Brought to you by:

KEYSIGHT TECHNOLOGIES

Breach & Attack Simulation

for dummies®
A Wiley Brand

Simulate the cyber attack kill chain

Continuously validate your defenses

Remediate gaps in your security

Keysight Technologies Special Edition

Jeff T. Parker

About Keysight Technologies

In 1938, Bill Hewlett and Dave Packard used a Palo Alto garage to build their their first product, an audio oscillator. Later used in Disney's groundbreaking movie Fantasia, that first product set the stage for Keysight's focus on the potential of using new technologies to see the unseen and test the untestable. With the 2017 acquisition of Ixia, Keysight added decades of experience as the source of truth for network equipment makers andnetwork operators to the portfolio. Recent security innovations like Threat Simulator, with a "hack yourself" approach, mean that previously unmeasurable things like an organization's security posture were now measurable and testable, allowing you to not only understand how effective your security efforts have been but also how to fill any gaps you discover.

Breach & Attack Simulation

Breach & Attack Simulation

Keysight Technologies Special Edition

by Jeff T. Parker

for dummies®
A Wiley Brand

Breach & Attack Simulation For Dummies®, Keysight Technologies Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-69968-2 (pbk); ISBN 978-1-119-69971-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner
Editorial Manager: Rev Mengle
Associate Publisher: Katie Mohr
Business Development Representative: Karen Hattan
Production Editor: Siddique Shaik

Table of Contents

Introduction

It seems cliché to say, but these statements are truer today than ever before:

- Your environment is increasingly complex.
- Attacks are more sophisticated and frequent.
- IT is too often reactive rather than proactive.
- Organizations need better intelligence — both about the traffic on their networks and about the external threats they are facing.

The ever-changing landscape of attacks on increasingly complex environments make a compelling argument that you need to take a proactive approach to security. This book covers that approach from beginning to end.

About This Book

This book covers attacks on your network. No, not the ones you expect — these are actually coming from *you.* The best way to know you're protected is to attack *yourself*. Imagine the ability to safely execute attacks on your own security environment to find the gaps, misconfigurations, and insecure policies.

It's time you took this proactive stance for defense, discussed in seven short chapters, each summarized here:

- **Chapter 1:** Learn about breaches and see your active defense as the big picture.
- **Chapter 2:** Measure your environment's security posture.
- **Chapter 3:** See how taking an active approach differs from a passive or reactive approach.
- **Chapter 4:** Learn how to take and keep the "high ground."
- **Chapter 5:** Establish your baseline and go forward.
- **Chapter 6:** Read ten important tips for breach and attack simulation.

A glossary ends the book with keywords and terms.

Icons Used in This Book

Throughout the book, a few icons will grab your attention. The icons offer more than a distraction away from the normal text. What they offer may be a valuable detail, additional technical context, or maybe something that makes your work go even smoother.

TIP

This icon tells you a juicy tidbit or recommendation related to the text. Collect these suggestions for easy reference later.

REMEMBER

This icon points out something important to remember, or something to recall from the last time you heard it.

TECHNICAL STUFF

Ah, something cool that will resonate with nerds, the geeks . . . you know, security staff. Bring these tidbits up casually at the next holiday party and you'll be the favorite of the crowd.

WARNING

As you might suspect, this icon denotes something to remember. And not in a charming way, but rather in a risk mitigating way. Take heed not to bypass this icon!

IN THIS CHAPTER

- Taking stock of the current situation
- Being threat-smart
- Testing your defenses where it counts
- Attack simulation impact on remediation

Chapter 1
Introducing Breach and Attack Simulation

The opportunity to secure ourselves against defeat lies in our own hands.

— SUN TSU

This chapter narrates the big picture of network defense and breach and attack simulation. Its sections cover specific aspects of the what, when, and how.

Evaluating Security Effectiveness

One of the challenges of assessing security effectiveness is that it has been hard to quantify in the past. Your security was either effective, meaning that you had not been breached, was not effective because you had been breached, or worse, you thought it was effective simply because you didn't know you had been breached.

Security teams have focused correctly on prevention and detection of attackers. With those technologies and processes in place, it has become critical to obtain a repeatable and ongoing measurement of your security posture in this production network. This would also provide you with an understanding of gaps and

ideally, in cases where gaps were found, some sort of guidance on how to address those gaps.

When you find gaps

When you find gaps (the question is *when* you'll find them, not *if*) it is one thing to know that you have an issue. It is another thing entirely to be provided with actionable intelligence. Knowing how to fix the problem ("Firewall Rule 1 is not turned on; turn it on and stop that attack") is far more useful than simply being alerted to that problem.

Through the lens of attackers

The path to protecting your IT environment, personnel, and business is through the lens of the attacker. Step into their shoes and ask yourself "What would I do to exploit that?"

The risk of staying ignorant of today's exploits and attack techniques cannot be understated.

REMEMBER

"Over half of the most common security vulnerabilities exploited by criminals to conduct cyberattacks and distribute malware are more than a year old, and some are over five years old" (ZDnet, February 4, 2020).

Attacking Yourself, Before They Do

When was your environment last breached? Has the breach even been detected yet? From containment through recovery, were you reasonably prepared? And now, how well are you prepared to handle the next one?

These questions cut to the chase for most CISOs. From discovery through incident response, containment, and recovery, the race is on. Business must resume quickly and confidently. For you, there's no tolerance for panic and no time for preparation.

REMEMBER

In a recent Keysight survey, 75 percent of respondents said their company had experienced a security breach and nearly half (47 percent) reported they experienced three or more breaches in the past three years. Underscoring the significance, a February 2020 survey by Security.org revealed one in four Americans won't do business with companies whose data was breached.

The issue is no longer *if* an attack will occur, but *when.* It's less important to discuss what happened and more important to prepare for the next time. Attacks will happen again.

Nothing validates your defenses like putting them to the test. When the security team assures you all is well, you can take their claims in good faith. However, it's still prudent to confirm with a trial-by-fire exercise, or "breach and attack simulation" (BAS).

REMEMBER

Keysight's survey found that barely a third (35 percent) of respondents have test-based evidence to prove their security products are configured and working correctly. For more details of the Keysight survey, see `https://about.keysight.com/en/newsroom/pr/2020/12feb-nr20020-securityeffectivenessreport.pdf`.

Enabling Breach and Attack Simulation

Being aware of today's threat landscape is vital to identifying the soft spots in your own environment. Threat intelligence comes in a variety of flavors and nearly every security product has a "threat intel" feed that allows it to understand what to defend against. The end goal of threat intelligence is to provide knowledge that allows you and your tools to make the right decision.

Traditionally, threat intelligence has been used in a proactive manner to either stop a known bad actor, perform incident response, or breach forensics. Security teams are beginning to realize that the same knowledge about attack exploits and techniques can be used proactively to harden security before an attack.

To be proactive in using threat intel it is critical to also have a long history of knowledge alongside the data, as well as expertise to understand the latest threats. Keysight has been collecting and distributing threat intelligence for more than 15 years. The Keysight Application and Threat Intelligence (ATI) team manages a continuously updated database cataloguing millions of known and emerging threats from a global honeypot network, as well as public and private threat feeds. The team analyzes this research, develops threats and application protocols for simulation, and performs reputation and security research that is then packaged into Keysight products.

TIP

Keysight's breach and attack simulation product, Threat Simulator, allows organizations to probe their live production networks to safely and proactively measure the effectiveness of their network security. Threat Simulator provides easy-to-understand, easy-to-follow, step-by-step instructions to remediate whatever gaps you find.

Threat Remediation: Measuring SecOps Impact

Breach and attack simulation exposes the gaps in your security environment, but it also helps you fix the problems and then re-audit to confidently know your work has made your security stronger. For too long, security professionals have often had to simply guess that what they did on a Monday helped the company's security on Friday. With BAS, that is no longer a question. You know now the impact of your time and resources, allowing you to accurately measure security operations effectiveness and costs.

Tying It All Together

Today's world demands a higher level of due diligence. Your organization is under attack, unceasingly. Thus, your organization's security posture must remain strong and up to date, continuously.

There is no excuse for not verifying the effectiveness of remediation efforts. Verifying that the patch was installed is not sufficient. The correct answer is verifying that the vulnerability is not exploitable.

TIP

Keysight ATI delivers threat intelligence to simulate realistic, relevant attacks from a large database of exploits, using the entire kill chain so you know exactly where to focus.

IN THIS CHAPTER

- Defining your current security posture
- Evaluating your equipment and effectiveness
- Assessing the difference between today and where you need to be
- Establishing a defensive security posture

Chapter 2
Measuring Your Security Posture

As a wise map salesman once said, "You can't move ahead without first looking at where you are."

This chapter helps you understand and evaluate what your security posture is today and how to bridge to where you want to be. It shows you how to test the effectiveness of your current equipment to better recognize any gaps and risks present. You then assess those gaps with the desired end-state in mind. Lastly, the chapter explains how to establish a solid defensive security posture.

Your Security Posture: Current Baseline and Future State

Picture this: You're in the elevator. Your boss gets on and asks for your assessment of the company's security posture. What do you say?

Granted, the proper answer may not fit in 30 seconds, and maybe your boss is really asking for more than a short response. But the real issue is: Can you answer the question — concisely and completely?

Security posture is the "big picture" — a collective information security appraisal of the organization's hardware, software, network, data, configurations, policies, and services. Personnel with their ability to react and respond to a security event form part of the total equation.

Measuring security posture does not necessarily mean evaluating each area and asset in great detail. Security posture is the sum of those assets and how well the organization manages its information security. Essentially, your boss's question is, "Is our security posture stronger today than it was yesterday?"

Measuring starts at the top

Measuring how secure a company is begins with policy. Policies dictate how the company should conduct business, and most policies, especially information security policies, are framed with risk appetite in mind. Both policy and risk appetite tend not to change much over time, if at all. When a policy gets written and signed, it's adhered to because, well, "it's policy."

Policies form the foundation for standards and guidelines, which drive how business gets put into production. Because the impact of policy fully influences decisions regarding production technology, processes, and procedure, the measuring of *security posture* begins at the top.

REMEMBER

A key success factor for policy is executive support. Senior management must communicate those policies periodically to all who are expected to adhere to it. With expressed support, policy is not just an official statement, but instead helps empower future decisions. For key managers responsible for maintaining the security posture through changing times, a well-supported policy is helpful to gain buy-in.

Changing with innovation

Recall what life was like before the popularity of personal devices? With personal devices connecting to the network, do you remember the changes made *just to preserve the current security posture?*

Changes include bring-your-own-device (BYOD), expanded remote access equipment and procedures, and amended awareness training.

Do you recall life before the cloud? Remember the changes made *to maintain an acceptable security posture?* Today, companies heavily rely on cloud computing, and with it come an extended network perimeter, lost control, and a larger attack surface.

The same questions can be asked about other trends and other innovative changes. In the end, a company recognizes the innovation and adapts. The real danger is that innovation occurs without a corresponding change to maintain the organization's security posture.

As the bad guys innovate, if you don't act accordingly, your security posture unknowingly grows weaker. Those innovations go unseen or unchecked until it's too late.

Assessing Current Equipment and Effectiveness

You need to be confident of your security equipment's value and purpose to the organization, as well as its ability to serve its purpose for prevention, detection, or alerting. For each item, a few questions arise:

- Does this equipment provide the value expected of it within my unique environment?
- Is this equipment detecting, preventing, or alerting the right behaviors?
- Is this equipment configured properly and within our established policies?

If your company is like most, a few realities influence your judgement of your equipment's purpose and effectiveness. For example, the person who maintains equipment today may not be the person who originally specified the need for it, installed it, and configured it. And, it is always changing and being reconfigured.

To sum up the major hurdles to testing equipment effectiveness, they are:

- Ability to measure effectiveness specific to *your* company
- Assurance that prevention, detection and alerts are happening as needed
- Validation that configurations are correct and policies are adhered to

Keep those factors in mind when reviewing the effectiveness of all equipment and capabilities. What follows is a step-by-step approach to evaluating objectively.

Understanding how business needs relate to equipment

Ask yourself: "How does this tool secure our company while allowing us to get our jobs done?" Begin answering this question by recognizing breach and attack simulation (BAS) for its ability to test your security posture and do so while the production network continues without interruption. BAS informs you of gaps and offers guidance on how to correct them. Security staff responsible for administering the equipment can be assured their equipment configurations are valid and effective.

WARNING

When studying how business and equipment relate at the individual process level, you may find setups that seem unnecessarily complicated and possibly even counterproductive. Often these issues exist because of an attitude that "it's always been that way" or "if it isn't broken, don't fix it." Right now is *not* the time to fix the problem, but make a note to address it later.

Understanding equipment effectiveness

Just because the equipment has a purpose doesn't mean the equipment is performing its job well.

Ask yourself two questions:

- **"How well is this security solution doing its job?"**
- **"Will this security solution perform satisfactorily under any condition?"**

These questions can be hard to answer if you simply look at logs or basic status cues. The best course of action is to employ a service designed to stress your security equipment and test its effectiveness. For example, Keysight Threat Simulator, a BAS product, safely creates live attacks to measure the effectiveness of your entire security environment.

Only through attacking your own production environment will you understand if your security protocols are effective, even in the face of simple misconfigurations or full kill chain malware.

Threat Simulator emulates the entire cyberattack kill chain with simulated attacks: phishing, bad user behavior, malware transfer and infection. With these kinds of assaults, you'll test the effectiveness of your security tools the right way.

Recognizing the Gaps; Assessing the Risks

In Keysight's February 2020 survey, 86 percent of respondents said they would value a solution that finds and helps to remediate vulnerabilities in a company's security posture.

This conclusion offers insight into an opportunity. Organizations don't want to just find vulnerabilities; they want help fixing them as well.

Continuous assessment

Based upon the ATT&CK framework (see Chapter 5 for details), Keysight's BAS product is designed to operate as the attacker does, discover security gaps in real-time, immediately alert those responsible to close those gaps, and provide guidance on how to close them. Threat Simulator draws from a knowledge base that is updated nonstop.

Continuous remediation

Having a flat list of gaps to close is not enough. An organization needs to know how to address those issues. Keysight's Threat Simulator provides easy-to-follow, step-by-step instructions. That's the epitome of actionable intelligence.

Architecting a Proactive Security Posture

An environment cannot survive only by reacting and staying on the defense. The solution cannot be that security personnel take more initiative alone, but rather that they are guided by a continual test and audit of the organization's security posture.

Designing a proactive security posture requires preparation across multiple levels. The following sections delve into what makes a proactive security posture and how to gauge your preparedness to take action.

Engaging the experts

Being prepared is critical, no argument there. And the most valuable preparation doesn't come from guidelines or books. The best preparation stems from within the company, from the in-house experience your staff gain on the job.

The frontline security staff know the systems, put out the fires, and have handled all the incidents. Regardless of whether past incident responses were heroic or lackluster, security staff are the people who know the history and peculiarities of your organization.

Harnessing that experience

Those frontline security staff have the potential to accomplish so much more. They can adopt a proactive approach when their time is saved by targeting their efforts toward the right issues.

Keysight's Threat Simulator draws attention to the right areas, keeping staff focused on what matters and ultimately raising efficiency of both your defenses and staff.

REMEMBER

Threat Simulator doesn't just provide a list of problems that it has found in a scan. Instead, it gives you instructions for how to fix those problems, whether it is applying a certain patch to a server or closing an open port on a firewall. Intelligence is far more useful if it is actionable, and that's what Threat Simulator provides.

Putting it into practice

Employing Threat Simulator is akin to having a Red Team constantly employed and active. This automated, virtualized version of a Red Team immediately takes research and expertise from Keysight and translates it into actual defense.


TIP

Threat Simulator does not require any disruption to your production network, nor is it disruptive while running. By utilizing a BAS, you discover vulnerabilities and liabilities before they become a cost to production. Being armed with Threat Simulator is to be forewarned and ready to address the issues at hand.

At the same time that you're improving your security posture with BAS, you're maximizing the utility of all your security products. Only 50 percent of the respondents to a Keysight survey said they found a security solution was not working as expected. Unfortunately, this discovery comes after a breach occurs. Surprisingly, far fewer (35 percent) of the respondents said they actively validate with test-based evidence to prove their security products are configured and working correctly. Unsurprisingly, more than 85 percent of respondents said they would value a solution that finds and helps to remediate vulnerabilities in a company's security posture.

IN THIS CHAPTER

- Exploring the value of a simulated attack
- Distinguishing between programmatic, repeated simulations, and pen testing
- Understanding and benefiting from third-party expertise
- Utilizing recommendations generated from threat simulation

Chapter 3
Hacking Your Perimeter Before They Do

This chapter explains how attacking your defenses greatly improves your survival under attack by others.

Applying Breach and Attack Simulation

Quick question: Why do organizations wait for something bad to happen to them?

Quick answer: They don't want to, but until now have had little choice.

Organizations have consistently tried to be proactive using a variety of tools and services. Unfortunately, many of these, such as penetration testing and vulnerability scanning, only give you a point-in-time reference, and Red Team services are extraordinarily expensive.

Now because of the power of proactive threat intelligence, real-world attack simulation capabilities, and a renewed focus on making security testing easy to use, organizations, no matter

their size, are finally able to continuously simulate an attack on their own terms and get a better idea of their strengths and weaknesses.

The best defense is a good offense

At some point, you will be attacked. This isn't fearmongering — it's a fact.

Whether internal, external, by accident, or maliciously, whether scripted or conducted by people, attacks happen. And they will continue to happen.

The best way to guard your company and strengthen your security posture is to be better prepared. You can prepare in either of two ways:

- Wait to be attacked and see how it goes.
- Simulate an attack against yourself and see how well your defenses work.

Here's hoping you prefer the second choice.

On your own terms

With breach and attack simulation, you can effectively measure your security posture by quantifying where you are strong and also where you need some help. Once you have done this, you can take steps to improve.

With ongoing, automated tests, you are better able to deal with drift or unplanned change. You can catch problems, misconfigurations, or temporary workarounds before the bad guys do.

Not at your expense

You can be in control of your own "offense" without risking unauthorized access, altered data, or downtime.

The textbook trio of information security is confidentiality, integrity, and availability. Failure in protecting those results in unauthorized access, altered data, and downtime or inaccessibility, respectively. The more technical terms are: disclosure, alteration and destruction.

In order for an attack simulation to be most effective, you have to run it against your production environment. That's where the process gets tricky, because you need to be careful that although you conduct an effective test, you don't disrupt your own network. Make sure that the probing you do is safe to do on a production network but also effective enough to provide the intelligence you need.


TIP

Keysight Threat Simulator is a breach and attack simulation (BAS) product that tests your network's security posture. BAS does that using the latest attacks and exploits, but in a way that is safe and undisruptive to your production environment. It conducts probes in an ongoing, automated manner, ensuring that you have a continually updated view into the effectiveness of your security.

In contrast, penetration or "pen" testing is conducted against a target at one defined point in time. By the time you get the results of a pen test, they are already out of date. Meanwhile, new threats have emerged, vulnerabilities have been exposed, and configurations have changed.

Alternative necessity

What would you call a service that conducts a controlled attack on your defenses? This service is penetration testing. Penetration testing pokes and prods a system or network in order to reveal its vulnerabilities. The service traditionally means hiring an individual or group to visit, get up to speed on scope and parameters, and carry out the testing. After some time, a report gets prepared and distributed.

Although required for maintaining compliance, manual penetration testing has its drawbacks:

- **Done once:** The individual or team arrives, tests, and leaves. Testing doesn't continue repeatedly 24/7.
- **Unvalidated:** After closing a vulnerability, the individual or team typically doesn't immediately return to validate it.
- **Various procedures:** Testing *methods* vary per person or team and are often difficult to reproduce.
- **Outdated report:** By the day their report arrives, your vulnerabilities may have changed.

By name, that's penetration testing. By practice, it is a slower, single "one-off" approach to testing your environment. However, pen testing is challenging to reproduce and is a relatively expensive snapshot in time.

Keysight's Threat Simulator, on the other hand, tests your environment in a manner far less costly over time and safely, without interruption to the production network. Threat simulation is not a one-off test — it is ongoing, automated testing of the effectiveness of your security.

The truth is, in today's environment, testing your systems should be done repeatedly and reliably.


REMEMBER

Keysight Threat Simulator is not simply an equivalent to exploitative attacks by a human pen tester. It operates programmatically and in a dependable manner. The most concrete value in having a 24/7 "pen tester" is verification that the security gaps or misconfigurations you addressed last week don't get reopened this week without anyone noticing.

On tools

A Keysight executive, Scott Register, observes that "enterprises are faced with a continuous stream of cyberattacks that threaten their businesses, and in many cases they attempt to deal with these by buying more security tools." Information security is a necessary department, but management watches the return on investment (ROI) as with any other department. With information security, you need to ensure no costs are redundant or wasted.

Scott explains that good security tools are occasionally misconfigured, or security team members lack the adequate skills to recognize those misconfigurations. In these cases, resources are being wasted or with diminished success. These are opportunities to save resources and costs.


REMEMBER

Keysight's February 2020 survey found 66 percent of companies are using security solutions whose functions overlap, and for 41 percent of respondents this overlap is unintentional, wasting security budgets and management time without strengthening the organization's security posture.

When a security tool can identify those issues, not at a "snapshot" in time, but continuously, you're saving resources and heightening your security posture. Keysight's Threat Simulator is the tool that continuously checks for those issues.


TECHNICAL STUFF

New exploits and vulnerabilities are constantly being discovered. Often they are shared or sold. On the dark web, you can even choose from extensive menus or order custom malware packages. This is why security needs to be an ongoing process rather than a single, "won and done" snapshot in time.

Recommendations May Be Required

If someone asks you for guidance, you offer them your leadership. If someone asks for instruction, you offer them education. After every request for help, recommendations follow. The same can be said for information security consulting. Recommendations come at the end, because what you really want is the answer to "How do I close the gap?"


TIP

This is where Keysight's Threat Simulator brings unique value to the table. Knowing you have a problem is only a small part of winning the battle, so the folks at Keysight built a patented recommendation engine into their breach and attack simulation solution. After you run your scan, you get a report where you can drill down for step-by-step recommendations to fix each issue found. Maybe you need to patch a server, or perhaps you need to close a well known port on your firewall. Actionable intelligence is key to rapidly taking steps to enhance your security posture.

Speaking of recommendations, that brings up the next topic — *regulatory compliance* — two words that may give you either bragging rights or nightmares.


WARNING

If your business includes maintaining regulatory compliance, such as the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and now the General Data Protection Regulation (GDPR), you need to stay abreast of penalties for non-compliance. In 2019, the U.S. Department of Health and Human Services revamped the penalty system for HIPAA violations, markedly increasing the civil monetary fees.

Any organization with the added responsibility of demonstrating compliance knows that ignorance is not an excuse.


TIP

The Latin for "ignorance is not an excuse" is: "*ignorantia juris non excusat*." Maintaining non-compliance, willfully or not, significantly raises the odds you'll see this Latin phrase again.

There are many consequences for non-compliance. Some are statutory (legal) penalties, which for a company can result in poor public relations, harm to your reputation, or loss of clients. Consequences can include monetary penalties, sometimes very large ones. Other significant consequences include the resources spent on resolving the issue, which may have been avoidable in the first place, a diminished credit rating, and even loss of contracts or the ability to process credit card transactions. Like it or not, these things have teeth.

IN THIS CHAPTER

- Benefiting from real-time intelligence
- Holding the superior position
- Reporting and presenting

Chapter 4
Maintaining a Superior Posture

Ever seen your favorite basketball team take a 25-point lead . . . and then lose the game? Or watched a track and field race, where the winner starts celebrating just a bit too early? Keeping the winning position takes more than great training, planning, and execution. Right up to the finish line, the winning position requires you keep your lead.

This chapter covers keeping your lead when fighting against hackers and those threatening your organization. Maintaining a superior posture requires utilizing what's available.

A Real-Time Threat Intelligence Feed

With good help, the tables turn against hackers dramatically. Security companies that specialize on that need can deliver that high-quality help. Keysight, for example, powers its security solutions with a threat intelligence feed, continuously updated with the latest threats and exploits.

Intelligence is more than being smart

Intelligence has two meanings. The more common one is having brilliance of mind. The second meaning is having the right information to make the right decision. Granted, you already possess the first. Threat intel is about getting to the second.

How to create intel

Creating valuable intelligence requires a step-by-step process:

- **Collection:** Gather information from public and private threat feeds, global honeypots, and more.
- **Analysis:** Evaluate and reproduce threats and vulnerabilities to create useful intelligence.
- **Processing:** Package the threat intelligence in the most helpful and practical manner for its consumer.
- **Dissemination:** Deliver the threat intelligence in a timely and handy manner that doesn't demand a hands-on approach.

Putting "intel" to good use means the difference between gaining the upper hand and staying in the dark. The real benefit to Keysight's threat intelligence feed is this intel comes to you without requiring active participation of a security individual dedicating to researching all of it personally.

When to use intel

Here's a good question: "When do you use valuable intel?" The only right answer is, "When you need it," which of course means, "All the time." The important variable is how soon or if the threat will strike.


TIP

Unfortunately, when dealing with threats to your systems and networks, no one knows when will happen. You know only that more likely sooner than later. With malicious actors, automated scripts, and zero-day exploits, the best-case scenario is to put your intel to use immediately.

Real time means knowing now

Effective information security requires keeping up to date on threats and new techniques used to carry out those threats. A myriad of sources, from blogs to news feeds, keep you abreast

of the latest security threats. These sources start and steer conversations around future controls implemented at the organization. Unfortunately, another way of learning the latest techniques comes from investigating after a "successful" incident.

In any case, you have your choice from multiple sources of news. That intelligence is valuable. Whatever you follow, whether by email or some printable form, you eventually set aside time to read it, digest it, and then apply it.

Reading and applying manually does not give you the advantage that a real-time threat intelligence feed can. When receiving threat intelligence in real time, that means intel is applied immediately, to an application or appliance, right then and there.


TIP

One example of a legitimate real-time threat intelligence feed source is that from the Keysight Application and Threat Intelligence (ATI) Research Center. The center continually aggregates newly discovered attacks and malware. To ensure no target gets away, these collected attacks take aim at more than 400 applications, and the number is growing. The applications your organization uses are likely among those.

Keysight's ATI team manages a continuously updated database cataloguing millions of known and emerging threats from a global honeypot network, as well as from public and private threat feeds. The team analyzes this research, develops threats and application protocols for simulation, and performs reputation and security research that is then packaged into Keysight products.

Maintaining Superiority

Maintaining a superior position requires exploiting your strengths and also keeping your weaknesses from being exploited. Like doing a strengths, weaknesses, opportunities, and threats (SWOT) analysis on a risk, each side of the coin has its own strengths and weaknesses.


REMEMBER

A SWOT analysis is a brainstorming approach of identifying distinct aspects of a risk, both good and bad. It is optimal for analyzing one issue or opportunity, not a pair or more of issues, where aspects may conflict. A strength for one group may be a weakness for another.

Recognizing your shortcomings

When talking about good guys versus bad guys, consider each side's strengths and weaknesses. Your organization's information security team has advantages over the hackers. Yet, you are lacking in one important aspect: Manually, it's impossible to outperform the hackers out there.

Hackers have these advantages over organizations:

- **Hackers collaborate.** They share new tactics and vulnerabilities with each other.
- **Hackers innovate.** They invent with creativity and speed.
- **Hackers deliver.** Exploits quickly develop, mature, and are put into "production."
- **Hackers aren't corporate.** Hackers are free from cost approvals, agile project management, and long implementation cycles.

So, how do you battle against this level of creativity, speed, and execution? If you successfully defend a zero-day attack this afternoon, can you promise the same success against a new attack next week?

There are no promises. At least, not without help, and not without advantages of your own.

Reinforcing your strengths

To gain the upper hand, you need to exploit your strengths to their fullest.

Organizations cannot be expected to singlehandedly overcome hackers' advantages. If by good fortune, a well-placed defense or countermeasure wards off an attack this time, hackers still have the advantage for the next time. For continued success, organizations require a continued feed of prepared intelligence that they can put into action in real time. Lastly, that continual protection must be monitored and must prove itself through reporting.

REMEMBER

Keysight ATI recognizes and practices the same advantages hackers enjoy. ATI delivers threat intelligence to its clients, updated every five minutes, continuously. Keysight clients can utilize the Threat Intelligence feed by emulating the newest attacks with Threat Simulator or by updating an on-prem gateway, ThreatARMOR.

TIP

WHY NOT TRY IT YOURSELF?

Curious about what a breach-and-attack simulation system might find on your network? Try it out!

Keysight offers a free trial version of Threat Simulator — validate your defenses, find vulnerabilities, and get step-by-step instructions for remediating gaps.

The URL is: `https://www.keysight.com/products/network-security/breach-defense/threat-simulator.html`.

Reporting

Reporting is vital as you take advantage of the measures and controls employed to protect the network. Every step taken to bolster your security posture should include some function of monitoring and reporting.

Network visibility

The complexity of modern enterprise networks, with increasingly amorphous hybrid architectures, can make visibility into network traffic a real challenge. This is more than a theoretical problem because monitoring and security tools depend on visibility into not just some, but all of the traffic on the network. With this in mind, many organizations are deploying network visibility solutions that allow visibility into encrypted, encapsulated, virtual, and other forms of challenging network traffic while also enabling security resiliency, greater efficiency through filtering and deduplication, and even load balancing. It's like having your cake and eating it, too.

TIP

Dropped packets are the nemesis of a secure network. Some approaches to network visibility are prone to dropped packets under load or when features and filters are turned on. When implementing a network visibility solution, go with a hardware architecture that supports the functions and features you need at line rate without dropping packets.

Keeping it relevant

Reporting should fit the needs of the end-user or person doing the monitoring. One way of doing this is to ensure that alerts are meaningful. Although your tools are likely doing a good job of generating alerts, if your organization is like many others, they are doing *too* good a job and your team is overwhelmed with alerts.

REMEMBER

ThreatARMOR is a threat intelligence gateway that functions as a first-line defense, blocking up to 80 percent of inbound malicious traffic. This reduces security information and event management (SIEM) alerts and fatigue on the SecOps staff.

The New You: Safer, Smarter, and Business-Aligned

An enhanced security posture leaves the IT team in a far better position — safer, stronger, and in better alignment with the business.

Safer

With regard to your systems and network, the words *secure* and *safe* are essentially synonymous. Being more secure is being safer — not just safer for the valuable data being protected, but also for the company's good reputation and its sustained future in the market.

Hackers and other threats to your organization are operating at phenomenal speed and with high creativity. That creativity means new malware is released every day.

At best, today's new malware has a signature similar to yesterday's or last week's. In that case, catching it becomes a bit easier. However, hackers' creativity can bring about the kind of malware that's never been seen before.

Any product with the purpose of keeping the organization safer requires that product be ready for threats not yet seen.

TECHNICAL STUFF

In information security parlance, newly released malware is "zero-day malware," referring to a short existence of zero days.

Smarter

Keysight's threat intelligence gateway product ThreatARMOR provides protection against zero-day malware including ransomware. It does so not by blocking bad guys based on signatures, but rather by blocking IP addresses of known bad actors. The theory is that you will never catch every new threat with signatures and sandboxes, but if you know that bad traffic is coming from a particular address, blocking that address helps reduce your overall security burden. ThreatARMOR also blocks not just inbound, but also outbound traffic to known bad sites, stopping exfiltration as well as command and control traffic.

TECHNICAL STUFF

Command and control (C&C) servers are external, hacker-controlled systems waiting for the malware to "phone home." Once contacted by its malware, the C&C server replies with additional instructions or malware composed of more insidious tools and software poised to root farther into the infiltrated network. By stopping the initial contact to C&C servers, a small incident is stopped before it becomes worse.

Business-aligned

An organization functions best when its decisions and choices align with the needs of business. Choices have to support business sustainability and profitability. That covers a lot of different choices, such as where to build, what talented people to hire, payment and collection terms and so on.

With regard to information security, the choices tend to stem from risk appetite and risk tolerance.

In project management, almost all choices revolve around the famous three constraints: quality, cost, and time. You already know the balancing act among those constraints: If you prioritize one, then one or both of the others may degrade. For example, you can prioritize costs, but perhaps at the expense of a lesser quality.

There is also the challenge of maximizing the return on investment (ROI) for existing infrastructure. This is where a breach and attack (BAS) solution can provide considerable benefit. You paid for the firewall, but if you inadvertently leave a port open and something bad happens, one tiny slip has negated a hefty investment. With solutions like Threat Simulator you can not only find problems like this one, but also save time with step-by-step instructions that tell your team how to plug whatever gaps are found.

REMEMBER

With respect to aligning with business needs, the prospect of utilizing a real-time intelligence feed is a "win" for all three — quality, cost, and time — with regard to the organization's security.

IN THIS CHAPTER

- Assessing your current situation
- Understanding how the Mitre ATT&CK Framework can strengthen your security posture
- Measuring maturity level
- Testing defense in depth

Chapter 5
Assess. Detect. Remediate.

Your organization may have the most solid cybersecurity program possible, but knowing exactly what techniques those defenses are thwarting will help you make your cybersecurity program great. The Mitre Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) framework is an excellent resource to provide that understanding.

Mitre developed the ATT&CK framework to show how attackers penetrate and progress through your network. ATT&CK gives you the attacker's perspective. It walks you through the attacker's behaviors and objectives, as well as the tactics and techniques you can expect the attacker to use. Understanding ATT&CK helps you predict the attacker's likely next moves.

This chapter leans on the ATT&CK framework to offer the best approach for strengthening your information security program.

Assessing the Current Situation

Before your organization can consider shoring up its security posture, you first need to assess your current situation.

This isn't simply taking inventory of assets or creating a baseline test on network performance. You should examine the environment with those proposed changes in mind.

Taking a nod from ATT&CK, here are some goals that fall under the early task of assessing your environment:

- **Review your coverage.** From ATT&CK, you can plainly read an attacker's likely series of tactics. Can your environment see them?
- **Examine your analytics.** What exactly are you looking for? What are you tracking or trending?
- **Define detection.** "Prevention is ideal, but detection is a must." Will you detect something new, or only the known?
- **Identify your sources.** What sources are you using to collect data? Are your tools overlooking any others?
- **Create a risk heat map.** You must prioritize assessed risks before considering risk responses.

Depending on how well-trained and capable the organization's security team is, leverage ATT&CK to perform the assessment:

- For the smaller organizations or those with few security members, select only one or two ATT&CK techniques. Don't burn out those few resources with too many techniques.
- For larger, better staffed companies, you have no reason not to use a large subset of techniques across ATT&CK. You may even add mitigations. Associate current mitigations with the ATT&CK techniques you've chosen.

But why worry about having ample, capable staff when assessment and mitigation tracking can be done in a much more hands-off way? Keysight's breach and attack simulation performs these tasks automatically.

Assessing as the adversary

The ATT&CK framework follows the tactics and techniques attackers use to penetrate and progress through your network. The framework walks you through the attacker's perspective and shows how the attacker behaves. The steps of the ATT&CK framework provide a walkthrough of what is targeted and illustrate how

the successes of an earlier step provide the prerequisites for the next step.

As such, the ATT&CK framework provides an outline for assessing an organization's readiness to repel attacks. This activity is called *adversary emulation.*

Adversary emulation is invaluable as a tool to test both prevention and detection (as opposed to penetration testing, which focuses more on prevention). Taking this approach to test your defenses as the adversary is arguably the best way to test your security posture.

Testing the defenses

The organization will find more assurance in its security after testing it and shedding light on areas for improvement.

Testing your security infrastructure requires a special kind of tool — one that can replicate the barrage and variety of malicious traffic stemming from an attack, but not destructive or disruptive.

ATT&CK provides the methodical approach to test your defenses. ATT&CK helps you define what to look for. And, because it represents the attacker's "tactics, techniques, and common knowledge," ATT&CK is perfectly structured for attack simulation.

TIP

Keysight's breach and attack simulation product attacks to evaluate security posture and, if you've closed those identified gaps, returns to validate that the gaps are indeed closed.

Keysight offers a solution called BreakingPoint, available as either a hardware appliance on-premises or as a virtual/cloud offering. BreakingPoint simulates more than 38,000 types of malware, in addition to legitimate traffic, making tests for pre-production networks diverse and comprehensive.

Most recently, Keysight launched the "QuickTest" version of BreakingPoint, which accelerates time to test with preconfigured templates and immediate security effectiveness assessments.

Beyond malware, BreakingPoint can also help organizations validate their ability to stand up to distributed denial of service (DDoS) attacks.

Detecting Gaps

Maintaining an effective security posture requires that gaps between the current and desired states be measured. "Yesterday's" desired state is likely no longer adequate today, a necessary evil to recognize how new gaps can appear.

Detecting gaps in your security is an ongoing process. Thus, closing those gaps is also an ongoing process. In order to counter obsolescence, you must rely on sources that continuously deliver the most recent awareness of threats.

Here are some steps to help you identify gaps between the current situation and the desired state:

- **Identify mitigation approaches.** Ask what the plan is toward responding to those identified gaps.
- **Translate mitigation into desired outcomes.** Map responses toward the end goals.
- **Review and outline security priorities.** Revisit the path to close gaps and realize the end state in a responsible manner.

Gaps in detection

Detection itself, as a capability, can have gaps. A significant gap in an organization's capacity to identify and flag traffic on the network as suspicious is a disaster in the making. An ability gap in detecting suspect traffic means the difference between successfully stopping an attack in progress and learning about the attack while responding to it.

But how do you close that gap in detection? With the right solution, one that is reliant on multiple ways of detection. Consider the antivirus software that relies only on a definition file containing known virus signatures. Or the intrusion detection system relying on heuristics, suspect behaviors, or patterns. Or an upstream appliance able to protect from denial-of-service attacks by traffic load. All of these solutions are effective at detecting within their capacity. But if a new, previously unknown malware is invited in by a user's action, then the malware's next move will likely happen undetected by those means. You need a solution already aware of activities beyond your organization's boundary, and able to act.

Gaps in defense in depth

Keysight threat simulation can identify those gaps using knowledge of actual threats and attack methods.

Threat Simulator

No matter what controls are in place, and no matter how seemingly impenetrable the current defenses are, a breach can happen. How better to identify those gaps than to continually "Red Team" it?

A human Red Team may expose weaknesses, but their methods are not nearly as predictable, repeatable, and objective as a virtualized, programmatic method. Threat Simulator is continuous, providing an automated Red Team for far less cost.

Detecting the gaps left behind

Were you aware that, in the course of troubleshooting a problem, a member of your team temporarily opened a port on the firewall? Oops — what protection do you have?

First, your organization's typical list of network defenses include:

- **Firewall:** A perimeter network device to block inbound traffic and malware, based on rules
- **IPS/IDS:** Intrusion prevention/detection systems that might respond to, or at least alert to, suspicious behavior after installation
- **The host system's antivirus:** Software that identifies threats by signature and/or heuristically

All these lines of defense work well to protect the network. Each of those defenses is valuable and will, in a best-case scenario, identify malicious traffic that has entered the network.

In this case, a rule on the firewall was opened with the harmless intention of keeping it that way for only a few minutes while testing a front-facing application. Unfortunately, the team member responsible for resetting that rule was sidetracked and has forgotten to correct the misconfiguration. This break in defense will not be caught unless or until an attacker takes advantage of it.

Finding that break requires you to be looking for it. If you have Threat Simulator, you've been doing exactly that, since before the port was opened.

Remediating with Guidance

When gaps have been identified and you have a plan for closure, it is time to start remediation. This is one of the most important tasks in improving security posture. A Keysight survey showed that seven of eight respondents said they would value a solution that finds and helps to remediate vulnerabilities in a company's security posture.

Mitigating for users inviting an incident

You must admit, it's often a user who unwittingly invites malware onto the network. It happens innocently enough and easily enough. The best users are productive and willing to help their peers be productive as well. And as such, well-intended users have become the attacker's most productive attack surface when targeting the organization.

Users are reliant on several internal applications, each presenting a potential avenue of attack. Hackers know this and will prod and poke users with good intentions until a piece of malware is invited in.

It's a harsh truth because no technology can stop a user from instigating the initial "invite." The best technology can only react and remediate immediately after a user does so.

Case study: Catch 'em by the address

Keysight's ThreatARMOR demonstrates the strength of defense in depth, particularly when armed with intelligence. Here's a step-by-step illustration of how ThreatARMOR stopped a ransomware variant.

The "what"

The malware, a nasty variant of Locky ransomware, was hard to detect. It used advanced obfuscation and evasion techniques to go unfound by most common antivirus and IPS systems.

The "how"

How was it recognized as malware? The malicious nature of this malware was revealed by its attempt to contact an external IP address. Although the malware itself was undetectable, the IP address of its C&C server on the Internet was in the threat intel database and already blocked, illustrating how this approach can provide protection against zero-day and other hard-to-detect threats.

The "what if?"

Had the malware been able to "phone home," then a number of systems likely would have been locked, encrypted, and ransomed. The victim would then have to either explore options including paying ransom (not recommended) or exploring how well their backups have been running (not for the faint of heart).

IN THIS CHAPTER

- Cultivating legitimate strengths and knowledge from your attackers
- Identifying, reviewing, and closing gaps in your environment
- Leveraging the research of skilled sources
- Sustaining and holding the greater standard of your security posture

Chapter 6
Ten Tips for Breach and Attack Simulation

An organization will be genuinely assured in its security posture only after having it tested. Being "tested" is not a euphemism for suffering a breach. Being tested means deploying a breach and attack simulation (BAS) solution to continuously create security audits. Continuous breach simulation, sending real-world attack traffic against your organization's defenses, identifies weak spots and misconfigurations to be more closely monitored. With breach and attack simulation, an organization gains first-hand insight into how the attack will succeed — without the consequences and disruption.

If you want to achieve and maintain a strong security posture, look toward BAS. This chapter offers ten points to remember as you do.

Know Thyself

Respect the organization's strengths *and* weaknesses. Exploit strengths of the organization and security staff. Continue to use best practices like defense in depth and segregation of duties.

As for weaknesses, compensate for an organization's lack of a real-time threat intelligence feed by leveraging the dedicated research and technologies of security firms like Keysight.

Your security posture will thank you.

Change Management Is Crucial

A strong security posture requires a strong change management program and buy-in from all. Document any rogue devices, misconfigured systems, or augmented controls when the change is made or discovered. If changes occur without documentation, the organization misses the chance to validate the security consequences. The problem may not be discovered until it's too late. Make it easy for others to learn from your experience.

Exploit Others' Know-How

To fight off today's threats, your company needs threat intelligence. Remember that threat intelligence comes in a variety of flavors, from stand-alone feeds to automatically ingested intel that makes a solution stronger. Choose what is right for you and your team, and ask the vendor how they collect, analyze, and reconstruct threat data before sending it out as intelligence.

REMEMBER

Threat intelligence is all about helping you make the right decisions.

Use Guilt by Association

In interpersonal interactions, people try to refrain from guilt by association. Security doesn't work that way. With considerable effort going into evasion and obfuscation, sandboxes and signatures are going to miss a few from time to time, guaranteed. One way around this problem is to use guilt by association. Block not just known malware, but everything coming from proven bad addresses. This way you catch zero-day exploits and successful evasions.

Simulations Are "No-Fault" Exercises

The first time you run BAS against your production network, you're going to find some gaps that may be embarrassing to your staff. Be careful to make this a "no fault" exercise — remember, you want your team to embrace this new approach, not fear it.

Trust But Verify

When you deploy a new security solution, make sure you test it. Many good security solutions are available, but sometimes things like manual configuration of regular expression filters, overlapping rules, Boolean confusion, and other factors (often on the human side) can result in unexpected gaps. Verify that you got it right with a solution like Threat Simulator.


TIP

To validate that an appliance, hardware or virtual, is capable of performing as needed under load with a realistic traffic mix, use BreakingPoint.

Validating Security Functions

Security appliances and technologies that perform functions such as deep packet inspection (DPI), data loss prevention (DLP), and lawful intercept (LI) are becoming more common for larger organizations. But organizations still find those functions a challenge to validate. These advanced functions are well within the scope of BreakingPoint for testing and validation. When you need these important functions, you don't want to discover that they're broken.

Exposing the Shadows

As networks become more complicated, and as the number of mobile devices attaching to them rapidly grows, it's normal for a network to develop a few blind spots. These blind spots can come from network segments going unmonitored, or they can be the result of overworked switches or tools dropping packets.


TIP

One way around blind spots is to use network taps instead of switch-based mirrored or SPAN ports. In addition, use a visibility fabric powered by network packet brokers with the right hardware architecture to prevent loss traffic and dropped packets.

If You Can't Measure It, You Can't Improve It

Peter Drucker, said by many to the founder of modern management and the author of the philosophical foundations of modern business, was a big fan of data-driven management. Security has traditionally been hard to measure — a business could easily measure the performance of a switch or the throughput of a firewall, but the organization's overall security posture was difficult to quantify.


TIP

Keysight's Threat Simulator changes the game by allowing you to effectively measure your security posture. Even better, when gaps are found, the system makes easy-to-follow, step-by-step recommendations for how you can fix those gaps. Now, both measuring and improving security are possible.

It's a Journey, not a Destination

Sure, it may be a cliché to say that security is a journey and not a destination — meaning that it is an ongoing process and not a single "won and done" event — but it's true. You should regularly patch and update systems and regularly test your security and remediate gaps. You should also make plans to cover things that you know are going to happen — things like zero-day exploits and what to do when an attack gets through.

Glossary

baseline: The starting point or reference, against which a future reference point can be compared.

bring-your-own-device (BYOD) policy: The organization's statement on allowing personally owned devices onto company protected networks and their use to store and/or transmit company data.

CMMI: Capability Maturity Model, a five-level model created by the Software Engineering Institute (SEI) at Carnegie Mellon University. The levels are initial, repeatable, defined, managed and optimizing.

DLP: Data loss prevention, a tool or process that monitors for sensitive data, ensuring it is not lost, corrupted, or subject to unauthorized access.

incident response: The process of handling a security incident in a phased approach of preparation, detection, analysis, containment, eradication, and recovery, as well as a post-incident or lessons learned activity.

IDS: Intrusion detection system, a system that monitors and alerts on malicious or suspected traffic.

IPS: Intrusion prevention system, a system that monitors, alerts and/or responds to malicious or suspected traffic.

information security triad: Confidentiality, integrity, and availability, the opposites of which are disclosure, alteration, and destruction.

LI: Lawful intercept, legally sanctioned access to communications for law enforcement purposes.

NIST CSF: National Institute of Standards and Technology Cyber Security Framework, a structured collection of industry-adopted standards, guidelines, and best practices intended as guidance for any organization.

penetration testing: The process of ethical hacking or conducting sanctioned attacks against a system for the purpose of identifying weaknesses and likely threat surfaces to be exploited by actual hackers.

ransomware: Malware that, when executed, encrypts data on the local device, often as well as networked storage, with intent to extort the data owner for a ransom for the decryption key.

regulatory compliance: Assurance an organization has taken steps necessary to comply with the requirements set by relevant legislation such as the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), or the General Data Protection Regulation (GDPR).

risk management: The process of identifying, assessing, responding to, and monitoring risks.

risk response: One of four responses to an assessed risk, namely accept, mitigate, transfer, or avoid.

security posture: A collective "big picture" overview of an organization's security status and readiness to handle potential security incidents.

threat simulation: The use of generated network traffic to duplicate reconnaissance and exploitative code for the purpose of evaluating secured system and network response.

ThreatARMOR: A hardware appliance with a cloud security service used to monitor and, when needed, block malicious traffic, malware, and connections.

Threat Simulator: A cloud/SaaS offering providing the ability to simulate the cyberattack kill chain, validate defenses, and provide step-by-step instructions for remediating gaps discovered in automated probes.

Go on, hack yourself

This book covers attacks on your network. No, not the ones you expect — these are actually coming from you. The best way to know you're protected is to attack yourself. Imagine the ability to safely execute attacks on your own security environment to find the gaps, misconfigurations, and insecure policies.

Inside...

- Simulate attacks
- Measure your security posture
- Detect misconfigurations
- Find vulnerabilities
- Plug gaps

Jeff T. Parker is an information security enthusiast and U.S. Air Force veteran with 20 years experience in IT risk management and systems security. Jeff's experience ranges from third-level support engineering to IT policy and governance.

ISBN: 978-1-119-69968-2
Not For Resale

for dummies®
A Wiley Brand

July 23, 2020, 7120-1219.EN

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.