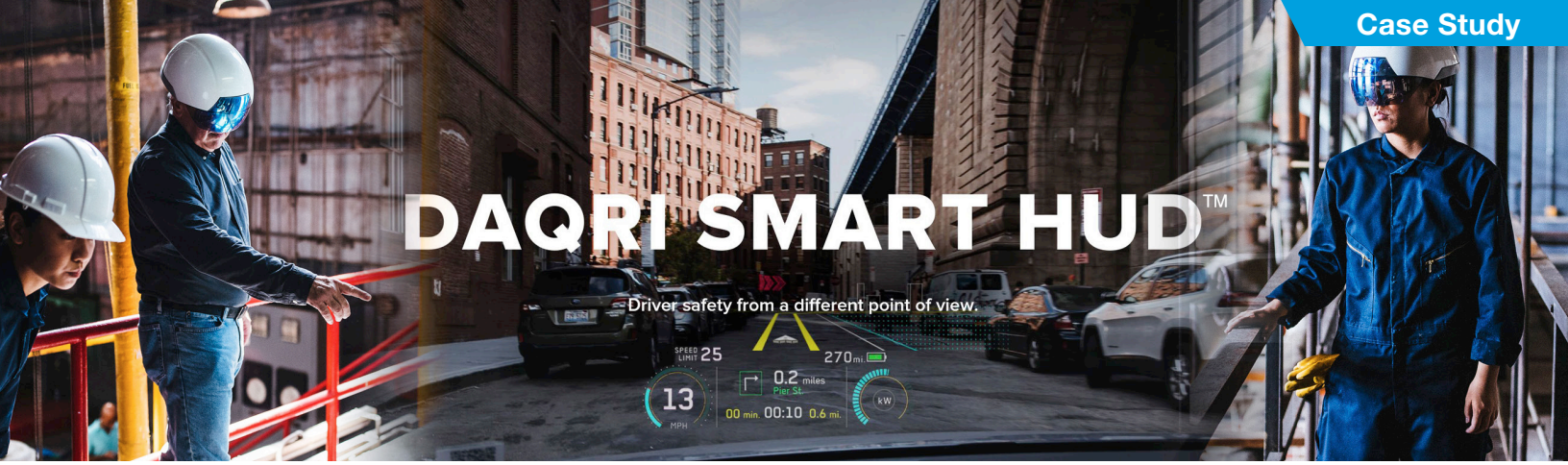
Case Study



Transforming the industrial workplace

AI-powered cybersecurity protects DAQRI's mission to deliver augmented reality to the industrial workplace

Augmented reality promises to transform the industrial workplace, providing workers with maintenance instructions, situational awareness and access to remote experts across oil fields, factory floors, construction sites and other industrial sectors. That's the mission of DAQRI, with its astronaut-like DAQRI Smart Helmet® and other new technologies.

Fueling the next industrial revolution

"My primary focus is to protect our confidential intellectual property responsible for this transformation," says Minuk Kim, director of information security at DAQRI.

As a well-funded startup, DAQRI is moving fast to shape the future. It has a global presence and a cloud-centric mindset.

"We adopt and enable a lot of bleeding-edge technology into our internal and customerfacing products," says Kim. "I need to make sure that we have proper visibility and can respond to security incidents quickly."

The challenge is, as always, one of prioritizing corporate resources.

In his first three months at DAQRI, Kim spent two or three hours every day analyzing firewall, intrusion detection and other security logs.

"I wasn't getting much value out of it," he says. "It was repetitive, manual work that provided little progress toward my ultimate goals of enhancing network, reducing the attack surface, assessing vulnerabilities and protecting our intellectual property."

An overabundance of security events and their tedious, time-consuming analysis is a common lament among cybersecurity professionals.

DAQRI

Organization

DAQRI®

Industry

Augmented reality technology

Challenge

Reduce the time spent hunting for threats

Selection criteria

Automate the hunt for cyberattackers and speed-up incident response using artificial intelligence

Results

- Reduced time spent hunting for threats from hours to minutes
- Protect the development of augmented reality technology
- Prioritize and stop the highest-risk threats before damage is done
- Faster cyberattacker detection and response in the corporate network, virtual private cloud and global offices

VECTRA®
Security that thinks.®

"The reality is that you have too few people to deal with an enormous volume of tasks," says Kim. "How do you approach the problem when you still need to review every incident and resolve them one-by-one, regardless of actual importance?"

Automating the hunt for cyberattackers

Kim knew he needed to find a better way, and he took inspiration from his company's expertise – using technology to highlight and present information that amplifies the worker's efficiency to perform complex tasks.

That's when he discovered the Cognito® automated network detection and response platform from Vectra®.

Cognito offers the fastest, most efficient way to find and stop attackers inside networks. DAQRI deployed Cognito in its corporate headquarters network and global offices. The company also plans to deploy Cognito in its Amazon Web Services (AWS) cloud.

Providing real-time attack visibility and non-stop automated threat analytics that's powered by always-learning behavioral models, Cognito analyzes all network traffic from the campus to the cloud, leaving attackers nowhere to hide.

With Cognito, Kim can quickly and effectively find elusive cyberattackers in the network before they cause irreparable damage.

"It's not that security problems don't exist anymore," says Kim. "But with Vectra, I can focus on attacking problems that have the greatest potential impact. Now I look at a half-dozen events a day. If there's something really important, Vectra will let me know."

Now that DAQRI has successfully automated the hunt for cyberattackers in its network, Kim has reclaimed more than 10 hours a week to concentrate on strategic security initiatives.

Visibility into the cloud

Cyberattackers like to establish a hidden beachhead in cloud workloads to inflict lasting damage.

"The biggest thing in security right now is how to handle the cloud," says Kim. "You don't own the cloud infrastructure; you're consuming a service."

With Cognito, Kim now has the ability to identify advanced persistent threat behaviors within AWS that were previously impossible to detect. For example, hijacking an open server port is the most effective way to install a malicious payload that provides lateral movement between hosts and ultimately data exfiltration. But Cognito detects previously unseen backdoors by monitoring all traffic in the cloud.

Distinguishing anomalies from attack behaviors

"What I love about Vectra is that the technology is adaptive," says Kim. "Technology needs to be adaptive to fit every unique and changing environment."

Every company is unique – and so is its network traffic. What might be a threat in one company's network could be routine in another. Suspicious traffic that is a result of out-of-the-ordinary user behavior is not the same as a threat actor with malicious intent inside your network.

"We have talented engineers pushing the boundaries with new applications of technology," says Kim. "In most corporate environments, port scans and large data transfers to the cloud may be suspicious. But in our environment, it could be normal engineering activity."

"The modern machine learning techniques used by Vectra distinguish between a host that does something every day at 9:05 a.m. because it's a developer's machine and a user whose device has never done that before," he says.

"Vectra easily tells the difference between anomalous user behaviors and attacker behaviors," Kim added. "That lets me focus my attention on the threats that matter most."

With Cognito, detected threats are automatically prioritized and correlated with compromised host devices and key assets that are under attack. Cognito always puts the most relevant information in context at Kim's fingertips.

"Some people say the biggest benefit of Vectra is that it lets you know when something bad happens," he says. "But for me, the real value is the insight we get from Vectra. Knowing what is happening in your network at the packet level is a tremendous advantage when dealing with attackers who always have to go down to that layer to operate."

It's the difference between a flashlight and a bright lamp, he says. "When you turn on the light with Vectra, you see a much bigger surface area. Vectra gives me visibility into all network traffic at any given moment."

Next steps

In addition to extending the reach of Cognito across the global enterprise network, the virtual private cloud and AWS, plans are currently underway to integrate Cognito with DAQRI security orchestration platform, endpoint security and other enforcement points.

VECTRA® Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020 www.vectra.ai