fact.

That approach is no longer viable at the current pace. “If we do not adapt, we are doomed,” he says.

Instead, Fred is focused on embedding security directly into how work gets done. His goal is to define clear requirements and standards that are automatically applied as developers build. “If I play my cards right, I have a shot at making developers meet my expectations from the get-go,” he explains.

This shift represents a fundamental change in mindset. Security is no longer a gate at the end of the process instead it becomes part of the process itself.

## MANAGING AI THROUGH AI

To address the scale challenge, Fred is exploring a model where AI helps secure AI-driven development. “My theory at this point is that I will manage AI through AI,” he says.

Instead of relying on manual reviews, he is implementing AI agents that evaluate work as it progresses. These systems can assess risk, determine whether additional review is needed, and even generate threat models in a fraction of the time it would take a human.

“Claude will build a threat model that is of better quality than a human that is not motivated to do so,” he explains.

This approach allows his team to focus on what matters most. “I am hoping I will take the edge off and have my team focus on the true risk, not the rubber stamping process,”

Fred says.

For him, the opportunity is clear. By leveraging AI in the right way, security can scale alongside the business instead of becoming a bottleneck.

## VISIBILITY AS THE FOUNDATION

While AI introduces new capabilities, Fred is clear that many of the core challenges remain unchanged. “You cannot protect what you do not know of,” he says.

His focus is on building comprehensive visibility across the organization, including systems, data, and what he refers to as the “virtual workforce” of AI agents. “We need to have an inventory of virtual workforce. What do they do, who manages them, and where can you find them?” he explains.

This visibility is critical not only for security, but for understanding value. “We are spending an obscene amount of money in AI right now, and we do not have good controls to understand what the ROI is,” he says.

For Fred, inventory is not just a technical requirement. It is the foundation for control, accountability, and decision-making.

## AI WILL RESHAPE THE WORKFORCE

Fred is also candid about the broader impact AI will have on how organizations operate. “I suspect we are going to see a serious amount of restructuring in the next six months,” he says.

While AI will improve efficiency, it will also change the types of roles organizations need. Some functions will be automated, while others will evolve to focus on oversight, problem solving, and higher-level decision-making.

At the same time, he emphasizes the importance of long-term thinking. Eliminating entry-level roles entirely could create gaps in the future pipeline of talent.

His perspective reflects a balanced view. AI will drive change, but how organizations manage that transition will determine long-term success.

## RETHINKING SECURITY FUNDAMENTALS

Beyond AI, Fred remains focused on core security disciplines that continue to challenge organizations. Inventory, access control, and patching remain top priorities. “We do not know our perimeter,” he says.

He also highlights identity and access management as an ongoing issue. “We give access to people without thinking it through,” he explains.

Patching is another area where he sees an opportunity for change. Rather than relying on manual processes, he advocates for a more automated approach. “We humans are not able to

keep up with patching requirements,” he says.

These priorities reinforce a consistent theme. Even as AI transforms the landscape, the fundamentals still matter.

## ADAPTING TO WHAT COMES NEXT

For Fred, the defining challenge is not just AI itself, but the speed at which everything is evolving.

The combination of increased development velocity, expanding attack surfaces, and rising expectations from the business is forcing security leaders to rethink how they operate.

At Accela, Fred is focused on building a program that can adapt to that reality. One that integrates security into development, leverages AI to scale, and maintains visibility across an increasingly complex environment.

Because in this new era, standing still is not an option.