Cymulate
Extended Security Posture Management

How Healthcare Organizations Can Stay One Step Ahead of Ransomware Attacks

Automated Preparedness Safeguards Critical Assets

01 Overview

Healthcare entities of all sizes are fighting an ongoing war against cybercriminals. Over the last few years, Ransomware attacks, in particular, have become increasingly common and sophisticated[1],making them harder to detect and prevent.
Cybercriminals target healthcare primarily out of financial motivation. In this highly regulated industry, the cost of loss or exposure of confidential patient information is high, often resulting in fines and lawsuits. The high cost of data loss and the risk of potentially life-threatening disruption[2] gives cybercriminals confidence that healthcare entities will be more likely to pay a high price to avoid the impact of a breach.

Healthcare security teams have to safeguard new medical technology and protect patient-monitoring equipment, often across multiple locations. And with the COVID pandemic, new ways of interacting remotely between medical staff and patients have created more avenues of attack for cybercriminals. New external threats frequently emerge, creating a constant flow of challenges to the team charged with stopping cyberattacks.

Given the high level of new technology adoption in healthcare, an organization's security team must continuously validate its network security to quickly reveal vulnerabilities caused by misconfigured or non-compliant systems. Typical security validation methods such as Vulnerability Scans, Penetration Tests (pen tests), and Red Team Exercises have become a standard part of assessing security risk, completing security audits, as well as meeting regulatory requirements.
However, to keep up with the pace of change in healthcare IT—both from internal changes and external threats —security validation must occur much more frequently to ensure security efficacy at any point in time, especially against sophisticated, multi-vector attacks.

One of the most practical and effective way for a security team to test their network's security against ransomware and other malicious attacks is to use targeted attack simulations that mimic the modes of attack used by the criminals themselves. These kinds of simulations are known as Breach and Attack Simulations (BAS). By combining frequent BAS simulations with other security testing methodologies, a security team can build a security validation program that can match the pace of change in their network while also assuring their system can defend against the latest threats. This paper examines the benefits and costs of commonly used security testing and validation tools.
It also recommends the addition of automated BAS security validation at a cadence required to assess your security in the dynamic environment you operate in.

[1] https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf.
[2] Patient in Germany dies because of a ransomware attack.

02 Business Problem

Ransomware: a Growing Threat to the Healthcare Industry

Probably no other security threat keeps a Chief Information Security Officer up at night more often than ransomware. This is especially true in highly-regulated industries such as healthcare. Safeguarding access to private client information is not only a central part of doing business. But the costs of losing confidential data-or having such data released to the public—can be disastrous. And while successful attacks can result in large fines and even lawsuits, the costs are not only financial. A recent ransomware attack at Universal Health Services (UHS), one of the largest healthcare providers in the US and Europe, shut down the entire network at dozens of sites across their network. Doctors could not view patient records, access test results, or perform vital procedures, leaving them in a worst-case scenario: doctors could not provide critical patient care.

The cybercriminals who attempt to steal or encrypt a hospital's confidential information are not individual hackers working out of a basement. These are organized criminal enterprises, dedicated to finding new ways to to breach a network undetected. These groups automate their attacks and follow a known kill chain to uncover common security vulnerabilities. They choose their targets based on the availability of vulnerable systems and stolen credentials to ensure the attack has the highest likelihood of success and the potential financial return on their investment.

Healthcare security is both highly sophisticated and extremely complex. Given that healthcare security must cover a wide range of devices—from devices based on legacy operating systems that leave them prone to exploitation, to a constant stream of new medical equipment and an increasing variety of remote endpoints—most healthcare companies invest in state-of-the-art security to stay ahead of attackers. But high complexity combined with best of breed point products creates management challenges.

A security group can implement the best protection available, but regular network changes and new threats can result in security drift, exposing or creating new, exploitable vulnerabilities.

A properly configured, multi-layered security architecture, rapid detection capabilities and robust incident response program will reduce the likelihood of a successful ransomware attack. Fortunately, the tools exist to ensure that your security technology, people and processes function optimally at any time. New Breach and Attack Simulation (BAS) products have come to market that provide continuous, automated, multi-vector security control validation. These products simulate attacks along the entire kill chain, using the techniques that the criminals themselves use to expose any vulnerabilities that have surfaced due to internal changes or newly-developed external threats. These tests probe the strength of your defenses and offer remediation guidance if any weaknesses appear. In this paper, we will examine the tools that most companies use to assess the efficacy of their security, the additional capabilities now available with BAS, and a recommended cadence for using the full range of tools at your disposal.

03 Business Need

Stopping Ransomware Attacks Before Payload Deployment

Today's standard practice for security validation consists of four well-defined processes: Security Audits, Vulnerability Scans, Pen Tests, and Red Team Exercises. These methods, if performed regularly, help the security organization answer a variety of questions.

Security Audits: Security Audits examine overall security strategy and assess whether all of the proper controls and processes are in place to prevent, or respond to, an attack.
A regular Security Audit creates a firm foundation for any successful security program. And while security testing is a cornerstone of a healthy security program, the audit itself does not validate an organization’s security posture.

Red Team Exercises: Red Team Exercises mimic "real-life" attacks and evaluate the security team's response to any breaches that occur. These tests are especially helpful for gauging the effectiveness of a team’s incident management procedures. While costly and time-consuming, the benefits of Red Teaming are tangible, particularly for improving a team’s response to real-life attacks.

Vulnerability Scans: Vulnerability Scans check for known weaknesses. These include known vulnerabilities in networks, software bugs in host systems, missing operating system patches, insecure default configurations, and web application weaknesses. While these scans help automate a vital element of a healthcare organization’s security posture, their findings can be overwhelming. They can also include false positives because they do not take into account, nor do they validate, protections supplied by compensating controls.

Pen Testing: The de facto method of meeting the HIPAA Security Rule requiring a periodic assessment of how well an organization's security policies and procedures meet its requirements. Pen testing provides realistic, actionable results to mitigate uncovered vulnerabilities and weaknesses.
However, pen tests offer only a snapshot of your network defenses. They are also costly and time-consuming, making it unrealistic to perform them with the frequency needed to provide continuous security validation.

While valuable and necessary, these tests cannot confirm that your security architecture will always work as designed. They do not give the regular visibility, validation, and assurance required to know if your security infrastructure is at its optimal state on any given day.
If testing frequency can't keep up with the rate of change (internal or external), your network is vulnerable during the "gaps" between tests.

04 Solution

Expand Current Security Assurance Program with continuous security validation

To ensure your security architecture is protecting your organization effectively, we recommend expanding your security assurance programs to include BAS-based continuous security validation. Frequent assessments reduces any exposure caused by security drift during "gaps" between manual penetration tests delivering tangible benefits that increase overall security effectiveness:

Increased visibility: BAS provides visibility into the entire security environment, giving real-time insight into potential security gaps. This visibility identifies your organization's strengths and weaknesses, enabling you to allocate resources effectively and make targeted procurement. Increased visibility and attack context also help to prioritize vulnerabilities so that they can be addressed before an attack occurs.

Security optimization: Multi vector attack simulations enable security teams to optimize their security controls efficacy and incident response capabilities. They are continuously updated to match the pace of the evolving external threat landscape, always searching for new threats that bypass existing policies and defences.

Security assurance: Automated assessments can verify that network changes or changes to security controls have not opened up new windows of attack for cybercriminals to exploit. As the team deploys new medical devices, moves servers, updates security hardware or software, BAS ensures your security controls are functioning as expected. These assessments verify that your security policies are enforced correctly and look for "unintended consequences" of changes made to the network by the entire IT organization.

To meet the pace of threat evolutions and business driven changes in IT we recommend adding the following four types of automated security risk assessments:

Policy Enforcement Validation: Policies frequently change in response to changes in your network. A timely example is the impact of Covid-19, which has forced healthcare organizations to support a larger remote workforce and subsequently modify policies and their enforcement.

This form of validation verifies policy enforcement across the entire system, examining access controls, the configuration of new medical device security controls, user-onboarding policies, and unexpected effects of network maintenance. This test also validates policy enforcement due to any internal IT changes. For example, this test verifies that the correct network segmentation policies are in place between classified networks and non-classified networks.

Purple Team Automation: Purple Team Automation enables security teams to craft and launch attack flows to exercise threat hunting and incident response capabilities. Automation makes Purple Team exercises accessible and achievable for security teams with minimal adversarial skills by leveraging out-of-the-box attack scenarios. Sophisticated customizability enables companies with in-house red team or pen tester resources to scale the expertise of these individuals by leveraging automation, without limiting their creativity.

Security Control Validation: This assessment subjects security controls to a broad spectrum of attacks and threats. It validates the efficacy of the security controls and provides guidance for optimizing them. For example, this type of test measures the efficacy of security compensating controls put in place to protect devices that may have outmoded built-in security or may be waiting for the manufacturer's approval to install a patch to fix a software vulnerability.

Threat Intelligence-Based Assessments: Cybercriminals never sleep. A vital part of any security assurance program requires validation testing against novel threats. This test allows you to stay abreast of the latest attack vectors and methods, prove your ability to prevent new attacks, and expose any vulnerabilities caused by these threats. It provides you real-time visibility into the state of security against the evolving threat landscape, optimizes your security controls against new threats, and reduce security drift, letting you stay ahead of the latest attacks before the criminals deploy them against you.

The following table provides an overview of the above tests, along with guidance for a recommended cadence to fully protect your network.

05 Recommended Security Assurance Programs and Frequency

Security Audit Yearly	• A technical assessment of an organization's IT infrastructure • Policy review and audit	• Review security assurance program • Identify new strategic investments
Red Team Exercise Yearly	• Mimics "real-life" attacks evaluating team response • Valuable for threat detection and response process improvements	• Stress-tests organizational processes • Costly and resource-intensive; may inhibit adoption by smaller healthcare organizations
Pen Testing Yearly to Quarterly	• Manual attempt to penetrate the network • Exposes vulnerabilities; identifies areas of weakness • Results provide a snapshot in time	• Combined with continuous security validation can automate time consuming processes
Vulnerability Scans * Monthly to Weekly	• Does not take into account compensating controls and lacks attack path context	• Scans the IT infrastructure for known software vulnerabilities • Automated
Purple Team Automation * Weekly to Daily	• Frequently exercise and validate incident response playbooks • Validate SOC rapid and accurate detection capabilities	• Exercise pro-active threat hunting • Scale in-house security-offense skills
Policy Enforcement Validation * Monthly to Weekly	• Verifies effective network policy enforcements • Discovers inadvertent impairments due to IT changes	• Requires customization to match the unique environment and policies • Automated
Security Control Validation * Weekly to Daily	• Validates security control efficacy • Provides actionable guidance to optimize security controls • Automated	• Provides visibility to establish, measure and track security KPIs for efficient resource allocation and targeted procurements
Threat Intelligence Based Assessments Daily	• Validates security efficacy against emerging threats • Identifies latest attack vectors • Helps prioritize patching efforts	• Provides actionable remediation guidance • Automated

Figure 1

*Depends on the frequency of change in the IT infrastructure, policy changes, changes applied to enforcement points, and security controls.

06 Conclusion

Recommended Security Assurance Program Elements and Frequency

Healthcare entities that have implemented such a program have achieved tangible and quantifiable results. According to a recent survey of Cymulate healthcare customers, during the first nine months of 2020 customers performed, on average, 3.04 Immediate Threat intelligence assessments a week. During the same period, these customers averaged 1.21 Endpoint Security Control validation assessments a week, improving effectiveness over time.
For example, one major healthcare and private hospital provider halved their risk score, dropping from 34 to 17 (on a scale of 0-100 where 0 represents the lowest risk).

By implementing a Security Assurance Program that includes all of these tests at the proper cadence, the security team can prevent even the most complex and sophisticated ransomware attacks. When defining your validation program, the guiding principle is to schedule tests in response to the rate of change in the internal or external environment. The only practical way to keep pace with the frequency of change in today's healthcare environment is to make use of automated BAS testing. To learn more about the Cymulate BAS platform and how to build a more effective Security Assurance Program, visit www.cymulate.com.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate continuously enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

Contact us for a live demo, or get started with a free trial

Request a Demo