WHITE PAPER

Attack the Attacker

HOW A MANAGED SECURITY SERVICE IMPROVES EFFICIENCY AND SAVES COST
Table of Contents

THE SECURITY MAZE ......................................................... 3
THE CHALLENGE .......................................................... 4
THE IMPORTANCE OF MONITORING .................................. 6
RAPID INCIDENT RESPONSE IS CRITICAL .......................... 7
COST-EFFECTIVE SOLUTIONS .......................................... 8
LEIDOS MANAGED SECURITY SERVICE ............................. 9
LEIDOS CYBERSECURITY SOLUTION ............................... 10
The Security Maze

You need your organization to be different. You need to catch these intrusions and repel them before they can be successful. And you need to do this in minutes, not months.

Your organization has spent a lot on cybersecurity. Your security is complex, expensive, and hard to operate and maintain. You have painstakingly put the layers together so everything is defended and protected.

Yet, you stay up nights wondering:

“Have I done enough?”
“What happens when my organization is attacked?”
“Will the defenses work as they were designed to?”
“Have we been attacked already, and just don’t know it?”
“Are we being attacked right now, and can’t even see it?”

It’s an uncomfortable situation, made more uncomfortable as you read articles and watch news reports of devastating security breaches striking so many healthcare organizations. You are bothered by that nagging feeling that maybe … you are missing something.

Most likely, you are missing something.

For most of us, the reality is that the system of security controls that we have painstakingly deployed are like a maze that slows attackers down, but does not actually stop them. Skilled attackers are able to leverage tools, techniques and time to slowly penetrate our defenses, one layer at a time. And if we do not catch them in the act, identify their techniques, and remove them from the enterprise, they will eventually navigate the maze and accomplish their goals – all at our expense.
The Challenge

The challenge of the security maze is well known, well-understood, and well-documented by the experts in cybersecurity.

The Ernst & Young Global Information Security Survey 2013, “Under cyber attack” begins with this chilling observation:

“In the time it takes to review this report, a significant percentage of readers will learn of an attack that will have breached their organization’s security. The infiltration could have occurred days, weeks or even months ago – and they didn’t even know it. When the knowledge and magnitude of the breach does surface, the associated costs to the organization may be staggering.”

Mandiant, in their 2013 Threat Report, speaks to the danger of the “Security Gap”:
“There is no such thing as perfect security. Advances in technology will always outpace our ability to effectively secure our networks from attackers. At Mandiant, we call this the ‘Security Gap.’ There is no technical or legislative solution that can eliminate this gap. Security breaches are inevitable because determined attackers will always find a way through the gap. This sounds disparaging, but it is not new information. Seasoned security professionals have been aware of the security gap throughout their careers.”
Verizon, in their 2013 Data Breach Investigations Report, emphasizes the importance of detection of threats:

“Picking over the remains of breach victims might paint a grim picture of our current state, but it’s not a hopeless one … We strongly recommend readers consider the detection of failures [in a reasonable time frame] as a success. The security industry has long been overly focused on prevention. Let’s keep preventing, but enhance our ability to detect threats that slip through our defenses [which they will inevitably do].”

A February 2014 article in Healthcare IT News shines light on breach data in healthcare:

- 29.3 million patient health records were compromised in a HIPAA data breach since 2009
- 138 percent more health records have been breached from 2012 to the present.
- Breaches involving the health records of fewer than 500 individuals are not required to be publicly reported, which skews the final numbers.
- Lisa Gallagher, senior director of privacy and security for HIMSS, said speaking at the 2012 Boston Privacy and Security Forum, that somewhere between 40 million to 45 million patient records have actually been compromised.
- Many of these breaches, officials say, can be easily avoided through regular risk analysis and updating company policies, including a remediation plan that significantly lowers your risk of breach.

Experian, in their 2014 Data Breach Industry Forecast, projects even greater breaches to come:

“The healthcare industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches in 2014. The sheer size of the industry … from local physicians to large hospital networks, provide an expanded attack surface for breaches.

“Healthcare data is valuable, and that makes it a target. On the black market, personal records suitable for use in identity theft are worth $10-$12 each at the low end or maybe $25-$28 for a particularly attractive identity, he said. When enriched with health data, the value of an identity data set jumps to about $50 per record, because then it can be used for medical and insurance fraud.”

With all these thoughts in mind, your organization needs to build not just a maze, but a trap that catches your adversaries and stops them cold.
Mandiant notes in their 2013 report that the median number of days from the earliest evidence of compromise to the discovery of the compromise was 243 days. That is the median – meaning that half of the incidents they investigated went on for more than 243 days. That’s about eight months where an attacker is inside your network, moving around, accessing your systems and examining your defenses. That attacker is researching your networks, computers, people and operations to find what they want, defeat your security, and get away with it before you even notice they are there. And eight months gives them a lot of time to do their job very well.

The difference is visibility. You have to be able to see the intrusions to stop them. And that’s where monitoring comes in. We need to remember that these attacks are perpetrated by people, and that these people are not simply going to give up and go away when they run into defenses.

Our adversaries are competent, smart, creative and clever, and they truly have nothing else to do except figure out how to breach our defenses. But defenses alone are not going to stop them. They will only be stopped by other people who observe, analyze and respond to their actions, and repel them from the enterprise.

Monitoring makes this possible. Monitoring – with 24x7 response – raises the alerts that allow your people to go into action, and stop your adversaries before they can succeed. Does stopping an attack this way make you successful? Yes it does, but just for one day. Rest assured that the adversary will be back again tomorrow, trying again with new techniques, new tools, and from new locations. Only with constant vigilance and constant response will you truly protect yourself.
Rapid Incident Response is Critical

The longer an intrusion is allowed to persist, the greater the damage. So it is critical to detect, identify and stop intrusions as quickly as possible. Timely response requires correlating data across a large number of enterprise systems, using that data to identify patterns that indicate malicious activity, and then using that knowledge to formulate an effective response. All this takes time.

With rapid incident response, this process is compressed down to the shortest time possible. This is done by empowering the team to assess, contain and remediate the incident all at once in a well-orchestrated and well-rehearsed process. This allows you to respond as quickly as possible and reduces the time available to the attacker.

A rapid incident response capability compresses the time needed for incident identification and response from days to minutes. This capability dramatically limits or even eliminates the damages and losses incurred by our customers.
So far we have discussed the challenges of building effective security, detecting modern attacks and responding in a timely manner. The biggest hurdle to meeting these challenges is of course: cost. An effective detection program requires sophisticated and expensive technologies operated by trained staff who are watching and responding 24x7. For all but the largest of organizations, these costs can rapidly become prohibitive.

**When calculating monitoring and incident response costs, you should include:**
- Security Incident and Event Management (SIEM) technology
- Event collectors and storage (may be separate from core SIEM)
- Interfaces, connectors and custom middleware, if required
- System licensing, installation, operation, maintenance and depreciation costs
- Staffing for 24x7 coverage for monitoring and incident response (it takes five staff working 40-hour weeks to cover a single position 24x7)
- Computer forensics and investigation expertise
- Staff supervision, management and engineering support
- Annual system tuning, upgrades and enhancements
- System audits, compliance validation, and reporting (if required)

If you are a large healthcare organization with numerous locations and networks, thousands of users and devices, and a large and sophisticated IT staff, you may want to incur these costs and make this investment in your security. For smaller organizations, these high fixed costs do not make always make financial sense.

With cost in mind, you should consider a managed security service. With a managed security service, your service provider incurs the fixed costs, and then spreads them out across multiple clients, providing everyone with higher quality results at a more economical price. With a managed security service, you replace high capital costs with a simple expense, and you get the benefit of a comprehensive security team that is fully-trained, well-equipped and primed to respond to incidents when they occur.
Leidos Managed Security Service

Leidos monitoring experts have successfully identified attacker behaviors and indicators of compromises, and used that information to protect our customers from advanced threats. Our forensics and incident response teams deploy around the clock to analyze, diagnose and mitigate incidents on some of the nation’s largest military and commercial enterprise networks.

Our managed security customers are given a customized portal that provides 24x7 situational awareness into their security operations. This portal includes modules for security incident reports, analyst investigations, managed asset inventories and configurations, document repositories, and detection documentation.

Leidos’ own global network is a tremendous test bed for our solutions, services and technologies, and includes diverse operating environments across multiple zones of security. In our own environment we support over 20,000 active users and 50,000 devices, all with secure protected access to the global Internet.

Anticipate
Actively apply threat intelligence

Detect
Sense variances to data, system and network

Defend
Shield against real attacks

Protect
Safeguard key business assets, processes and data

Respond
Act and communicate in real-time to attacks

Recover
Fight through attacks and quickly restore operations
Our cybersecurity solution is one that is developed and customized for each client according to their unique situation and operational requirements. The Leidos threat intelligence team works to maintain awareness of adversary tactics, techniques and procedures (TTPs) and uses this understanding to take a behavior-based approach to threat detection across all steps of the cyber kill chain. We inspect communications links for indicators of adversary behavior whether it is cyber weapon delivery, installation, lateral movement, command and control, or data exfiltration. In your environment, we will tailor these Indicators of Compromise (IOCs) for your network and applications in order to ensure the highest probability of catching intrusions before they can do harm.

Leidos collaborates with your organization to develop a proactive plan that minimizes vulnerabilities, extends detection, prioritizes threats, establishes prevention, and refines security processes to deliver better visibility and control of information security risks. Regardless of the size of your organization, the Leidos cybersecurity solution can help you manage and protect your IT assets and sensitive data without incurring the costs of standing up your own in-house enterprise security operation.
ABOUT LEIDOS AND LEIDOS HEALTH

Leidos is a new company formed from the separation of FORTUNE 500® company SAIC on Sept. 27, 2013.

For more than 25 years, Leidos has provided critical information security services for the United States military and federal government. By combining this deep security expertise with our healthcare experience, Leidos Health is helping healthcare organizations manage and protect IT assets and sensitive data. Our security solutions span the full lifecycle and include security education, security management, incident response, monitoring and remediation, and risk assessment.

Leidos Health helps healthcare organizations achieve their goals of meeting regulatory requirements, improving quality of care, reducing costs and enhancing the patient experience. Its services include implementation and optimization of EHRs for all major vendors, as well as solutions for critical initiatives such as IT strategy, revenue cycle, clinical optimization, cybersecurity, Meaningful Use, ICD-10, technology infrastructure, and project management. Previously part of SAIC and including the former companies of maxIT Healthcare and Vitalize Consulting Solutions, Leidos Health is a new company with uncommon capabilities and a 40 year legacy of success.

For more information, visit leidoshealth.com.