Proficio

When network performance fell at a major North American hospital, it was a sign that years of IT security neglect had led to serious problems. The hospital had developed a reputation as a soft target and experienced daily network attacks. Its weakened defenses also contributed to a poor rating in a pre-audit security assessment.

Today, network attacks have decreased dramatically, the hospital has passed its audit, and they have avoided the expense of building a security operations center (SOC). Threats are now addressed before they become a serious issue, protecting the hospital's reputation.

Overview

California-based managed security services provider (MSSP) Proficio led the turnaround at the hospital, relying on Micro Focus security information and event management tool ArcSight. Proficio's challenge is not only to protect organizations overwhelmed by security alerts, but also to do so quickly and accurately.

"When we become engaged in a proof of concept, we have won every single time. The reason is the accuracy of our alert notifications."

Brad Taylor
Chief Executive Officer
Proficio

Challenge

"The hospital was experiencing more than 10,000 malicious logon attempts each day," says Proficio Chief Executive Officer Brad Taylor. "This was alarming to the hospital. The scans they were experiencing were recurring scans, basically mapping their entire internal network."

The hospital undertook a major network refresh as part of its effort to digitize health records, but security had taken a back seat. Security staff members did not realize the extent of the attacks and network performance was suffering. Staff members using applications with the wrong passwords cached, and users were connecting inappropriately to guest networks and sharing administrator accounts.

For some of Proficio's customers, the problem is not a lack of IT security tools, but not having the resources to properly monitor them. As a result, they become bombarded with unnecessary alerts. Taylor describes some solutions as a "black box," generating plenty of notifications without providing an easy way to quickly separate the most important alerts.

PROFICIO™

At a Glance

Industry

Software & Technology

Location

United States

Challenge

To substantially decrease the rate of malicious network attacks, reduce exposure to compliance problems, and avoid the expense of building an in-house security operations center (SOC).

Products and Services

ArcSight Enterprise Security Manager

Critical Success Factors

- Actionable alerts have been reduced from 1000's to 3-4 per day.
- Response time for a compromised device is now 5 minutes compared to hours or days.
- Threat detection time takes less than 15 minutes instead of 48 hours or more.

The cost of deploying in-house security tools, staff, and other resources can be extremely high. The hospital had considered setting up its own SOC, but this would have required more than a year to complete. Hiring IT security staff can also be difficult and costly. "Right now, it's extremely hard to hire anyone in the security field. In the US, 50 percent of the job postings in IT security go unfilled," observes Taylor.

Solution

Proficio uses ArcSight to provide around-the-clock monitoring. ArcSight's usefulness is twofold—first, it can ingest a large number of security events, allowing Proficio's SOC analysts to monitor a growing number of users and devices. Second, it automatically filters the list of events to identify the threats that matter most, so staff members do not need to manually sift through hundreds or thousands of events. This correlation process translates to threats being identified quickly.

To save time, Proficio uses ArcSight to apply business rules, so the customer can concentrate on the alerts that matter most. For example, Proficio applies acceptable use policies for networked medical devices at the hospital, telling ArcSight which activity is acceptable and which is not.

"I can add a sizeable number of use case correlation rules to ArcSight," explains Taylor. "We have over 300 use case and multi-vector rules firing constantly for all of our customers." This reduces the number of "false positives," so Proficio does not waste time checking unnecessary alerts.

To further improve the speed at which threats are dealt with, Proficio has created modules to automatically block the IP addresses of high-risk traffic. These Active Defense modules work with ArcSight and link to Active Directory and perimeter control devices such as firewalls. This means threats can be blocked even faster, reducing the potential for them to impact operations.

Results

Minimizing Security Noise

Rather than sifting through a flood of notifications, the hospital relies on Proficio for its day-to-day monitoring. The number of actionable alerts has been reduced from thousands to a more manageable three to four per day. The mean time taken to respond and contain a compromised device has fallen from hours, or often days, to about five minutes. The time to detect threats has fallen from at least 48 hours to less than 15 minutes. If a device is compromised while IT staff members are unavailable, the hospital no longer needs to wait for the next shift for the problem to be resolved.

Proficio provides the hospital with daily, weekly, and monthly ArcSight security reports, which allows staff members to monitor group policy changes and statistical anomalies. "This is a true partnership. They're looking at things from a top-end view," says Taylor.

With ArcSight reducing the number of alerts and Proficio taking care of monitoring, customers can avoid spending money hiring analysts to monitor security logs, a monotonous job that typically leads to high staff turnover.

Improving Reputation

The rate of attacks on the hospital was substantially reduced as the customer became more proactive with IT security. "The word got out in the community. The result is what the management and CIO wanted to achieve," Taylor explains. "They went from a position of reactive, blind frustration to one of the most proactive attack responses we've seen in healthcare or any industry." Taylor estimates that it would have cost double for the hospital to set up its own internal SOC.

Global Success

Proficio's approach has seen it consistently grow revenue by 100 percent, for which it was named in the 2015 Deloitte Technology Fast 500. Its reputation has attracted a global customer base, which it services from SOCs in California and Singapore.

Customers include a large semiconductor company that was struggling to manage a growing network without the resources to monitor security events. Proficio detected and contained a targeted attack on this company, preventing intruders from accessing proprietary intellectual property.

Proficio also assisted a large entertainment company that was overwhelmed by alerts despite engaging another security services provider. The customer was using Splunk to investigate incidents, but Taylor says it didn't provide the context needed to prioritize the most important alerts. Using ArcSight and security analysts providing active monitoring, Proficio was able to improve the accuracy of these alerts from 50 percent to 98 percent. The mean time to detect an actionable alert went from 48 hours to less than 15 minutes, saving time and protecting the business.

Taylor attributes the success in part to ArcSight: "When we become engaged in a proof of concept we have won every single time. The reason is the accuracy of our alert notifications. For most MSSPs, about half

“I can add a sizeable number of use case correlation rules to ArcSight. We have over 300 use case and multi-vector rules firing constantly for all of our customers.”

Brad Taylor
Chief Executive Officer
Proficio

Contact us at **CyberRes.com**
Like what you read? Share it.

of their alert notifications are false positives. We have very few misses.”

Proficio demonstrates why being at the forefront when it comes to IT security can protect your business’s assets, its operations, and its reputation.

Learn more at
www.microfocus.com/en-us/cyberres/use-cases/preemptive-threat-detection

CyberRes
A Micro Focus Line of Business