accenture

Strategy | Consulting | Digital | Technology | Operations

Security Technology Vision 2016:

Empowering Your Cyber Defenders to Enable Digital Trust

High performance. Delivered.

Empowering Your Cyber Defenders to Enable Digital Trust

Cyber-enhanced human capabilities are already a reality in some unique situations: Jet fighter pilots, for example, have long benefited from artificial intelligence, cockpit automation and the latest virtual reality visualization technologies to elevate their reaction times and abilities to peak levels.

While that may seem very different from the way security centers operate today, 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 rely on new, more flexible staffing models to make sure they have the "top gun" security expertise they need, when they need it. And underpinning it all will be the mandate to establish a clear-eyed understanding of how effective security is at supporting the business imperative to attain digital trust.

These changes will enhance and scale the security workforce's capabilities to address the growing threat and diversity of digital attacks that enterprises can expect in the coming years. Their combined impact will fundamentally affect the careers and workday lives of security professionals. Consequently, security-focused executives need to understand and prepare for the change that's coming in order to position their companies to survive in the rapidly evolving digital age.

Enterprises will rely on new, more flexible staffing models to make sure they have the "top gun" security expertise they need, when they need it.

Disruptions Drive a Mandate for Digital Trust

New technologies and workforce models, along with the rapid pace of change in the digital economy, raise potent new digital risks. Compounding these risks, the huge scale that gives software much of its power also amplifies the potential problems. Digital businesses will encounter and create risks that traditional enterprises never experienced: new security vectors, for example, and an increased responsibility for consumer privacy. Security professionals will have a stronger stake in supporting the business, shifting from their current internal function to an engaged, customer-focused one, which will require them to attain ever-greater cyber defense effectiveness.

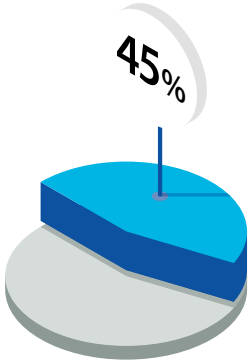
Cyber Threats Continue to Outstrip Defender Capabilities

Technology alone can never resolve all of an enterprise's security threats. To carry out effective cyber hunting, which requires organizations both to understand the full scope of a breach and to seek out indications of breaches as yet undetected, enterprises need to take a "people first" approach. That means focusing not only on attracting highly skilled resources (which remain in short supply), but also further developing the skills within their current workforce.

Neither feat will be easy, but both are essential to cybersecurity success. Recent studies show that up to 45 percent of companies say they have increasing difficulty finding qualified people.[1] That problem becomes clear when cyber attackers overwhelm organizations that are unable to monitor events and correlate threat behaviors because they lack highly skilled people with "eyes on glass" to make sense of it all. One study estimated the average annual cost of cybercrimes to organizations at $7.7 million a year—a figure that increases annually.[2]

And the future looks even more challenging for the already stretched security professional. The growth and connectedness of the Internet of Things (IoT) as it becomes part of the IT network will force companies to deal with sophisticated attacks in higher volumes and across an expanded attack surface. As such, the firehose-sized volume of data flowing into security monitoring systems today—as well as its variety and velocity—will continue to increase. Hiding within this tsunami of data will become even easier for adversaries.

In fact, keeping up with—and rapidly adapting to—the latest attack strategies has become a security imperative. Take remote access trojans, or RATs: Hackers use these seemingly harmless remote support tools to gain control over affected devices, opening companies up to massive fraud attacks, and exponentially increasing risk.[3] What's interesting is how quickly RATs and similar tools are evolving. A cybersecurity firm discovered one that changed its obfuscation methods three times during their eight-month investigation.[4] In that time, the attackers actively tracked the security operations team on their trail using methods that enabled them to monitor the defenders' responses, and employed counter-intelligence to mask and remove activity. Clearly, when attackers can watch defenders responding to their own attacks, they've learned to pivot too quickly for more traditional cybersecurity methods to keep up. To survive this escalating arms race and generate actionable intelligence, enterprises need to arm their people with skills and technologies that can help them reach entirely new levels of performance.



Recent studies show that up to 45% of companies say they have increasing difficulty finding qualified people.

New Business Technologies will Revitalize the Security Workforce

Leading organizations are pushing the boundaries of productivity and smart technology by adopting innovations like intelligent automation and the liquid workforce. These two innovations, coupled with complementary technologies and approaches such as visualization and process automation, are enabling companies to reimagine their business models as agile, continuously innovating value generators. While good for business, these innovations promise to have an outsized impact on the security workforce in two ways. First, by applying artificial intelligence (AI), automation and visualization, intelligent automation will enhance a security professional's capabilities and reduce the ramp-up time needed to gain situational awareness and become an effective part of the security organization.

Second, by making it easier to bring new hires onboard the security organization, these solutions will help reduce the challenges companies encounter in accessing security talent and enable more flexible workforce capabilities such as freelancing or crowdsourcing, where organizations solicit services or ideas from a crowd of people, rather than from traditional employees or suppliers.

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 as they attempt to keep the company's digital assets safe from encroaching attackers. These trends will have a pronounced impact on the ways security professionals approach their jobs.

Understanding the probable implications of these changes will help security leaders position their organizations for success over the next five years. A number of technology breakthroughs will enable tomorrow's security innovations. For example, advances in AI will make it easier to manage the complexity of validating a threat. The introduction of open ecosystems that enable automation will make it easier to apply this technology in security functions. In fact, the degree of automation used between devices will increase, and the application of interactive visualization will significantly expand the professional's ability to interpret and investigate threats.

In addition to making use of major advances in visualization, future security professionals will harness intelligent automation in innovative ways and operate in new, more collaborative staffing configurations, all of which will irrevocably change the ways people interact with security technology and defend against adversaries.

The following perspective looks ahead to 2020 and describes the probable changes security defenders can expect, given the anticipated pace of technological change over the next five years.

Intelligent Automation Steps Up

In their efforts to automate security, organizations will use AI models capable of understanding specific concepts and predicting future actions. Hints of such next-generation capabilities are already emerging. For example, CylancePROTECT uses AI to validate the risks of endpoint behaviors.

Doing so enables it to determine whether anything malicious is lurking and whether the tool should block it. This next-generation antivirus concept thus goes beyond flagging a risk; it actually models how a security professional thinks and validates the threats.

Such models will allow security teams to shift from simply detecting risks to actively identifying threats and enabling automated responses to the activity. Essentially, intelligent automation will turn a proficient analyst into a highly skilled one.

This change will require two things: first, automation that uses AI to identify subtle threats; and second, automated security functions and capabilities that address the threat with a high degree of effectiveness. Equipped with AI-infused process automation, tomorrow's security professionals will be more competent and find it easier to plug themselves into the organization because they will have a common set of repeatable skills that allow them to respond to threats immediately.

How Artificial Intelligence will Enable Visualization

By 2020, visualization will be a core element of enterprise cybersecurity strategy, because it harnesses the innate human ability to recognize patterns quickly and pick out anomalies. Visualization enables 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 can 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 them as actual threats. This information, transformed into a visualization, then goes to the security analyst, who interprets the scope of the damage and investigates. Context will also include a rich picture of the asset—its business value, use, roles, and how it relates to other assets and entities. User experience matters; a good visualization should increase the proficiency and effectiveness of the analyst. It can also help security teams to zero in on appropriate responses to a threat.

Aided by AI, visualization helps organizations understand cascades of data quickly, cutting through "noise" to find clarity. Accenture worked with the US Federal Emergency Management Agency (FEMA) to make sense of decades of data on national disasters, creating a disaster visualization in the form of an interactive geographic map. People can use the map to discover how disasters have affected their own communities. Before this, hard-to-interpret spreadsheets contained all of the data, making it difficult to spot disaster trends and anomalies. On the security side, one North American telecommunications player established a visualization system for processing data to identify botnets and other threat-related traffic. It offered the innovation as a value-added service to the customers using its network.

Today, visualization remains nascent, but within two years, the security professional will be able to visualize the entire enterprise. Within three years, the power of advanced graphics processing units will enable leading organizations to do this in real time. One benefit of this progress will be that today's big data will once again become simply "data" as technology begins to gain the upper hand, enabling security staff to make sense of it all.

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. Imagine a team that undertakes a forensic "dump" of a system (e.g. memory, filesystem, network connections and processes). Using visualization and AI, the system maps out how each artifact in that forensics dump interacts with the other elements.

This approach will enable analysts to not only automate the retrieval of the forensics dump process, but also reveal how to interpret it to identify indicators of compromise, or find other artifacts to search for elsewhere in the organization. By combining AI with security function automation, it becomes possible to either fully or partially automate and guide the process—to the point where ancillary tasks become trivial to execute, thus enabling staff to concentrate on major threats instead of minor issues, and scaling the effectiveness of resource-constrained security organizations.

Automation will introduce new engagement models and give defenders increasingly sophisticated ways to respond to attackers. These will include the near-real-time manipulation of data that subtly changes what adversaries see as they target an organization. Automation will also reduce the time the security team spends focusing on noise. Other intelligent automation benefits include the automated validation of, and response to, common activities such as phishing attacks, and the ability to reduce the number and frequency of these kinds of "block and tackle" tasks.

The use of automation will make many security activities increasingly seamless. Consider a situation where analysts need to interpret information in unfamiliar log file formats generated by new software. While a potential showstopper today, future security tools will make use of intelligent automation to "think" like a security professional and interpret critical information even though they lack access to a schema of the log file. They will be able to contextualize the events seen in the file and correlate them with other events from other logs and devices to understand the larger context. Eventually, analysts will be able to use automated reasoning tools to monitor and even predict the progression of a cyberattack. Accenture has already been working with Invincea Labs on developing a distributed cybersecurity analysis tool for the Defense Advanced Research Projects Agency (DARPA) as part of its Integrated Cyber Analysis System (ICAS) program. The tool automatically discovers all data sources on endpoint devices and then interprets and links data sources, providing a data platform for real-time forensics.

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, intelligent 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 help their people become a more fluid, agile and flexible workforce.

From a security perspective, firms currently face challenges in "onboarding" new staff, particularly when it comes to gaining the institutional context that analysts need to validate and respond to threats effectively. In fact, a 2015 SANS Institute survey reveals that 59 percent of respondents cited a lack of skills and dedicated resources as the main obstacles to discovering and acting on cybersecurity incidents and breaches. The liquid workforce model could be the answer, since the use of freelancers and crowdsourcing are major elements of the approach. In fact, Accenture believes 40 percent of a business' workforce will be freelance by 2020.

Where most companies currently maintain hybrid security organizations using a mix of talent insourcing and outsourcing, in 2020 the liquid workforce model will include innovations like crowdsourcing and broad-based collaboration.

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, enabling companies to benefit from a far greater pool of security experience and expertise than may be available today. This in turn will prompt the need for collaboration and staffing models that support these activities. This trend is already apparent in "bug hunting" activities; going forward, it will emerge in higher-skill functions such as threat modeling and incident response.

Numerous crowdsourcing solutions already exist in the business world, such as CrowdFlower, which enables firms to tap into worldwide expertise to solve complex problems. CrowdFlower claims it has access to data scientists who can help clients build models that are useful in intelligent automation applications. Likewise, Stealth Worker offers a portfolio of security services, and claims it can provide capable security workers "at a fraction of the cost" of traditional full-time employees for short-duration projects—useful for small businesses that may not want to retain people on a full-time basis. Another player, 418 Intelligence, is developing an advanced platform capable of modeling the ways adversaries would attack a specific business or industry. The service uses crowdsourcing to work through probable attack scenarios, giving businesses seeking more brainpower access to leading-edge thinking without having to hire full-time thinkers.

Innovations like intelligent automation often create new cycles of security needs, and the same is true regarding the liquid workforce. While the benefits companies receive from this more collaborative and flexible staffing model could be substantial, they will also have to work through a number of technical constraints in supporting a distributed workforce. For instance, crowdsourcing can provide clear benefits, but can also expose a company to risks. 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, which offers freelance penetration tests via a private network of skilled, rigorously vetted security researchers from around the world. Synack employs specific technologies that help 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 augmented with crowdsourced and freelance labor to meet the demands of the digital business more efficiently and effectively.

Conclusion

To prepare for this security workforce of the future, organizations need to assess where they stand today. When considering intelligent automation applications, companies should determine which security functions are currently staff time-sinks—repetitive and low-impact activities that nonetheless help to sustain security.

Automation could offer opportunities to scale the security workforce's effectiveness in these areas. In a similar vein, the organization should look for security challenges where automated decisions make sense and identify areas where quick action could have a tangible impact on reducing the cost of the security incidents the company faces annually.

With an emphasis on how to exploit the innate capability of humans to interpret activity visually, organizations should look to increase their "visual literacy" and focus on presenting data in compelling ways. They also need to understand what's important in data security, and how to present that information to make it more insightful. Many times, great visualization ideas exist right next door, and security organizations should explore how other areas of the company employ this vital tool.

With these technology enablers in place, security leaders need to consider how the liquid workforce approach could affect their potential staffing models. They can evaluate the areas of security where the organization has traditionally struggled to find sufficient staff; those parts of security that require short-term but highly skilled professionals; or, those that would benefit greatly from access to a larger perspective of the data. Leaders should also explore the potential impact the liquid workforce will have on their industrial supply chain as smaller businesses take advantage of the availability of higher-skill talent to increase their security (and non-security) effectiveness.

The disruptions facing the digital security industry include everything from sophisticated hackers to new business technologies that will change the ways companies work but also expose them to unexpected new cyber 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.

References

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

[2] "2015 Cost of Cyber Crime Study: Global," sponsored by Hewlett Packard Enterprise, independently conducted by Ponemon Institute LLC, October 2015.

[3] "When RATs Become a Social Engineer's Best Friend," Information Week, December 18, 2015.

[4] Mandiant incident response team, discussed during the "No Easy Breach" talk at ShmooCon, 2016.

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.