REPORT REPRINT

SCADAfence parries threats to industrial control systems with visibility and detection

FEBRUARY 15 2019

By Patrick Daly, Jonathan Stern

Over the past several years, ICS security has become one of the more interesting topics in the overall market. With its Continuous Network Monitoring platform, startup SCADAfence offers continuous visibility and asset inventorying on top of guided incident response for large-scale ICS network operators.

Summary

Over the past several years, industrial control system (ICS) security has become one of the more interesting topics in the overall security market. This is in part due to the geopolitical fears of state-sponsored groups targeting critical infrastructure (some of which are overblown), but is mostly in response to the continued convergence of IT/OT systems and the proliferation of connectivity in ICS environments that have expanded the attack surface and left essential cyber-physical systems open to manipulation. The potential for destruction of equipment and injury or loss of life as a result of a sophisticated attack eventually became high enough that organizations began to recognize the need for more robust ICS security.

While incumbent IT security vendors are just beginning to evaluate how they can target this new market opportunity, a class of startups has already been at work for years developing products, building new distribution channels and gaining traction in the sector. One such startup is SCADAfence, whose SCADAfence Platform expands visibility and detects potential threats without thwarting production.

451 TAKE

Aside from continuing to invest in the SCADAfence Platform's core functions of asset visibility and threat detection, the company's emphasis on facilitating smoother incident response (evidenced by its partner strategy and playbooks) is a smart move. While there is a skills shortage across all of IT security, this is likely to be more prevalent in operational networks, where the importance of security only began to sink in over the past several years. As the scale of threats to ICS networks continues to grow, so too does the importance for expert advice on how to investigate and respond to incidents. The challenge inherent to this approach is that valuable incident-response playbooks are labor-intensive to build and require an exhaustive understanding of the vulnerability and threat landscape. This means pulling highly skilled and specialized resources away from more easily scalable areas of the business, but the fact that this process is so labor-intensive increases the value-add for prospective customers. On top of this, SCADAfence's commitment to speed and scalability in the largest industrial environments is key to its growth strategy as the number of connected devices present in ICS environments continues to grow.

Context

Headquartered at the Israel Cybersecurity Center of Excellence in Be'er Sheva with an R&D center in Tel Aviv, SCADAfence was founded in 2014 by VP of business development Yoni Shohet and CTO Ofer Shaked. Both founders previously served in the Israeli Defense Forces, with Shaked gaining his OT security experience in the IDF's Unit 8200 while Shohet led a range of cybersecurity initiatives as a project manager in the IDF's Intelligence Corps. In addition to the two founders, the company is led by CEO Elad Ben-Meir, who was previously VP of products and marketing at Indeni, CEO of Marketteer, and VP of strategic accounts and business development at CyberInt.

In November 2017, the company closed its second round of funding, bringing its total raised to $10m. SCADAfence claims that it has a few dozen active customer deployments. While its primary target customers are large, multinational manufacturers in the automotive, food and beverage, and chemical industries, the company says it also has engagements across hospitality, datacenters and critical infrastructure. In hospitality use cases, it is usually deployed to monitor and protect building management systems.

Products

SCADAfence's flagship offering, the SCADAfence Platform, is deployed as an appliance on a mirror or TAP port in the OT network, where it passively inspects traffic. As the SCADAfence Platform inspects traffic, it automatically discovers and inventories operational assets. Drilling down into an individual asset, customers can view identifying information such as model name, asset name, serial number, firmware version and firmware expansion. An optional active query into a specific asset yields more in-depth data. The SCADAfence Platform also generates a visual map of the network and subnet topology, color coding misconfigured assets to help customers identify and fix any misconfigurations that could expose the system to threats.

In addition to discovering and inventorying operational assets, the SCADAfence Platform identifies potential threats through a combination of techniques. These include behavioral analysis, rules-based detection and signature-based detection, all of which are correlated with threat intelligence to provide additional context around alerts. The company's internally built vulnerability database is also useful for both discovering vulnerable assets and providing further insight into the risk an anomalous event or active malware may pose to network operations. Once an alert is generated, SCADAfence's management system facilitates an automated incident-response process together with integrations with Check Point, Demisto and Fortinet that leverage playbooks developed by SCADAfence. These playbooks walk customer security teams through a step-by-step process for how to mitigate damages, remove a threat, and apply fixes that would prevent the same incident from occurring again.

Via the SCADAfence Platform's UI, customers are shown their full asset inventory (including information about which devices consume the most bandwidth), open alerts organized by severity, a chart tracking new alerts per day, and an overall measure of system health. The interface's responsiveness is a major priority for the company. SCADAfence notes that its goal is to always be able to load a desired page, such as a network map or a deep dive into the communications sent by a given asset, within one second regardless of the size of the deployment. Since the company is targeting large, multinational organizations with tens of thousands of connected assets, the SCADAfence Platform's ability to scale into these environments is critical. The responsiveness of its UI when handling large amounts of data is a key piece of this scalability.

Partners

Thus far, most of SCADAfence's partner strategy has revolved around integrating with existing security technologies to enable enhanced enforcement and incident-response capabilities. The company's most notable partners in this area include Check Point, Demisto and Fortinet, but we could see this list expand to include other security automation and orchestration providers. SCADAfence also partners with Gigamon to enhance its traffic ingestion capabilities and enhance customers' visibility into their network's operational status.

Customers

The company has several public customer case studies, including a medical device factory where it detected malware that had infiltrated the factory via the IT network, identified devices with unauthorized internet connections, and discovered undocumented assets that comprised 60% of the OT network. Other case studies with a German assembly line and body shop and an Asian pharmaceutical company's chemical production line similarly found misconfigured firewalls allowing for unauthorized remote access and a slew of previously undocumented devices. SCADAfence also says it has been chosen by Vestel, a European manufacturer of consumer electronics and home appliances, to secure its production facility, which is one of the largest factories in Europe. In addition, the company claims that it has been picked by Mitsui Fudosan to secure all of the building management systems for the Tokyo 2020 Olympics.

Competition

SCADAfence primarily competes with the cadre of ICS security pure plays that have carved out a meaningful share of the market thus far. These include Claroty, CyberX, Dragos, Indegy and Nozomi Networks. ForeScout also recently planted its flag in the ICS security space with the acquisition of SecurityMatters for $113m. While the base functionality shared among these vendors is the ability to passively discover assets, monitor communications and alert to any abnormal behavior, we are beginning to see firms build additional features in response to market needs. SCADAfence's focus on incident response and its option for active asset queries are two examples of this shift. The use of playbooks to augment security teams' capacity for incident response in industrial environments could draw comparisons with Dragos, while active asset queries are also supported by Indegy and Nozomi Networks. As the ICS security sector continues to mature, support for functions beyond passive monitoring is becoming increasingly essential. In addition, SCADAfence claims that its ability to support large-scale industrial environments while maintaining a low TCO is a core component of its value proposition.

SWOT Analysis

STRENGTHS

The SCADAfence Platform's intuitive and responsive UI makes it easy for customers to prioritize alerts, fix misconfigured assets and respond to security incidents, even in large-scale environments.

WEAKNESSES

Any detection engine using behavioral analytics may be susceptible to false positives, which can contribute to alert fatigue. SCADAfence attempts to mitigate this on the back end with prioritized alerts and automated incident response.

OPPORTUNITIES

Expanding its network of partners to simplify integrations with a customer's existing security architecture could help accelerate customer adoption and improve user experience. The company should prioritize IT security providers commonly deployed in current and prospective customer environments as potential partners.

THREATS

The ICS security arena is already crowded and it could become more cramped with the potential for more IT security vendors to follow ForeScout into the market.