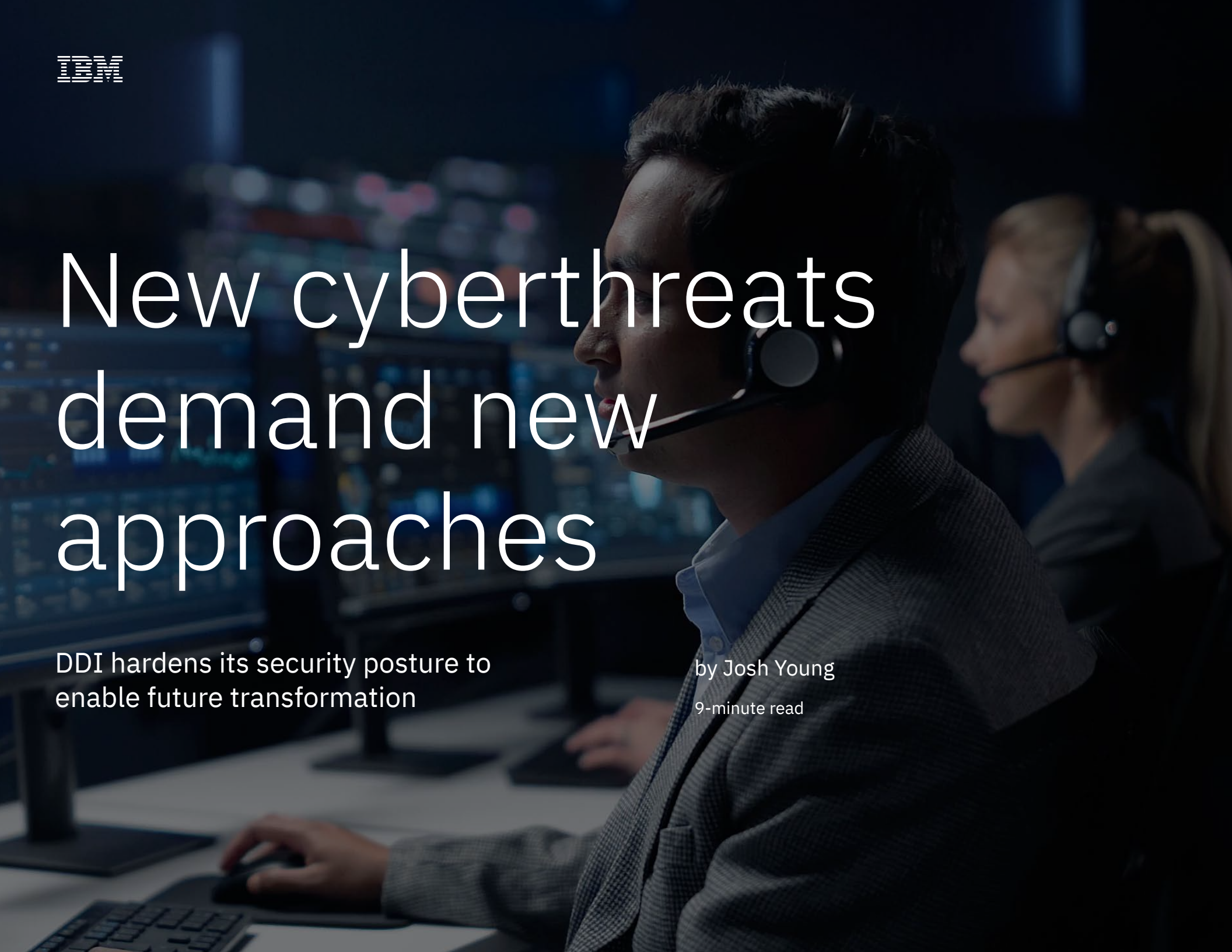


New cyberthreats demand new approaches

DDI hardens its security posture to enable future transformation

by Josh Young

9-minute read

Hey—we're testing out a new reporting tool. Could you click on the link below and run a couple of sample reports? We should have it running on our SSO, so if it asks for a password, just use your network one. Let me know what you think of the tool.

Legitimate email or targeted phishing attempt? That's the question that countless businesses and employees face every day, and as these attacks become more nuanced, telling the difference becomes even more challenging.

~40% of cyberattacks start through phishing

In fact, IBM observed in 2021 that phishing attempts had become the most common threat vector, serving as the starting point for roughly 40% of attacks.

And when criminals and scammers added a corresponding phone call—vishing, or voice phishing—the attempt was three times more likely to succeed. Similarly, ransomware attacks have become a leading cyberthreat, representing 21% of total attacks.

Even more traditional sectors are seeing an increase in cyberthreats—particularly as these businesses begin to explore how digital transformation can deliver a clear competitive advantage. According to IBM research, manufacturing replaced financial services as the top attacked industry in 2021, representing 23.2% of attacks that the business remediated that year.

Manufacturing: the most attacked industry in 2021

So as AI and hybrid cloud become more commonplace on the production floor and analytics-driven decision-making dictates real-time shifts to workflows, hackers and other illicit actors are finding new target-rich environments.

"It takes only one successful hacking attempt to compromise your company," notes Robert Oh, Executive Vice President - Head of Corporate Digital Strategy for the Doosan Group and Chief Operating Officer (COO) at Doosan Digital Innovation (DDI), an entity that provides IT and DT offerings primarily to the Doosan Group. "Or even just one non-malicious action by an employee, like clicking on a link they shouldn't have. And once that back door is open and they're inside, most companies don't know they've been compromised for over a month. That's a lot of time to cause some damage."

"With IBM, we now have an accurate 24-hour view of the world in real time."

Robert Oh, Executive Vice President - Head of Corporate Digital Strategy, Doosan Group and Chief Operating Officer, Doosan Digital Innovation

Envisioned and deployed an integrated, global security infrastructure in

< 1 year

from project launch

Uses SOAR to accelerate threat reactions, cutting

~ 85%

from response times

Changing a culture

In early 2021, along with his role as the Executive Vice President - Head of Corporate Digital Strategy for the Doosan Group, Oh was also appointed to the role of COO at DDI . And with this appointment, he considered the shifting security landscape and how to address it—believing that an effective, comprehensive cybersecurity program should be the foundation of any digital transformation effort. And fortunately, in his new roles, he bore the responsibility for shepherding the digital transformation journey for not just DDI but for the global Doosan Group.

“One of the first things that I mentioned to our top executive team was the importance of protecting our investment in digital transformation,” recalls Oh, “And as you might imagine, it took some convincing to get them to agree to harden our posture. Often security is taken for granted—nothing bad has happened, so nothing bad will happen. But I focused on demonstrating to them that security was a key foundational enabler of our future success. That it wasn’t something that existed alongside our transformation—it was the foundation of it.”

In particular, Oh wanted to shift the Doosan Group to a more proactive, globally-aware security posture. Previously, the company’s security efforts were managed from a business unit or regional level, which made collaboration between security teams somewhat inefficient.

“Across the Doosan Group, we operate in over 40 countries globally,” adds Oh. “With that global scale, you don’t have the time to get your people on the same page. They already need to be there through policies, processes and proactive technology enablers.”

He continues: “I wanted to make sure that everyone across our global security teams was looking at the same, consolidated view of every possible endpoint that we manage under our umbrella. That meant that we needed to build up our perimeter, and we needed to build in global, actionable and real-time visibility.”

Think globally, protect locally

Standardizing and centralizing security policy across 40 countries is not a simple task, as Oh recognizes. “At the start, I told my team that they were about to experience the adventure of a lifetime,” he recalls. “We seldom have transformational opportunities to impact global ways of working, but I knew with the right support, we could make this adventure much more predictable. And we found that support with IBM.”

As a first step, a remote IBM Security® X-Force® team evaluated and identified areas where visibility could be improved within DDI’s established processes.

Then the client’s security personnel coordinated with an onsite IBM Security X-Force consulting team to perform a more in-depth maturity analysis of the group’s global network. And armed with this information, the joint team assembled recommendations that would help further harden security systems and promote global governance that aligns with industry-accepted best practices.

As part of this effort, the DDI and IBM team identified and mapped out appropriate roles and responsibilities of the Doosan staff working within the security infrastructure. Similarly, the joint team engaged in capacity planning for this new security posture while identifying additional use case and incident response runbook options that would help bolster protection efforts.

The joint DDI and IBM team also determined that the Doosan Group would be better served by consolidating

its regional security operation centers (SOCs) to a unified, global SOC. With a more tightly integrated and standardized oversight strategy, the group could establish common performance metrics and more easily coordinate across sites and geographies.

Confident in this assessment, DDI moved forward with the recommended security improvements. The new global SOC, overseen by an IBM Security X-Force team, delivers around-the-clock monitoring and protection under a "follow the sun" model. Throughout each 24-hour period, security responsibility for Doosan's global infrastructure rotates across three IBM sites, aligning managed detection and response (MDR) support with the region most active at any point during the day.

In addition, the global SOC solution provides DDI with ongoing access to IBM industry experts and security consulting support, as well as the latest global threat intelligence. By taking advantage of this regularly-updated knowledge pool, DDI and the Doosan Group can stay better protected against the most recent threat vectors, including those specifically targeted at the manufacturing sector.

To control the operations of the global SOC, DDI worked with IBM to update its core security infrastructure. The team boosted the company's proactive security incident and event management (SIEM) efforts, deploying Cybereason EDR to oversee endpoint detection and response (EDR). The EDR software can quickly identify, react to and remediate potential threats. And IBM also integrated IBM Security QRadar® SOAR technology, delivered from IBM Cloud Pak® for Security, taking advantage of the open platform with the Cybereason EDR solution to deliver AI-based automation that further streamlines threat responses.

"We layered in the SOAR capability so that we could resolve false threat detections without occupying our employees' precious time," explains Oh. "It harmonizes with our global SOC, so we can now focus on what's relevant. And if the system does indeed find a legitimate issue, we can act with agility and conviction."

To drive continued growth, maturity and everchanging landscape, Doosan leverages IBM X-Force advice engagements to continually optimize security strategy, governance, metrics, and operating model. "Our security posture has changed," adds Oh. "Our ability to look at and react to a potential threat has changed. Our culture has changed. And our readiness for digital transformation has changed with the global DDI and IBM team."

" Our ability to look at and react to a potential threat has changed. Our culture has changed. And our readiness for digital transformation has changed with the global DDI and IBM team."

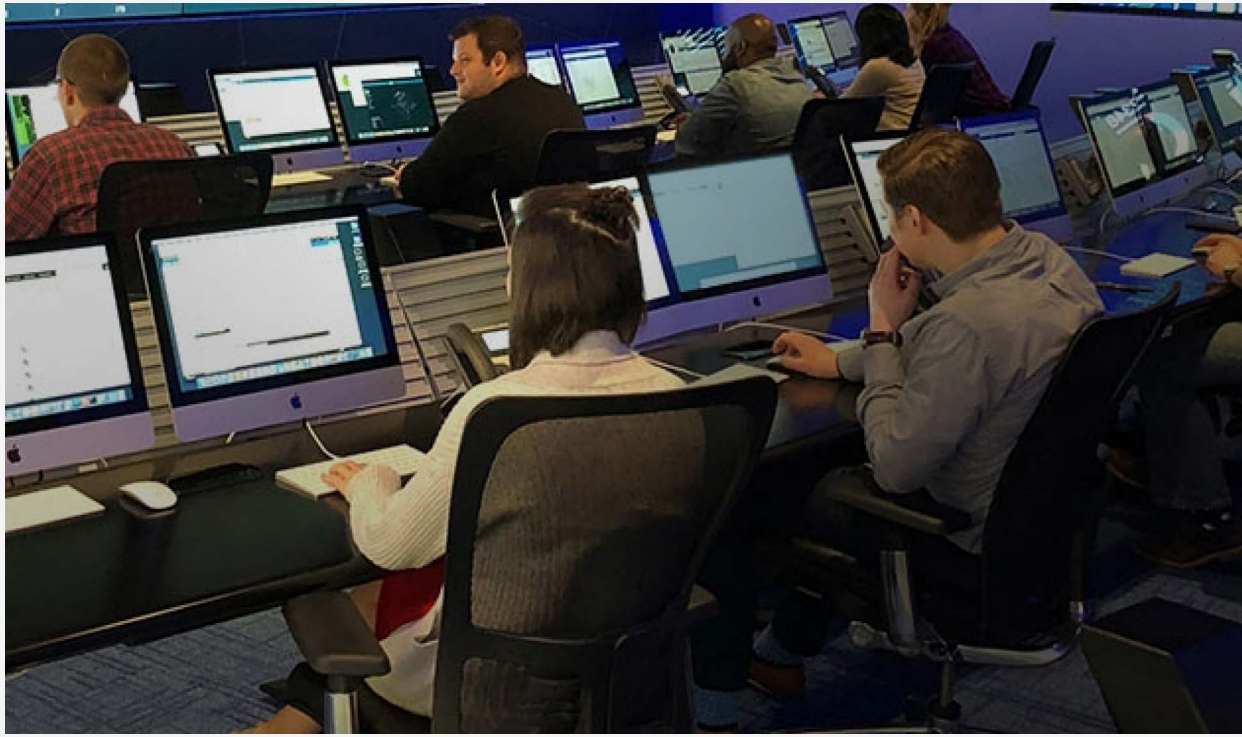
Robert Oh, Executive Vice President - Head of Corporate Digital Strategy, Doosan Group and Chief Operating Officer, Doosan Digital Innovation

See something, do something

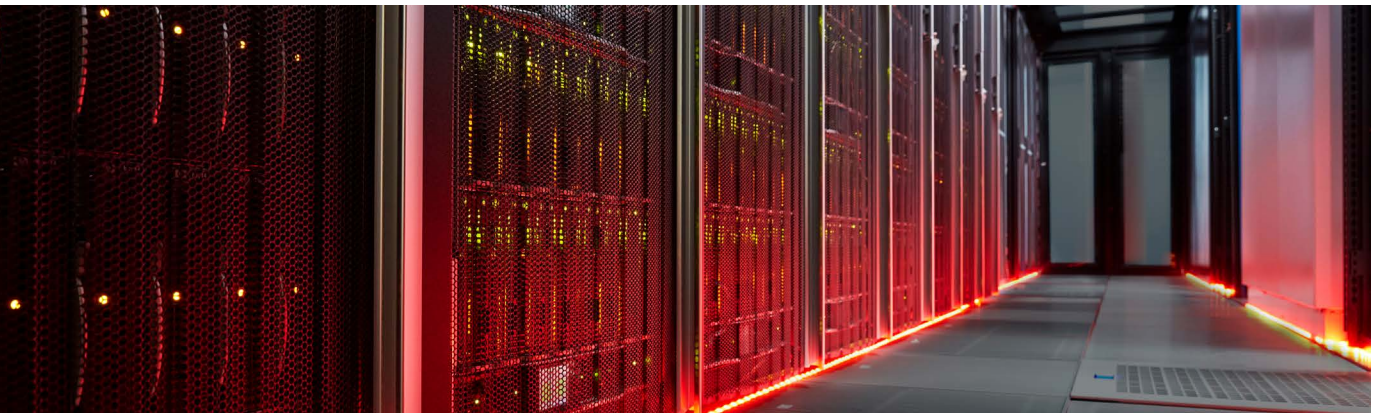
With the global SOC now live, Oh and Doosan feel much better prepared for the future and the present.

Imagine, if you will, that one of Doosan's employees across 40 countries accidentally clicks on a malicious link. Instantly, ransomware begins encrypting the employee's hard drive. Fortunately, Doosan's new EDR solution offers three layers of incident detection, so the platform already notices the suspicious encryption and acts, quarantining the relevant hard drive sector instantaneously.

At the same time, the automated security protocols notify an IBM Security Managed Detection and Response team. And after verifying that this was, in fact, an attack, the IBM team then coordinates with onsite staff to have the affected hard drive reformatted and back online promptly to help minimize business interruptions.



Faster action yields fewer complications



The global, real-time monitoring delivered by the IBM technology and team places DDI in a better position to navigate potential security incidents as they arise. “It’s doing what it’s supposed to,” notes Oh. “With the integrated EDR/MDR, we’re handling a large amount of potential threats each month. And we’re dealing with all those potential attacks without causing any interruption to our business.”

He continues: “And SOAR has also been critical. With the AI-based pattern matching being handled automatically up front, we can detect, decipher and act on incidents much faster, cutting response times by about 85%.”

Alongside the automation, the global SOC provides centralized visibility into the company’s security health and operations.

“We operate in 40 countries, so it’s important that we have a global view,” adds Oh. “With IBM, we now have an accurate 24-hour view of the world in real time. We can see every endpoint, every system. And that’s made our cross-team collaboration much more efficient.”

These standardized efforts also enable consistent, orchestrated threat investigations that deliver increased protection and oversight—all while simplifying reporting, tracking and auditing processes.

Beyond the functional enhancements that the updated security architecture and global SOC deliver, DDI has other reasons to work with IBM. “We did this whole project rapidly,” explains Oh. “I said, ‘I want to get this done in less than a year.’ And due to my global team’s unwavering commitment and IBM’s expertise, we pulled it off.”

Oh also recognizes the thought leadership delivered by the IBM team, as he states: “Our core business competency at Doosan isn’t cybersecurity. So working with global companies to transform Doosan’s cybersecurity culture and posture made sense. That’s why we engaged a global leader who can do the security work, who can focus on sharpening their minds and skills to deal with the everyday threats.”

Further, as DDI completed this project and prepped its digital transformation efforts, the business recognized a broader, cultural impact among its employees. “We’re paying a lot more attention to security,” notes Oh. “We do a lot of internal phishing email campaign training, meaning we send out mock phishing emails periodically to test our global employees. Well, over the past year as we’ve rolled out this transformation, the click rate on those tests dropped noticeably and continuously. And the number of users who were inattentive enough to compromise their password was cut dramatically.”

> “Our core business competency at Doosan isn’t cybersecurity. So working with global companies to transform Doosan’s cybersecurity culture and posture made sense.”

Robert Oh, Executive Vice President - Head of Corporate Digital Strategy, Doosan Group and Chief Operating Officer, Doosan Digital Innovation

The adventure continues

"Working with IBM has made our journey—our adventure— more predictable," adds Oh. "They fit in well with our 3A strategy of reducing ambiguity, building alliances and embracing Agile methodology. And I think that together we've gotten to a point where we can think about where to go next instead of what to enhance."

Some of those next steps are focused on further hardening DDI's security makeup. For example, the company is currently exploring the expanded use of zero-trust security principles. And now that DDI has secured the perimeter of its global network, the company is creating new layers of authentication as users navigate within the architecture.

"So when you're accessing more critical infrastructure or servers, you'll have to further prove yourself," explains Oh. "It will create a much more secure, much more controlled zero-trust environment."

And while DDI continues to reinforce its core security architecture, the business has taken sufficient steps to begin moving forward with its broader digital transformation. As Oh explains: "I'm no longer looking at what we need to do. I'm now looking at what we could do. How do we make things more efficient on the manufacturing floor using technology? How do we incorporate these new security capabilities into the products that we make? How do we use this transformation to create new businesses that we never thought possible?"

DOOSAN

About Doosan Digital Innovation (DDI)

DDI (link resides outside of ibm.com) is accountable for providing IT and DT offerings to the broader Doosan Group (link resides outside of ibm.com), a conglomerate of primarily manufacturing businesses. With a rich history stretching back to 1896, the Doosan Group operates across 40 countries globally, and both it and DDI are currently headquartered in Seoul, South Korea.

Solution components

- IBM Cloud Pak® for Security
- IBM Security® QRadar® SOAR
- IBM Security Managed Detection and Response
- IBM Security X-Force®