Thwarting cyber threats

Defense contractors need sophisticated security monitoring to protect against increasing threats and new adversaries

THE INCREASE IN ADVANCED THREAT ACTORS and adversaries targeting defense contractors and the supply chain underscores the need for robust security operations to detect and respond to threats.

There have been a wide variety of recent attacks targeting the Defense Industrial Base (DIB), including ransomware, which accounts for 38 percent of attacks against the DIB.

Ransomware is difficult to prevent because ransomware syndicates and affiliates work together to launch attacks, said Saif Rahman, CEO and Co-Founder, Quzara.

"There are multiple types of threat actors and multiple types of users that are part of the ransomware ecosystem, which makes the job of the defender really hard," he said. "You really have to have a strategy internally on how you're going to deal with ransomware."

There are other threats as well, including multichannel phishing where phishing attacks come from various sources such as email, SMS messages and through Word documents.

Security awareness training and products designed to prevent phishing only have about a 70 percent success rate, which means "there is a high probability that one of those phishing attacks will be successful," Rahman said.

As a result, organizations should increase employee awareness, improve the speed and quality of phishing triage processes and implement internal business controls, he said.

Another tactic adversaries use targets user identities, privileged accounts, contractors, and cloud-based services, to gain access to data. Multi-factor authentication and adaptive multi-factor authentication can help organizations protect against this, he said.

Operational technology and cyber physical systems are targets for hackers as well. Around 80 percent of the companies that are part of the DIB have legacy manufacturing systems that may not be secure enough to withstand increasing attacks, Rahman said.

Organizations need a system and environment to mitigate these increasing threats, he said. "In order to build an effective mechanism to counter supply chain, unmanaged end points and indicators of attack, you have to get raw data from a variety of different places" such as threat indicators and geolocation information.

> "Nation state activity is already at your doorstep. All your employee accounts, all your firewalls are being knocked on every day."
>
> **SAIF RAHMAN**
> CEO and Co-Founder, Quzara

Quzara offers a service called Cybertorch, which is a U.S. citizen only, 24 by 7 security operations center (SOC) to monitor, investigate and respond to advanced cyberattacks. It is FedRAMP high ready, and is architected to help customers comply with CMMC, FedRAMP and other compliance requirements.

"Incident response for CMMC and beyond isn't just a policy document that gets checked every three years."

SAIF RAHMAN
CEO and Co-Founder, Quzara

Whether an organization uses an in-house SOC or a service such as Quzara, "they have to start thinking in terms of high value security event monitoring," he said. They have to be able to determine what data to use, analyze it, pair it with specific threat intelligence, and report it.

Cybersecurity should be viewed as "a team sport," Rahman said, where everyone plays a part. "It's not just the SOC, not just the IT guy in the basement. Incident response for CMMC and beyond isn't just a policy document that gets checked every three years. It's critical that people exercise their security incident response plan."

Threat and security operations should be top of mind for companies doing business with DOD, he said. "Nation state activity is already at your doorstep. All your employee accounts, all your firewalls are being knocked on every day."

Defense organizations must realize they are being targeted no matter the size of their company, Rahman said. "You need to start building defenses within your budget constraints, within the people you have and the tools you are given, and get professional help, just to jumpstart your program."

Iaremenko / iStock