accenture

Strategy | Consulting | Digital | Technology | Operations

Security Technology Vision 2016:

Empowering Your Cyber Defenders to Enable Digital Trust

Executive Summary

High performance. Delivered.

Empowering Your Cyber Defenders to Enable Digital Trust

Fighter pilots depend on artificial intelligence, cockpit automation and the latest virtual reality visualization technologies to elevate their reaction times and abilities to peak levels. In the next five years, security professionals will employ similar technologies to predict, detect, respond to and remediate digital attacks. At the same time, enterprises will also rely on new, more flexible staffing models to make sure they have the "top gun" security expertise they need, when they need it.

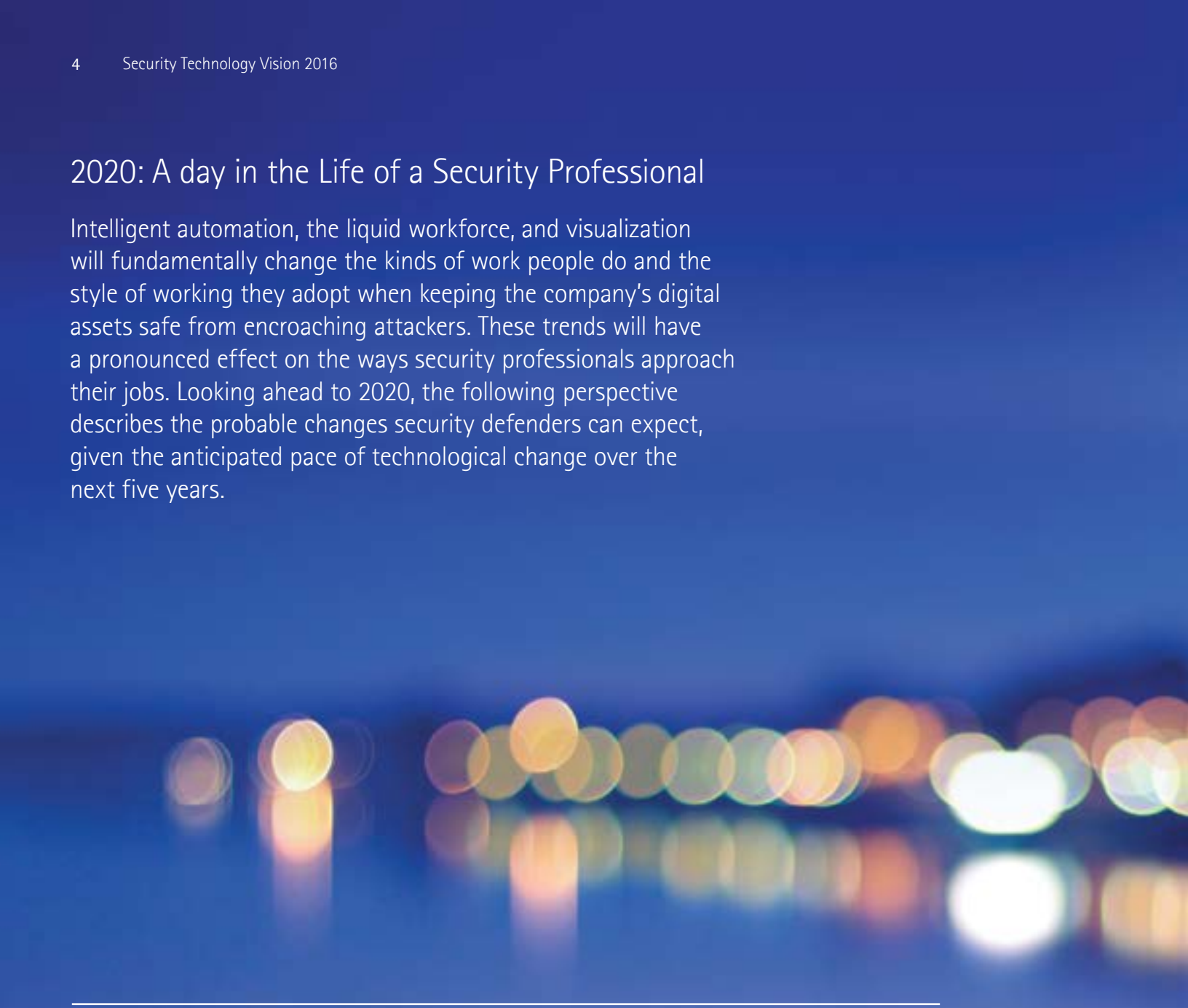
Underpinning all of this change will be the mandate to boost security's effectiveness in supporting the business' efforts to attain digital trust, as new technologies, workforce models and the rapid pace of change in the digital economy raise potent new digital risk issues. Digital businesses will encounter new risks that traditional enterprises never experienced. Consequently, security professionals must assume a more proactive stance as they engage with business owners to identify new risks, achieving even greater levels of security effectiveness. The need for this shift is already apparent: attackers are overwhelming organizations that lack enough highly skilled people with "eyes on glass" to make sense of it all and defend the enterprise. In fact, recent studies show that up to 45 percent of organizations say they have increasing difficulty finding qualified people.[1] And organizations don't just lack skilled analysts, either: they need qualified people in all security-related functions, including strategy.

In response, leading organizations are adopting disruptive innovations like intelligent automation and the liquid workforce. Intelligent automation will enable future security teams to link artificial intelligence (AI) models—thinking machines capable of assessing situations and taking action—with automation and interactive visualization in ways that enhance security professional capabilities. And the liquid workforce, with its crowdsourcing and freelance staffing options, will make it easier for enterprises to access talent for short-term projects. However, these disruptive innovations also represent potential security threats because they can open new attack surfaces within organizations that hackers can exploit.

[1] "The 2015 (ISC)² Global Information Security Workforce Study," Frost & Sullivan.

2020: A day in the Life of a Security Professional

Intelligent automation, the liquid workforce, and visualization will fundamentally change the kinds of work people do and the style of working they adopt when keeping the company's digital assets safe from encroaching attackers. These trends will have a pronounced effect on the ways security professionals approach their jobs. Looking ahead to 2020, the following perspective describes the probable changes security defenders can expect, given the anticipated pace of technological change over the next five years.



Aided by artificial intelligence, visualization enables organizations to understand a tsunami of data quickly, cutting through "noise" and finding clarity.

Intelligent Automation Steps Up

Organizations will increasingly use AI models capable of understanding specific concepts and predicting future actions. Such models will allow security teams to shift from simply detecting risks to actively normalizing, validating, contextualizing and prioritizing threats. AI will also enable automated responses to activities. Essentially, intelligent automation will turn a proficient analyst into a highly skilled one. Equipped with AI-infused process automation, tomorrow's professionals will be more competent and find it easier to plug themselves into an unfamiliar security organization. That's because they will work with a mature set of defined and automated security processes and have a clear understanding of what is critical within the business, enabling them to respond to threats effectively.

How Artificial Intelligence will Enable Visualization

By 2020, visualization will be a core element of enterprise cybersecurity strategy, harnessing the innate human ability to zero in on patterns quickly and pick out anomalies. Visualization will allow security teams to understand at a glance how contextually valid a threat is and which areas of the business it affects. By shifting away from log and text interpretations and replacing them with visual comprehension, organizations will be able to scale their ability to interpret security events. AI supports the interpretation of patterns and behaviors that could constitute risks, and with enough "learning" it can validate legitimate threats and enable the cyber hunt.

Aided by AI, visualization enables organizations to understand a tsunami of data quickly, cutting through "noise" and finding clarity. Today, visualization remains nascent, but within two years, the security professional will be able to visualize the entire enterprise. And within three years, the power of advanced graphics processing units will enable leading companies to do this in real time.

The Role of Artificial Intelligence in the Breach

Security will employ AI to understand the larger context of a breach and anticipate its subsequent evolution. By combining AI with security function automation, it becomes possible to automate and guide the process—to the point where ancillary tasks become trivial to execute. This will enable staff to concentrate on major threats by real threat actors instead of being distracted by minor issues. Automation will also introduce new engagement models and give defenders increasingly sophisticated ways to respond to attackers. These include the near-real-time manipulation of data that subtly changes what adversaries see as they target an organization, bringing active defense to the forefront of cyberdefense.

Today's fighter pilots augment their skills and training with cockpit automation that elevates their capabilities and enables them to fly massively complex aircraft routinely and safely. Likewise, automation will allow tomorrow's security professional with average capabilities and training to perform like a highly skilled practitioner. By standardizing excellent performance with automation, companies can begin to get their arms around the growing shortage of skilled security people.

The Liquid Workforce Enables Concrete Security Staffing Solutions

While organizations are investing in the tools and technologies they need to keep pace in the digital era, most are neglecting a critical factor—their people. In order to capitalize on the opportunities presented by technology innovations, future organizations will focus on helping their people become a more fluid, agile and flexible workforce. From a security perspective, firms currently face challenges in both finding and keeping new staff excited and intellectually engaged in problem-solving activities.

The liquid workforce model could be the answer, since the use of freelancers and crowdsourcing—where organizations solicit services from a crowd of people, rather than from traditional employees or suppliers—are major elements of the approach. In fact, Accenture believes 40 percent of a business' entire workforce will be freelance by 2020.

The outsourcing of security jobs requires an immense amount of trust—the sort that only emerges from a strong relationship between an organization and its service provider. Where such relationships exist or can be created in the future, a role for freelancers and crowdsourcing will emerge within the security function. Tomorrow's liquid workforce will enable companies to benefit from a far greater pool of security experience and expertise than may be available today.

However, while crowdsourcing can provide clear benefits, it can also expose a company to risk. In fact, a recent "bug hunter" who discovered an exploit in a popular social networking site caused tangible damage by abusing his discovery after reporting it to the company. One possible response to such risks involves Synack, a company that offers freelance penetration tests via a private network of skilled, rigorously vetted security researchers from around the world. Synack employs specific technologies that enable clients to control the scope and degree of access the tests allow.

Over the next five years, enterprises need to find ways to reduce the potential cybersecurity risks to acceptable levels. Successful companies will likely employ a core team of security people with high-powered skills that they will augment using crowdsourced and freelance labor to meet the demands of the digital business more efficiently and effectively.

Conclusion

The sheer volume, velocity and variety of data that security organizations process in the future will dwarf today's already massive information overload. Lurking within this deluge, increasingly sophisticated attackers will test every defense to its limit, even as new business technologies transform the ways organizations work, exposing them to unexpected threats. In response, security professionals must seek new ways to keep up with the rapid pace of change. Innovations like intelligent automation, visualization and the liquid workforce will all play prominent roles in tomorrow's security landscape, transforming an enterprise's security program to prepare it for 2020.

Contributors

Marc Carrel-Billiard
Global Managing Director,
Accenture Technology R&D
marc.carrel-billiard@accenture.com

Lisa O'Connor
Managing Director,
Accenture Technology Labs,
Security R&D
lisa.oconnor@accenture.com

Matthew Carver
Senior Manager,
Accenture Technology Labs,
Security R&D
matthew.carver@accenture.com

Malek Ben Salem
Principal,
Accenture Technology Labs,
Security R&D
malek.ben.salem@accenture.com

Joshua Patterson
Principal,
Accenture Technology Labs,
Security R&D
joshua.patterson@accenture.com

www.accenture.com/SecurityVision
@AccentureSecure

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.
Visit us at www.accenture.com.

12460351