O'REILLY®

Defensive Security Handbook

BEST PRACTICES FOR SECURING INFRASTRUCTURE

Lee Brotherston & Amanda Berlin

O'REILLY®

Defensive Security Handbook

Despite the increase in high-profile hacks, record-breaking data leaks, and ransomware attacks, many organizations don't have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost.

Each chapter in this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance, network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks.

- Learn fundamentals of starting or redesigning an InfoSec program
- Create a base set of policies, standards, and procedures
- Plan and design incident response, disaster recovery, compliance, and physical security
- Bolster Microsoft and Unix systems, network infrastructure, and password management
- Use segmentation practices and designs to compartmentalize your network
- Explore automated process and tools for vulnerability management
- Securely develop code to reduce exploitable errors
- Understand basic penetration testing concepts through purple teaming

"Anyone who's been asked to build a security program from the ground up will get immediate value adding the *Defensive Security Handbook* as a reference."

—**Allison Miller**
Security & Privacy, Google

"The *Defensive Security Handbook* gives us a solid curriculum for 'Security 101' and beyond, starting with fundamental concepts and working through a variety of practical steps to build a robust information security program."

— **Jack Daniel**
Security BSides

Lee Brotherston has spent more than a decade working in Information Security across many verticals including finance, telecommunications, hospitality, entertainment, and government.

Amanda Berlin is an Information Security Architect, co-hosts the "Brakeing Down Security" podcast, and writes for several blogs.

NETWORK SECURITY

US $49.99 CAN $65.99

ISBN: 978-1-491-96038-7

9 781491 960387 54999

Twitter: @oreillymedia
facebook.com/oreilly

Defensive Security Handbook

Best Practices for Securing Infrastructure

Lee Brotherston and Amanda Berlin

Beijing • Boston • Farnham • Sebastopol • Tokyo

O'REILLY®

Defensive Security Handbook
by Lee Brotherston and Amanda Berlin

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://oreilly.com/safari*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editors: Courtney Allen and Virginia Wilson
Production Editor: Melanie Yarbrough
Copyeditor: Kim Cofer
Proofreader: Eliahu Sussman
Indexer: Ellen Troutman-Zaig
Interior Designer: David Futato
Cover Designer: Karen Montgomery
Illustrator: Rebecca Demarest

April 2017: First Edition

Revision History for the First Edition
2017-03-31: First Release

See *http://oreilly.com/catalog/errata.csp?isbn=9781491960387* for release details.

978-1-491-96038-7

[LSI]

Table of Contents

Foreword

Spend any time in the information security world, and it will become quickly evident that most of the press and accolades go to those folks working on the offensive side of security. From finding new vulnerabilities, creating exploits, breaking into systems, bug bounties, the occasional cable TV show, and capture the flag contests, the red teams get all the glory. But there is more—much more—to the security world than just offense.

Being on the defensive side, the blue team, can seem a lonely, unappreciated battle. But doing defense is a vital, noble, and worthwhile pursuit. We defenders matter, greatly, to the future of our organizations and the jobs and livelihoods of our coworkers. When the bad guys win, people lose their jobs, organizations are distracted from their core goals, and the bad guys are often enriched to continue their nefarious pursuits. And, like something out of a cyberpunk novel, with the trend of the Internet of Things, soon actually lives may be at threat when the bad guys are successful.

So many of us got our start in the security world as tool engineers, running perhaps a firewall or IDS platform for our employer. Though those skills are highly valued, moving beyond them to a more holistic view of defensive security can sometimes be a challenge without the right resources to bring a bigger picture view. As we continue to experience a shortage of valuable information security defensive talent, we will need more folks than ever to continue to learn and grow into the defensive security role; and to do it well, they need a holistic view of the security landscape.

Another challenge we often face is that a great deal of the narrative around defenses, technology, threats, and thought leadership in the defensive security world comes from the vendors themselves, and their snazzy demos and marketing presentations. Though a lot can be learned from vendors in the space, as they are laser focused on the problems organizations are trying to solve, they also have a sometimes narrow view of the world. IT Security Vendors will often define the problem set as the problem they can solve with their technology, not necessarily the problem an organization

actually has. Countering that view with a holistic view of defensive security is vital to helping organizations become as secure as they can be.

This is why I am so honored to write the forward for the *Defensive Security Handbook*. The world of security is changing rapidly, and we need more folks on the defensive side, learning from the best practices and the hard-won lessons of those who came before. This book does a great job of laying out key principles and skills, and giving a broad overview of the complex and growing landscape of the defensive security side of the world. Amanda Berlin and Lee Brotherston have laid out an overview of the multifaceted world of defensive security. Certainly, whole books have been written on tiny segments of the topics covered, but this handbook does a marvelous job of giving a defensive security professional an overview of the myriad of skill sets necessary to be successful. This handbook is a great primer for those new to the world of information security defense, those who want to expand their skills into more areas, and even those who have many years in the industry and are looking to make sure they are covering all their bases.

I think you'll find this a valuable resource to keep nearby and reference throughout your career. Best of luck on your path, and remember to keep fighting the good fight. Even when it may seem lonely and tough, remember what you are doing matters, and there are many out there who can and will help. Amanda and Lee have done a great job sharing their experience; now it's up to us to learn from their experience.

— Andrew Kalat
Cohost of the Defensive
Security Podcast
February 2017

Introduction

Over the last decade, technology adoption has exploded worldwide and corporations have struggled to keep pace. Usability and revenue creation have been the key motivating factors, often ignoring the proactive design and security required for long-term stability. With the increase of breaking news hacks, record-breaking data leaks, and ransomware attacks, it is our job to not only scrape by with default installs but to secure our data and assets to the best of our abilities. There will always be cases where you will walk into an environment that is a metaphorical train wreck with so many fires that you don't even know where to start. This book will give you what you need to create a solid and secure design for the majority of situations that you may encounter.

Modern attacks can occur for many different motivations and are perpetrated by people ranging from organized crime groups seeking to monetize breaches, through to hacktivists seeking to enact retribution on the organizations they deem to be immoral or counter to public interest. Whatever the motivation and whomever the attacker, a large number of attacks are organized and carried out by skilled individuals, often with funding.

This change in landscape has led to many organizations engaging in a game of InfoSec catch-up, often realizing that their information security program has either not received the executive backing that it required or simply never existed in the first place. These organizations are seeking to correct this and begin along the path to initiating or maturing their information security efforts. There is, however, a problem.

Information security is an industry that is currently undergoing a period of negative unemployment; that is, that there are more open positions than there are candidates to fill those positions. Hiring people is hard, and hiring good people is harder. For those seeking employment, this is can be an advantageous situation; however, it is a high risk for employers seeking to hire someone into an information security position as they would be instilling a certain amount of trust with possible high dollar assets to a new hire.

For this reason, many companies that are only now embarking on their information security program have taken the route to promote someone from another role such as a system administrator or architect to an information security practitioner role. Another common practice is hiring a more junior information security professional into a role than would normally be the case, and expect the newly appointed employee to learn on the job. This situation is precisely what this book is intended to address.

A large number of issues encountered by companies with an immature information security program can be remedied, or at least vastly reduced, with some basic security hygiene. The knee-jerk reaction to the task of inheriting a new and immature security department can be to buy as many devices with pretty blinky LEDs as possible, in the hope that they will remedy issues. Some people would rather pay another company to set up an outsourcing agreement, which can be leveraged in order to assist. Both of these options require money. Many organizations that are new to information security do not have the budget to undertake either of these solutions to the problem—using the tools that are already in the environment may well be all you have.

Our Goal

Our goal is to not only make this a standard that can be applied to most enterprise networks, but also be a little entertaining to read along the way. There are already deep-dive standards out there from a variety of government and private organizations that can drone on and on about the validity of one security measure or the next. We want this to be an informative dialog backed by real-life experiences in the industry. There will be good policy, best practices, code snippets, screenshots, walkthroughs, and snark all mixed in together. We want to reach out to the masses—the net admins who can't get approval to hire help; directors who want to know they aren't the only ones fighting the battles that we see day in and day out; and the people who are getting their hands dirty in the trenches and aren't even close to being ready to start down the path of reading whitepapers and RFCs.

Who This Book Is For

This book is designed to serve as a Security 101 handbook that is applicable to as many environments as possible, in order to drive maximum improvement in your security posture for the minimum financial spend. Types of positions that will be able to take away knowledge and actionable data from this include upper-level CIOs, directors, security analysts, systems administrators, and other technological roles.

Navigating the Book

We have deliberately written this so that you do not have to adopt an all-or-nothing approach. Each of the chapters can serve as a standalone body of knowledge for a particular area of interest, meaning that you can pick and choose which subjects work for you and your organization, and ignore any that you feel may not apply. The aim is not to achieve compliance with a particular framework or compliance regime, but to improve on the current situation in sensible, pragmatic, manageable chunks.

We have purposefully ordered this book to begin with the fundamentals of starting or redesigning an information security program. It will take you from the skeleton steps of program creation on a wild rollercoaster ride into the depths of more technical topics.

Many people fail to realize that a large amount of work and implementation can be performed in an enterprise before any major capital is spent. A common problem faced in information security is not being able to get buy in from C-level executives. A step in the right direction in getting a security budget would be to prove that you have completed due diligence in your work. A large portion of this book includes steps, tools, processes, and ideas to secure an environment with little-to-no capital.

After the skeleton steps of planning out the new and shiny security program, we move on to creating a base set of policies, standards, and procedures. Doing so early in the stages of your security program will give you a good starting point for growth and maturation. Using policies as a method to communicate expectations allows you to align people across your organization with regard to what is expected of them and their role.

We included user education early on in the book as it is never too early to start teaching employees what to watch out for (and using them as a key role in detection). However, depending on the current strength of your defenses, it should not be a major focus until a strong foundation has been formed. Attackers aren't going to bother with human interaction if they can just connect remotely without one.

The book then moves on to planning and dealing with breaches, disasters, compliance, and physical security, all of which combine the management and organizational side of information security with the physical tools and infrastructure needed to complete them. Being prepared in the case of any type of physical or technical emergency can mean the difference between a smooth and steady recovery or a complete company failure—and anything in between.

A good, solid ground-up design is just the beginning. Now that we've covered part of the design of the overall program, we start to get into more technical categories and security architecture, beginning with the two main categories of operating systems. Both Microsoft and Unix have their pros and cons, but in regards to Microsoft, some

of what will be covered is installing the Enhanced Mitigation Experience Toolkit (EMET), Group Policy best practices, and Microsoft SQL security. For Unix, we will cover third-party updates and server/OS hardening, including disabling services, file permissions, host-based firewalls, disk partitions, and other access controls. Endpoint management also falls into this category. A common struggle that we see in corporations includes bring your own device (BYOD) practices and mobile device management (MDM). We will also go into managing and implementing endpoint encryption.

Two other important verticals that are often ignored (or not given as much love as they should be) are networking infrastructure and password management. While going over networking infrastructure, we will cover port security, disabling insecure technologies, device firmware, egress filtering, and more. We will cover segmentation, including implementing VLANs with ACLs to ensure the network isn't flat, delegation of permissions, and Network Access Controls. We will then look into vulnerability scanning and remediation. While most enterprise vulnerability scanners are not free, we talk about them in this chapter to prove their worth by using them for a free trial period (to work toward the purchase of the entire product) or getting the most out of a full version already in the organization.

Many organizations have their own development team; however, traditional training for developers typically focuses on performance optimization, scalability, and interoperability. Secure coding practices have only been included in software development training in relatively recent years. We discuss techniques that can be used to enhance the current situation and reduce the risk often associated with in-house development.

Purple teaming, which is the combination of both offensive (red team) and defensive (blue team) security, can be difficult to implement depending on staffing and corporate policies. It is a relatively new concept that has gained a significant amount of attention over the last couple of years. Chapter 18 covers some basic penetration testing concepts, as well as social engineering and open source intelligence.

Finally, some of the most time-intensive security practices and devices are covered as we go through IDS, IPS, SOC, logging, and monitoring. We have found that many organizations feel as though these technologies are a one-time install or setup procedure and you can walk away feeling protected. It is well worth the time, effort, and investment to have a continually in-progress configuration because your internal environment is always changing, as are the threats you should be concerned about. We won't be making any specific vendor recommendations, but rather have opted to discuss overall solutions and concepts that should stand the test of time a lot better than a specific vendor recommendation for the current toolset.

Oh, and the Extra Mile...that's the junk drawer where you will find our bits and pieces of configuration ideas and advice that didn't really have a home anywhere else.

Now that we have said all that, let's see what we can do about improving some things.

Conventions Used in This Book

The following typographical conventions are used in this book:

Italic
: Indicates new terms, URLs, email addresses, filenames, and file extensions.

`Constant width`
: Used for program listings, as well as within paragraphs to refer to program elements such as variable or function names, databases, data types, environment variables, statements, and keywords.

`Constant width bold`
: Shows commands or other text that should be typed literally by the user.

`Constant width italic`
: Shows text that should be replaced with user-supplied values or by values determined by context.

This element signifies a tip or suggestion.

This element signifies a general note.

This element indicates a warning or caution.

O'Reilly Safari

Safari (formerly Safari Books Online) is a membership-based training and reference platform for enterprise, government, educators, and individuals.

Members have access to thousands of books, training videos, Learning Paths, interactive tutorials, and curated playlists from over 250 publishers, including O'Reilly Media, Harvard Business Review, Prentice Hall Professional, Addison-Wesley Professional, Microsoft Press, Sams, Que, Peachpit Press, Adobe, Focal Press, Cisco Press, John Wiley & Sons, Syngress, Morgan Kaufmann, IBM Redbooks, Packt, Adobe Press, FT Press, Apress, Manning, New Riders, McGraw-Hill, Jones & Bartlett, and Course Technology, among others.

For more information, please visit *http://oreilly.com/safari*.

How to Contact Us

Please address comments and questions concerning this book to the publisher:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
800-998-9938 (in the United States or Canada)
707-829-0515 (international or local)
707-829-0104 (fax)

We have a web page for this book, where we list errata, examples, and any additional information. You can access this page at *http://oreil.ly/2mPWM6p*.

To comment or ask technical questions about this book, send email to *bookquestions@oreilly.com*.

For more information about our books, courses, conferences, and news, see our website at *http://www.oreilly.com*.

Find us on Facebook: *http://facebook.com/oreilly*

Follow us on Twitter: *http://twitter.com/oreillymedia*

Watch us on YouTube: *http://www.youtube.com/oreillymedia*

Acknowledgments

Amanda

I have so many people to thank; the plus of writing your own book is being able to keep going and going and going and...you get the idea. First and foremost I want to give special recognition to my three wonderful boys, Michael, James, and Wyatt. They have started to grow into such independent and amazing little men and without their support and understanding of my long hours over these last couple of years, I

wouldn't be where I am today. My mom for her continued support and encouragement, and for cleaning my house when I travel.

My coauthor Lee has been absolutely amazing. We've both pulled some crazy long hours to get this done. Reviewing each other's work and bouncing ideas off of each other makes for a good friendship and working partner. I couldn't have hoped for a better match. Courtney and the rest of the team at O'Reilly for walking us through this process and answering our stupid questions on a regular basis. They made writing this book a way better experience than I would have ever thought. To Virginia at O'Reilly for doing an incredible final edit. The incredibly intelligent and insightful help from our technical editors, Chris Blow, Mark Boltz-Robinson, Alex Hamerstone, and Steven Maske. Gal Shpantzer for his valuable insight.

I want to thank the coworkers I've had over the years and all of the times you've been there for me, mistakes and all. The people who I consider my mentors; some I've had my entire career, others since starting down the path to information security: Rob Fuller, Bill Gardner, Wolfgang Goerlich, Dave Kennedy, Denao Ruttino, Jayson Street. A special thanks to @_sn0ww for the help with content on physical security and social engineering, and Alan Burchill for his Group Policy knowledge and content. The information security community has helped me to continue to evolve daily while struggling with imposter syndrome and self doubt on a daily basis. You've been there for me when I needed you, to lean on, learn from, teach, and relax. While there are too many of you to list, I've cherished our in-depth conversations over drinks, hangouts, Facebook, Twitter, basements, and every other platform there is out there. Finally I would like to thank my arms for always being at my side, my legs for supporting me, my hips for not lying, and my fingers for always being able to count on them. Thanks for believing in me.

Lee

First of all, I have to thank Amanda for being fantastic to work with throughout the entire process, for all the hard work that she has put into this book, always being a true professional, becoming a good friend, and putting up with my sometimes "fun" calendar.

Courtney Allen for believing in us, endlessly kicking butt on our behalf, getting this whole project started in the first place, providing endless sage advice, and becoming a good friend to both Amanda and myself in the process.

Our technical editors, Chris Blow, Mark Boltz-Robinson, Alex Hamerstone, and Steven Maske, for their feedback and advice.

Virginia Wilson for all of her work to make this happen, invaluable feedback, and huge amounts of reading.

O'Reilly Media for their help and support.

My wife Kirsty, and our children Noah, Amy, and Dylan for being so supportive of everything that I do, having incredible patience, and affording me the time to work on this. Thank you. I love you, x x x.

Ben Hughes, for whom "blame" is perhaps a better word...I jest...sort of :)

There are also a number of other people who make up the exciting Venn Diagram of InfoSec community, colleagues, and friends whom I want to thank for helping me out with this project in terms of emotional support, mentoring, advice, caffeine, and alcohol. To avoid committing some kind of InfoSec name-ordering faux pas, I am going to list these in alphabetical order:

James Arlen, Frederic Dorré, Bill Gambardella, Nick Johnston, Alex Muentz, Brendan O'Connor, Allan Stojanovic, Wade W. Wilson, everyone at DFIRWL, and the 487 other people that I have inevitably failed to mention.

CHAPTER 1

Creating a Security Program

Creating or improving upon a security program can be a daunting task. With so many facets to consider, the more initial thought and planning that is put into the creation of this program, the easier it will be to manage in the long run. In this chapter, we will cover the skeleton of a security program and initial administrative steps.

Do not fall into the habit of performing tasks, going through routines, or completing configuration with the mindset of, "This is how we've always done it." That type of thinking will only hinder progress and decrease security posture as time goes on.

> Humans are allergic to change. They love to say, "We've always done it this way." I try to fight that. That's why I have a clock on my wall that runs counter-clockwise."
>
> *Grace Hopper, "The Wit and Wisdom of Grace Hopper" (1987)*

We recommend that when creating the program, you follow this chapter in order. While we attempted to group the remaining chapters accordingly, they can be followed as best fits a company.

Lay the Groundwork

It is not necessary to reinvent the wheel in order to lay out the initial groundwork for an information security program. There are a few standards that can be of great use that we will cover in Chapter 8. The National Institute of Standards & Technology (NIST) has a risk-based cybersecurity framework that covers many aspects of a program. The NIST Framework Core consists of five concurrent and continuous functions—Identify, Protect, Detect, Respond, and Recover. When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. Not only will a framework be a possible asset, so will compliance standards. Although poorly implemented compliance standards can hinder the overall security of an organization, they can also prove to be a great start-

ing point for a new program. We will cover compliance standards in more depth in Chapter 8. While resources like these can be a phenomenal value add, you must always keep in mind that every organization is different, and some aspects covered may not be relevant (there are continuous recurring reminders of this throughout the book).

Establish Teams

As with many other departments, there are virtues in having the correct staff on the correct teams in regards to security. Open cross-team communication should be a primary goal, as without it the security posture is severely weakened. A good security team consists of the following:

Executive team
: A chief information office (CIO) or chief information security office (CISO) will provide the leverage and authority needed for businesswide decisions and changes. An executive team will also be able to provide a long-term vision, communicate corporate risks, establish objectives, provide funding, and suggest milestones.

Risk team
: Many organizations already have a risk assessment team, and this may be a subset of that team. In the majority of organizations, security is not going to be the number-one priority. This team will calculate risks surrounding many other areas of the business, from sales to marketing and financials. Security may not be something they are extremely familiar with. In this case they can either be taught security basics case by case, or a security risk analyst could be added to the team. A risk framework such as the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework can assist with this.

Security team
: The security team will perform tasks to assess and strengthen the environment. The majority of this book is focused toward this and the executive team. They are responsible for daily security operations, including managing assets, assessing threats and vulnerabilities, monitoring the environment for attacks and threats, managing risks, and providing training. In a large enough environment, this team can be broken up into a variety of subteams such as networking, operation, application, and offensive security.

Auditing team
: It is always a good idea to have a system of checks and balances. This is not only to look for gaps in the security processes and controls, but also to ensure the correct tasks and milestones are being covered.

Baseline Security Posture

The unknowns in any environment are going to be scary. How will you know what level of success the program has had without knowing where it started? At the beginning of any new security program or any deep dive into an existing one, a baseline and discovery phase should be one of the first and foremost tasks at hand for all teams. Throughout this book we will cover asset management several times in different ways. The baseline of the security of the organization is just another step in that management. Items that should be gathered include:

- Policies and procedures
- Endpoints—desktops and servers, including implementation date and software version
- Licensing and software renewal, as well as SSL certificates
- Internet footprint—domains, mail servers, dmz devices
- Networking devices—routers, switches, APs, IDS/IPS, and Network Traffic
- Logging and monitoring
- Ingress/egress points—ISP contacts, account numbers, and IP addresses
- External vendors, with or without remote access, and primary contacts

Assess Threats and Risks

Assessing threats and risks will be incredibly different for each and every organization. Each internal and external footprint is unique when combined with the individual infrastructure involved. Assessing these includes both a high-level overview, as well as in-depth knowledge of assets. Without the knowledge of the threats and risks your organization faces, it is more difficult to custom fit technologies and recommendations to provide a suitable defense. Risk management is often split into four steps: identify, assess, mitigate, and monitor.

Identify

Organizations should be concerned with a large amount of threats and risks that will cross industry verticals. Focusing on industry trends and specific threats will allow the security program to be customized and prioritized to become more efficient. Many organizations have put very little thought into what threats and risks they face on a day-to-day basis, and will continue to do so until they fall victim to them. Invaluable resources in this case are available through Information Sharing and Analysis Centers (ISACs), which are brought together by the National Council of ISACs to share sector-specific Information Security. "ISACs collect, analyze and disseminate

actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency."[1]

Not only should industry-specific threats be identified, but also overall trending threats such as malware, ransomware, phishing, and remote exploits. Two very important places to make note of are the OWASP top 10 and the CIS 20 (previously known as SANS Top 20) Critical Security Controls. Every organization can make use of both these and the standards outlined by the Cloud Security Alliance. The majority of the items on these lists will be covered in more depth in this book, but keeping up-to-date with them year to year should be a key part of any strategic plan.

Assess

After the potential risks have been identified, assess these risks to determine if they apply to the particular environment. Tasks such as internal and external vulnerability scans, firewall rule audits, and asset management and discovery will lend a larger picture to the type of overall risk exposure.

Mitigate

Mitigation of risks is the meat and bones of why we're all here; it's also the purpose of the majority of this book. Options include avoiding, remediating, transferring, or accepting the risk. Some examples:

Risk avoidance
: Dave decides that storing Social Security numbers for customers is an unneeded process and discontinues the practice.

Risk remediation
: Alex starts turning off open ports, implementing stricter firewall rules, and patching endpoints.

Transferring of risk
: Ian outsources credit card processing to a third-party as opposed to storing data on site.

Accepting risk
: Kate knows that a certain endpoint has no access to other endpoints and runs a third-party application. This application has a low-risk vulnerability that is required for it to function. While nothing at that point can be changed or remediated with that vulnerability, the risk is low enough to accept.

1 *https://www.nationalisacs.org/about-isacs*

You should only accept risk as a last resort. If a risk ever makes it to this point, request full documentation from third-party vendors and the executive team, as well as documentation of processes that have been attempted prior to making this decision. Add at least an annual review of any accepted risks to ensure they are revisited accordingly.

Monitor

Keep track of the risk over time with scheduled quarterly or yearly meetings. Throughout the year, many changes will have taken place that affect the amount and type of risk that you should consider. As a part of any change monitoring or change control, determine if the change is affecting risk in any way.

Prioritize

Once threats and risks have been identified and assessed, they must also be prioritized from highest to lowest risk percentage for remediation, with a concentration on ongoing protection. This doesn't always have to be an expensive venture, however. A large amount of defensive mitigations can be performed at little or no cost to an organization. This enables many opportunities to start a security program without having a budget to do so. Performing the due diligence required to get the program off the ground for free should speak volumes to an executive team.

Do not always take vendor or third-party advice for prioritization. Every environment is different and should be treated as such. Prioritize tasks based on the bigger picture when all of the information has been collected.

This book wasn't written to be a sequential list of security tasks to complete. Prioritization can differ greatly from environment to environment. Just remember, if the environment is already on fire and under attack, don't start by creating policies or reversing malware. As a fire marshall, you shouldn't be worried about looking for the arsonist and point of origin when you haven't even put out the fire yet.

Create Milestones

Milestones will take you from where you are to where you want to be. They will be a general progression on the road to a secure environment. This is heading a little into project manager (PM) duties, but in many cases companies do not have dedicated PMs. Milestones can be broken up loosely into four lengths or tiers:

Tier 1: Quick wins
: The earliest milestones to meet should be quick wins that can be accomplished in hours or days—high vulnerabilities such as one-off unused endpoints that can be eliminated, legacy devices that can be moved to a more secure network, and third-party patches all could fall under this category. We will mention many free solutions as the sales process can take a significant time to complete.

Tier 2: This year
: Higher vulnerabilities that may need to go through a change management process, create a change in process, or be communicated to a significant amount of people might not end up in Tier 1. Major routing changes, user education implementation, and decommissioning shared accounts, services, and devices are all improvements that also require little-to-no-budget to accomplish.

Tier 3: Next year
: Vulnerabilities and changes that require a significant amount of planning or that rely on other fixes to be applied first fall into this tier. Domain upgrades, server and major infrastructure device replacements, monitoring, and authentication changes are all good examples.

Tier 4: Long-term
: Many times a milestone may take several years to accomplish, due to the length of a project, lack of budget, contract renewals, or difficulty of change. This could include items such as a network restructure, primary software replacement, or new datacenter builds.

It is helpful to tie milestones to critical controls and risks that have already been identified. Although starting with the higher risks and vulnerabilities is a good idea, they may not be easy fixes. In many cases, not only will these items take a significant amount of time and design, but they may require budget that is not available. All aspects need to be taken into account when creating each tier.

Use Cases, Tabletops, and Drills

Use cases are important for showcasing situations that may put critical infrastructure, sensitive data, or other assets at risk. Brainstorm with data owners and leaders to plan ahead for malicious attacks. It is best to come up with around three different use cases to focus on in the beginning and plan on building security mitigations and monitoring around them. Items such as ransomware, DDoS (Distributed Denial of Service), disgruntled employee, insider threat, and data exfiltration are all good examples of possible use cases. After several use cases have been chosen they can be broken down, analyzed, and correlated to each step of Lockheed Martin's Intrusion Kill Chain.

The Intrusion Kill Chain, sometimes called the Cyber Kill Chain, is "a model for actionable intelligence when defenders align enterprise defensive capabilities to the

specific processes an adversary undertakes to target that enterprise." It is composed of seven steps as described in the Lockheed Martin whitepaper:

1. Reconnaissance: research, identification, and selection of targets, often represented as crawling internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.
2. Weaponization: coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.
3. Delivery: transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payload are email attachments, websites, and USB removable media.
4. Exploitation: After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.
5. Installation: installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
6. Command and Control (C2): Typically, compromised hosts must beacon outbound to an internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have "hands on the keyboard" access inside the target environment.
7. Actions on Objectives: only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration, which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

This whitepaper has a good amount of information that can be used for creating use cases as well.

Table 1-1 is an example of a step-by-step kill chain use case we've created for a ransomware attack.