QUZARA

Augmenting security teams for a defense-in-depth strategy

Quzara Cybertorch™ enhances an organization's ability to understand and respond to threats

Saif Rahman
Quzara

The defense industrial base (DIB) faces continuous adversary attacks, given its crucial role in national security and involvement in sensitive transactions. Compliance serves as a vital tool, enabling DIB organizations to establish robust security operations. Frameworks like the Cybersecurity Maturity Model Certification (CMMC) outline specific requirements for DIB organizations, placing a strong emphasis on security monitoring, auditing and the generation of security logs. These logs are essential for empowering security teams to understand the threats they face.

Additionally, the CMMC framework includes criteria for incident management and the prevention of data exfiltration, which is particularly crucial when dealing with controlled unclassified information that may potentially leave the organization. Without proper visibility, an organization remains vulnerable to ongoing attacks. For example, if an employee's computer is communicating with a device in a country that is not a U.S. ally, it signals a potential incident that requires investigation. The ability to produce logs that facilitate such investigations is critical for enhancing overall cybersecurity measures.

> "Establishing trust in a security provider is paramount for any organization because it directly influences the trust built with the end customer."

Meaningful analysis and insight into vulnerabilities

As organizations progress through the CMMC levels, aligning with the National Institute of Standards and Technology's Special Publication 800-172 (CMMC Level 3), the emphasis on heightened security visibility is evident by the requirement to establish and maintain a security operations center (SOC) capability, deploy advanced automation and analytics capabilities, and conduct cyberthreat hunting activities. These requirements reinforce the framework's commitment to robust cybersecurity practices that provide meaningful analysis and insights into an organization's vulnerabilities.

As a leading managed extended detection and response provider, Quzara is dedicated to addressing the myriad security threats that organizations encounter. Through our innovative Quzara Cybertorch™ solution, subscribing organizations inherit a comprehensive set of controls covering auditing, logging, incident response and account monitoring.

Choosing Quzara Cybertorch™ means seamlessly integrating robust defense-in-depth measures into your cybersecurity framework. Our team meticulously reviews logs to offer insightful analysis and identify vulnerabilities. But it doesn't end there. We actively collaborate with our customers to craft tailored solutions that ensure a proactive and adaptive security posture. Quzara empowers organizations to navigate the dynamic threat landscape by providing not just a service but a fortified cybersecurity foundation.

iStock

Beyond a one-and-done activity

Quzara provides support through a professional advisory services division that assists organizations in conducting gap assessments and understanding their overall readiness for CMMC compliance. Additionally, our FedRAMP High Ready, 24/7 SOC as a service (SOCaaS)/MXDR, staffed exclusively by U.S. citizens, is anticipated to be the only SOCaaS/MXDR authorized at the FedRAMP High Baseline by the FedRAMP Joint Authorization Board in early spring 2024.

In situations where organizations aiming for CMMC compliance lack a robust IT or security team, Quzara takes a proactive approach. We extend our support beyond mere compliance, working to augment our customers' security teams continually. Our commitment is not a one-time activity focused solely on achieving compliance; it's an ongoing 24/7 operation in collaboration with our customers.

Establishing trust in a security provider is paramount for any organization because it directly influences the trust built with the end customer, particularly in the case of the Defense Department. An authorized FedRAMP High Ready service provider, such as Quzara, differs significantly from providers that offer existing services without undergoing the government's rigorous review process.

When DOD officials observe that a contractor's provider has a robust compliance background, it instills confidence in the contractor's ability to safeguard government data and networks effectively against potential adversaries. Quzara's commitment to FedRAMP High authorization underscores our dedication to providing top-tier security solutions for our clients. ■

Saif Rahman is CEO and co-founder of Quzara.