V E N I M U S , V I D I M U S , V I C I M U S

PRAETORIAN

team survival guide

Issue 08

#08

Sarah Kalmbach
Editor In Chief

CONTENTS

WELCOME

Life is a continuation of experiences and our time is limited. Through your acceptance of this opportunity, you have chosen to disrupt familiarity in the pursuit of something more. You have chosen risk over safety. You have chosen aspiration over satisfaction. You have chosen greatness over good enough. In return, we are committed to providing you an opportunity that you will not find anywhere else. In return, we are committed to ensuring your time at Praetorian encompasses a set of experiences that will remain with you for the rest of your life.

We are embarking on an extraordinary vision and dreams of this magnitude are never easy. The path forward will be extremely challenging, but the friends we find in adversity are those we cherish most. You are not alone in this choice. We will succeed together.

WELCOME TO THE GUARD.

Nathan Sportsman
Founder / CEO

Rise of the PRAETORIAN Guard

NEW RECRUITS

We would like to take this opportunity to welcome you to the Praetorian team.

The strength and integrity of our team defines Praetorian. Together, each one of us creates Praetorian's culture and demonstrates our commitment to provide the highest quality services, research, and products to our customers.

Praetorian is a company that has grown over the years into one of the industry's respected and rising leaders in information security. We will provide you the opportunities to gain expertise in our industry, develop your professional skills, and enrich your professional life. Ensuring the overall professional and personal well-being of our team members is the most important factor in determining our ability to become a viable industry leader. This is a principle we are committed to, as our team members are our number one asset.

Praetorian strives to be an organization where each and every team member has responsibility and accountability. We are committed to achieving excellence in everything we do. We strongly believe that realizing this objective is dependent upon maintaining the overall caliber of our team while continuing to foster a supportive environment in which they can continually thrive.

This Survival Guide was developed to ensure the rapid assimilation of new recruits and to instill in you the core beliefs, principles, and history of today's Praetorian Guard. This artifact memorializes major company events leading up to you being here today. As a new team member, it is your responsibility to familiarize yourself with the contents of this guide. It should be an excellent resource for answering any question you may have about the company's history prior to your recruitment.

YOUR FIRST WEEK AS A PRAETORIAN GUARD

Know what to expect during your first week...
and what we expect of you

For the services team, by the end of your first week you will have identified and pushed your first vulnerability to a customer.

For the product team, by the end of your first week you will have submitted your first pull request.

01

Monday the IT team will provide a provisioned laptop and you will begin the job shadowing process. You will start with a few warm-up exercises to kick-off the week. Reading the company magazine and completing the crossword puzzle are both day one activities. Today we answer the 'why' through an overview of the company's vision, mission, and values. Today you will have a company sponsored lunch with your manager.

02

Tuesday you will be given presentations covering information technology, operations, and finance. In addition, you can use Tuesday to complete any on-boarding paperwork and sign-in to the various solutions that form our tech stack. Tuesday is also the day that you will have your first 1:1 with your mentor. Today you will also have a company-sponsored lunch with your team.

03

Wednesday is for learning about Praetorian's current service offerings and the value that we deliver to our customers. Today you will also learn about Praetorian's current research and development efforts on the product size and Diana's longer term product road map.

04

Thursday is an opportunity to learn how marketing and sales works at Praetorian. You will get time with each department head as they expose you to the core revenue engines of the company. While most positions in the company are technical in nature, it's important for everyone to understand all aspects of the business at a high level.

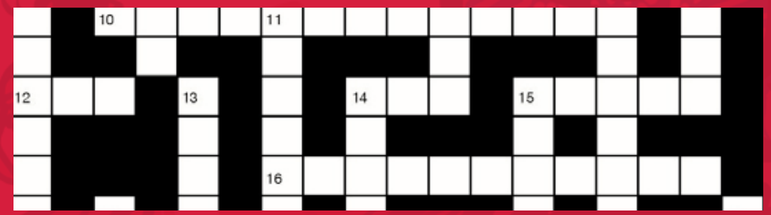
05

Friday is used to finish up any outstanding items from your week one on-boarding and obtain final magazine sign-off from your manager. On Friday, the company celebrates its weekly completions as a team. Finally, kick back and enjoy a virtual happy hour and trivia with the team"

WEEK 1 ASSIGNMENTS

Get Started Checklist

Complete all Get Started Checklist sections, including: Gear up, Identity/Creds, Tech stack, and other new hire items.



Crossword Challenge

Designed to test your knowledge of security terms and introduce you to life at Praetorian, this crossword puzzle will challenge even the greatest of recruits.

Required Reading

Throughout this Survival Guide you will find excerpts and links to full versions of required readings and a list of recommended reading.

Virtual Happy Hour and Teambuilding Event

Enjoy an afternoon virtual happy hour and teambuilding event with the entire company!

GET STARTED CHECKLIST

Enroll

- ❑ Complete I-9 and W-4 forms
- ❑ Enroll in direct deposit
- ❑ Enroll in 401k plan (optional)
- ❑ Review employee benefits
- ❑ Opt-in to health insurance
- ❑ Obtain Capital One card (if applicable)

Readings

- ❑ Read the Survival Guide
- ❑ Obtain copies of recommended books
- ❑ Begin month one readings from Box

Sign-in

- ❑ Okta
- ❑ *10,000ft*
- ❑ *VPN Access*
- ❑ *Lattice*
- ❑ *Box*
- ❑ *Confluence*
- ❑ *Diana*
- ❑ *Expensify*
- ❑ *Gerrit*
- ❑ *Gitlab*
- ❑ *Google Apps*
- ❑ *Jira*
- ❑ *1Password*
- ❑ *Office 365*
- ❑ *Pingboard*
- ❑ *Salesforce (if applicable)*
- ❑ *Slack*

Communication

- ❑ Setup Praetorian email signature
- ❑ Create bio and post it to Box.com
- ❑ Send an email to company@praetorian.com with a blurb about yourself
- ❑ Announce yourself in #warrior-room channel on Slack
- ❑ Join rooms of interest on Slack
- ❑ Connect with fellow Praetorians on your favorite social media platforms
- ❑ Update LinkedIn profile
- ❑ Complete all 9 company presentations
- ❑ Complete meeting with manager
- ❑ Complete meeting with mentor

Survival guide

- ❑ Complete crossword challenge
- ❑ Complete "Assembly" challenge
- ❑ Obtain signature from manager upon completion of this checklist

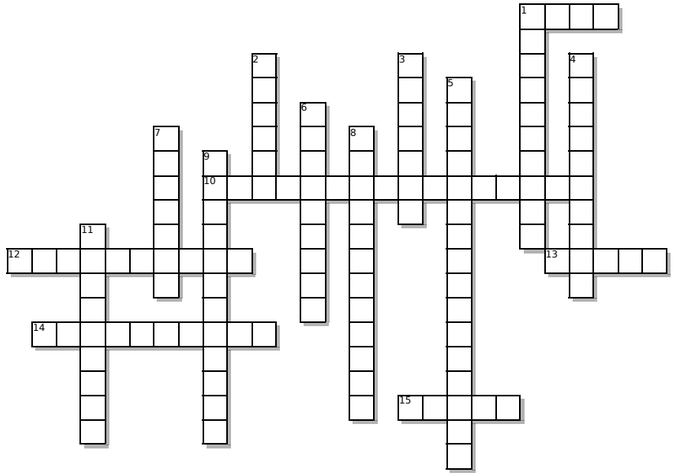
I have completed the requirements assigned to me during my first week of employment.

Teammate signature _____ Manager signature _____ Date _____

CROSSWORD CHALLENGE

This crossword puzzle was designed to test your knowledge of week one learning objectives and introduce you to life at Praetorian.

Answers can be found throughout this Survival Guide. If you get stuck, ask a team member. You should be able to finish this puzzle by the end of week one.



ACROSS

1. If you forget to lock your computer, everyone will know about your professed hate of this animal

10. Metamorphic APT designation acquired during a red team engagement

12. The only existing mathematically unbreakable encryption technique

13. The carbonated energy drink of choice for Praetorian

14. Food court catty-corner from the Austin office. A frequent destination for lunch trips

15. Praetorian pooled their arcade winnings to get this prize, which resides in the office

DOWN

1. Name of the service that Praetorian uses for its Wiki

2. Standard last word for Slack channels

3. Board game where a person must convey an idea to the rest of the players using only tokens and pictures on a board

4. cGxlYXNlaG9sZA==

5. The biggest Lego set in the Austin office

6. Despite this bar's name, you don't actually need a mustache to get in

7. Makes Praetorian more secure, but also can send unintentional and unintelligible Slack messages

8. Nickname of the Corporate Security team

9. At the beginning of each week, a new pun of these gets released

11. If you hear this William Onyeabor song, Schneider is probably the culprit

SURVIVAL GUIDE 101: TECH STACK ESSENTIALS

Get familiar with these tools & services. They will most likely be open on your desktop at all times. These tools allow us to outpace large enterprise competitors who are stuck on legacy systems.

Box

We use Box to store all of our content online, so we can access, manage and share it from anywhere. It also enables us to collaborate on all sorts of documents together.

Predictive Index

PI is used to hire candidates who are hardwired to be a great fit, to design teams that perform like magic, and to manage employees in a way that pushes them to perform at the top of their game.

Expensify

Expensify streamlines the way we report expenses, the way expenses are approved, and the way we export that information for accounting purposes.

JIRA & Confluence

Team collaboration, bug tracking, issue tracking, and project management functions. Confluence and JIRA are like bacon and eggs; coffee and cake; Simon and Garfunkel. Separately, they're great, but together, they're amazing!

Salesforce

Salesforce is used by our Sales and Marketing team but it is important for everyone to understand the power that this platform brings to Praetorian's operations. You'll hear more about Salesforce during the presentations in week one.

Slack

Rally your coworkers with messaging, calls, files and your favorite apps in one place: Slack. Share your work in searchable conversations and automate your team's routine tasks to make everyone's work more productive.

Pingboard

This modern company directory connects employees so you can focus on the team and culture. Everyone in the company has quick access to a powerful org chart that includes contact info, who's out sick or working remote, birthdays and anniversaries, and who knows Ruby or loves to bike.

Okta

Okta is a secure identity cloud that links all your apps, logins, and devices into a unified digital fabric. Praetorian uses Okta to manage employee's access to many applications and devices

BetterWorks

BetterWorks helps manage strategic plans, collaborative goals and ongoing performance conversations. Consider it the operating system for our business, helping everyone get aligned, engaged and executing more effectively.

Diana

Diana is a freemium orchestration and automation platform that allows our customers to connect all their disparate security tools in their CI/CD pipelines into one central view.

1Password

1Password is used to generate, store, and retrieve complex passwords. 1Password is there when you need to login, generate a password for a new site, or access shared company credentials. Please note: Praetorian recommends using the 1Password desktop app but not the plug-in, due to potential security vulnerability issues.

Lattice

Lattice is the people management platform that empowers us to build engaged, high-performing teams and inspires our culture.

The Reading List

Books we've all read, that have evolved our thinking as a company, and that we refer back to constantly

BUSINESS READING

Creativity, Inc

Reminding us of the importance in defending the new and overcoming the unseen forces that stand in the way of true inspiration.

Only the Paranoid Survive

Strategies that companies can adopt to survive – and even exploit – those sink-or-swim moments in a company's existence.

High Output Management

Managers must constantly enhance value by learning and adapting to a changing, often unpredictable business environment.

Radical Focus

OKRs are a tool to help teams focus on their goals, creating a framework for regular check-ins and the beauty of a good fail.

First, Break All The Rules

Learn how great management differs from conventional approaches and the key notions that great managers use in their jobs.

The Hard Thing About Hard Things

Practical wisdom for managing the toughest problems business school doesn't cover.

Principles

Finding truth is the best way to make decisions. Strategies to circumvent ego, emotion, and blind spots that prevent you from discovering the truth.

Work Rules!

An inquiry into the philosophy of work - and a blueprint for attracting the most spectacular talent to your business and ensuring that they succeed.

The Monk and The Riddle

Focus on being happy and doing things that make you happy today, instead of deferring to a 'better time'. Find passion and purpose in what you do.

Team of Teams

Create shared consciousness in your organization by sharing information and building genuine relationships and trust.

A Message to Garcia

The greatest hero is someone who simply does their duty, completing the task no matter the obstacles.

Thinking: Fast And Slow

A tour of the mind that explains the two systems that drive the way we think and the way these systems shape our judgments and decisions.

PRODUCT SECURITY READING

Web Application Hacker's Handbook

This recommended reading will serve as a practical guide to discovering and exploiting security flaws in web applications.

The Hardware Hacker

Focusing on the ins and outs of open source hardware, The Hardware Hacker is an invaluable resource for aspiring builders and breakers.

The Art of the Software Security Assessment

This book is highly recommended to members of Praetorian's ProdSec team. It approaches software assurance as an engineering discipline.

The Tangled Web

Thorough and comprehensive coverage from one of the foremost experts in browser security.

Hands-On AWS Penetration Testing with Kali Linux

Identify tools and techniques to secure and perform a penetration test on an AWS infrastructure using Kali Linux.book.

iOS & Android Hacker Handbooks

Discover security risks and exploits that threaten iOS and Android mobile devices.

CORPORATE SECURITY READING

Advanced Penetration Testing

Go beyond Kali linux and Metasploit to learn advanced, multidisciplinary pen testing approaches for high security networks.

Windows Sysinternals

Delve inside Windows architecture and internals, and see how core components work behind the scenes.

The Go Programming Language

The authoritative resource for any programmer who wants to learn Go. It shows how to write clear and idiomatic Go to solve real-world problems.

Learn Windows Powershell in a Month of Lunches

Just set aside one hour a day for a month, and you'll be automating Windows tasks faster than you ever thought possible.

Red Team: How to Succeed By Thinking Like the Enemy

An in-depth investigation into the work of red teams, revealing the best practices, most common pitfalls, and most effective applications.

Gray Hat C#

Learn to use C#'s set of core libraries to automate tedious yet important tasks like vulnerability scans, malware analysis, and incident response.

Start With **WHY**

The security industry's priorities are upside down with a fixation on community status rather than a fixation on customer success.

by Nathan Sportsman

For reasons that stem from its counterculture roots of the 80s and 90s, the industry exerts too much of its energy on a destructive "break all the things" mindset, on creating images of celebrity status and self-validation, and on framing a hierarchal status between peers and competitors. In this unproductive worldview, the security community has created more problems than it has solved. With over two decades under its belt, the security industry has completely failed in its halfhearted attempts to respond to the rising dangers of a more interconnected world. Given how our industry chooses to spend its time, this is not surprising. It's just sad.

Even worse, and in some perverted attempt at self-perpetuation, many security vendors leverage internal security research as marketing collateral for sensationalizing news headlines, extorting client verticals, creating community currency, and/or for publicly shaming software and hardware manufacturers. How does this help solve anything?

Where is the iconic security company of our day? The one that sets the example and defines what great looks like. Where is the Tesla or SpaceX of our industry? The one that they will write about 100 years from now. The brand that causes future security engineers to dream. Where is the Elon Musk of the security community? The one whose ultimate mission is more important than any risk taken or any reward given. Where is the company that I'd be proud to work for?

Our pejorative view of the security community has created a schism between us and the rest of our industry. We have decided to take the road less traveled where we are hyper focused on building a different kind of security company — one that reframes the conversation, celebrates customer success, and moves society forward. In a fragmented market of failed security land grabs and constant acquisition exits, we set out to claim our future while others sell theirs short. We enter on our own terms. We create something where nothing existed — a company to call our own.

In a crowded sea of sameness, we are often asked why we even started a security company. We founded Praetorian to end the status quo. We founded Praetorian to solve a real problem. We operate with absolute resolve and long-term conviction in our mission of securing our future and making the world a safer and more secure place.

FROM PUBLIC SECTOR TO PRIVATE SECTOR

by John Novak

One of the things Praetorian prides itself on is having a collective of highly technical talent from across the security industry. Listening to the CEO during your first week at Praetorian, it's clear that the talent comes not only from companies like Symantec, McAfee, Sun Microsystems, RedHat, Google, and Microsoft, but also includes former public sector employees from the National Security Agency, Central Intelligence Agency, Idaho National Laboratory, and Lawrence Livermore National Laboratory.

As someone who spent over a decade in the public sector, the shock of moving to a fast-paced company like Praetorian was something I fully expected but still took some getting used to. Before, I might have spent months or years on the same project, whereas now, it's rare to spend more than a month with any one client. The rapid pace of engagements and technical work is a refreshing change and constantly keeps me on my toes.

Along with a good helping of technical work to keep me engaged, Praetorian has given me a great amount of responsibility when it comes to contributing and growing the company. In the public sector, it took me years to climb the GS scale and pursue projects or assignments I deemed important. Now, within six months of working at Praetorian, I've already learned our business flow enough to work on solo engagements, earned the coveted OSCP certification, and worked to shape the future of our company through university recruiting events. This same responsibility and freedom is given to every employee whether they have an extensive background or are a fresh recruit out of college.

Another challenge some face in transitioning to the private sector is finding a company that shares the same noble values that drove and motivated committed employees in the public sector. My prior employment specifically focused on service, loyalty, lawfulness, and integrity. These promote one of the best virtues of the public sector; namely, a pledge to work for your country and do so while retaining the trust of the American public.

At Praetorian, we share our own unique set of values proudly on our website. These values not only encompass my prior employer's values, but they take it a step further. Praetorian's values also promote innovation, teamwork, and passion for what you do. Our core business values go beyond the external facing business and dive into what truly makes the business great — the people. Each person embodies these values and takes them to heart from day one; whether it's putting together a client report the night before Thanksgiving, 'putting the client first', or completing all five of Praetorian's tech challenges, just because you 'love the work you do'.

There were still a couple things I haven't gotten used to yet. A few times before we were about to kickoff a new engagement with a client, we found out that the contract had not been fully signed. Most of the time this is due to the fast pace of business in the private sector. In my former job, I would have scrambled to "pull strings" and get the right management supervisor to address this particular issue. At Praetorian, I can trust the company "to orient to action" and address it immediately so that I don't have to use my time and talent on bureaucratic tasks that don't directly contribute value to the customer. Going even further, there is a continuous push to automate simple or repetitive tasks at Praetorian so that employees can focus on the truly interesting work. This propensity to get things done shows just how much Praetorian values its employees and clients.

Since day one I've been excited to work with the highly skilled group of individuals around me at Praetorian. I believe this culture will push me to gain many new skills that can be reinvested into this fast-growing company.

GUIDING PRINCIPLES

It can be accepted as a new axiom that the importance of security will continue to increase as technology continues to extend. It's a brave new world where security, as one of the great technical challenges of our day, presents unending opportunity to do real and permanent good.

In a fragmented market of failed security land grabs and constant exits, we set out to claim our future while others sell theirs short. Picked up by the bootstraps, we enter on our own terms. We create something where nothing existed — a company to call our own.

1. **Default to open.**
   Bias toward brutal truth over hypocritical politeness.
2. **Orient to action.**
   Make decisions. Make mistakes. Just take the initiative.
3. **Lean into Discomfort.**
   Growth and innovation comes from tension and change.
4. **Be humble.**
   Constantly pressure test your opinions, convictions, and believability.
5. **Yes, and...**
   Start with yes by encouraging new ideas and expanding on them.
6. **Follow your passion.**
   If your vocation is your avocation, you will never work a day in your life.
7. **Put the customer first.**
   Everything else will work itself out.
8. **Make craters.**
   Find success and meaning through impactful work.
9. **Performance matters.**
   This is a small company trying to do big things. Every individual effort counts.
10. **Try harder.**
    Failure is inevitable, but fortitude will prevail. Nothing is impossible.
11. **Struggle and celebrate together.**
    Everything we do, we do as a team.

VISION

To solve the cybersecurity problem.

MISSION

To make the world a safer and more secure place.

Praetorian Guard by Madspeitersen

BUILDING A CULTURE OF EXCELLENCE

These core principles are critical to the success of creating a strong culture at Praetorian. You should think of these values as the DNA of Praetorian's company culture. Defining our values in this way creates the foundation from which culture can be built in a clear, intentional way. If they are living by these clearly defined values, team members will have different ideas about what the culture of the company is supposed to be and what is expected of them.

These defined principles serve as the basis for institutionalizing Praetorian's culture; that is, putting in just the right amount of structure at the appropriate time to ensure that the intended culture scales as the company grows. These values, and the set of key associated behaviors that embody them in our company, should be invoked when making key strategic and tactical decisions. Do so, and you will help create a truly extraordinary company.

THE VOICE OF THE CLIENT

by Thomas Reburn

At Praetorian we have a culture of client obsession. We believe our success hinges on not only meeting but exceeding expectations. One method that we use to gauge client satisfaction is the Net Promoter Score (NPS) system.

The NPS survey asks customers a simple question on a scale of 0 to 10: "What is the likelihood that you would recommend Praetorian to a friend or colleague?" Those who answer 9 or 10 are considered "promoters" and those answering 0-6 "detractors." Subtracting the percentage of detractors from the percentage of promoters yields your NPS. In 2018 the NPS for popular companies varied: Apple had a 72%, Netflix a 68%, and Amazon a 62%. Praetorian has a lifetime NPS of 87.7%.

The information Praetorian collects alongside the NPS arguably is more valuable than the rating itself. We have learned the importance of understanding the context behind each client's score.

HERE ARE COMMENTS FROM A FEW OF OUR NPS PROMOTERS:

NPS 10	"Excellent and consistent project management. Very capable technical staff."
NPS 10	"As usual, loved both the service and the value we got out of the testing."
NPS 10	"It was great to work with a very organized, technical and knowledgeable team. The team took the time to understand our environment before diving in and was very thorough in their assessment. We appreciate the daily status update on tasks that have been completed and providing us heads up on upcoming tasks. That made it easier for us to line up internal SME to assist with the engagement. Anna and the team provided great post-assessment finding summaries and did a great job of walking us through the report."
NPS 10	"The team has provided exceptional service, guidance, and consideration toward some of the unique challenges we face currently at Coty. The level of transparency, technical resolve, and adaptability allowed for not only a smooth engagement, but also meaningful conversation internally with stakeholders, driving truly demonstrable value. Overall, another great experience working with the team at Praetorian from start to finish."
NPS 10	"The entire Praetorian team was extremely professional throughout the project and took the time to address any questions and/or comments that arose. This engagement exceeded our expectations and the quality of work outputted by the Praetorian team was excellent."

As we earn new business and work with clients who return over the years, we use this feedback to ensure our most effective processes and most beneficial cultural elements remain consistent as we grow. NPS is a capstone measure of impact and helps capture the voice of the client, from our first introductory call through years of collaboration.

INC 5000

by Alex Ionescu

"IF YOUR COMPANY IS ON THE INC. 5000, IT'S UNPARALLELED RECOGNITION OF YOUR YEARS OF HARD WORK AND SACRIFICE."

PRAETORIAN NAMED AN INC. 5000 FASTEST-GROWING PRIVATE COMPANY FOR SEVENTH CONSECUTIVE YEAR

In 2020 Praetorian was included for the seventh consecutive year on Inc. Magazine's 39th annual Inc. 5000 list, the most prestigious ranking of the nation's fastest-growing private companies. We are proud to be included in the Inc. 5000 list, which represents a unique look at the most successful companies within America's most dynamic economy segment—its independent small businesses.

Inc. editor in chief James Ledbetter has said of companies inclusion in the list that, "it's unparalleled recognition of [their] years of hard work and sacrifice. The lines of business may come and go or come and stay. What doesn't change is the way entrepreneurs create and accelerate the forces that shape our lives." Microsoft, Dell, Domino's Pizza, Pandora, Timberland, LinkedIn, Yelp, Zillow, and many other well-known names gained their first national exposure as honorees on the Inc. 5000.

Every year a group of Praetorian shareholders is invited to attend the annual three-day event that brings the nation's brightest, most successful business minds together to celebrate the remarkable achievements of companies named on this list. The 2019 Inc. 5000 Conference and Gala took place from October 10-12 at the JW Marriott Phoenix Desert Ridge & Spa in Phoenix, Arizona.

The Inc. 5000 Conference featured renowned entrepreneurs and business experts from widely admired brands like Zoom Video Communications, US Mobile, and KnowBe4, who delivered three days of thought-provoking sessions. We gained powerful business insights to share with our colleagues, and applauded our entire team's hard work during the final evening's black tie gala. It was the perfect opportunity to toast to Praetorian's success during an evening of celebration, complete with cocktails, dancing, and a gourmet three-course meal. Ken Jeong, comedian and star of the television show "Community", kept us laughing all night as the master of ceremony.

The 2019 Inc 5000 Conference provided a special moment to pause and celebrate what we have accomplished as a collective, and an injection of new business ideas to help us increase momentum and growth. The future is bright at Praetorian and there is a lot more work to do.

Travel Perspective, AMSTERDAM

by Thomas Hendrickson

I once was, arguably, the most significant contributor to a losing trivia endeavor on a Tuesday night at a college bar. Hold the applause. Obstinately staying true to my superior knowledge, emboldened by half of the cheapest grain based beverage from the menu, I convinced my teammates that the Van Gogh Museum resides strictly within the city radius of Arles, France. Our team captain, a washed up high school trivia jock, futilely insisted that he had, in fact, visited the Van Gogh Museum and furthermore, claimed his rendezvous with Vincent's work occurred far outside the city radius of Arles, France. Impossible; I myself had been there not two years back. Our submission was Arles, end of discussion.

Skip ahead to last year, when I had the opportunity to travel to Amsterdam to work onsite with one of Praetorian's clients. The trip was my first to Holland's capital city, and I was excited. My overnight flight landed early Sunday, so I spent the first part of the day wandering around half asleep in the Rijksmuseum. Rembrandt's works looked as impressive as the hundreds of art history textbooks say they are, but perhaps not quite as good as lunch tasted later that afternoon. That evening I relaxed at an Irish pub watching the opening games of the European soccer ("football") season.

The following week passed by quickly. Our client was easy and accommodating to work with, and my Praetorian colleague and I continuously made good progress on our project. In the mornings I occasionally went for a run in the nearby Vondelpark. After the trip I read a news article that discussed how a member of the Dutch royal family frequently commutes through the same Vondelpark in the mornings. Perhaps I unknowingly jogged next to them. Spending time in Amsterdam is easy, as there is always a new restaurant recommendation to evaluate or a famous site to see. On Thursday we asked our clients for dining recommendations and received significantly more recommendations than meals left in our trip.

Friday night I realized my flight departed in the afternoon the following day. So, I decided to spend the next morning going to one of the most famous museums in the city: the Van Gogh Museum. Yes, yes, I was wrong that day at trivia. The Fondation Vincent Van Gogh Arles is a completely different institution than the Van Gogh Museum in Amsterdam. I cost my team third to last place and we tragically failed to recover, never playing another trivia game again. Regardless, I showed up Saturday morning to the museum bright and early, thirty minutes before doors open only to discover that all tickets were sold out. I reluctantly paid twenty dollars to enter the nearby Stedelisjk Museum showcasing modern art, about which I have no comment. But at least I know to buy tickets in advance for the Van Gogh Museum the next time I travel to Amsterdam for work.

The INVESTIGATIVE Mindset

Incident response is when the cybersecurity good guys meet the cybersecurity bad guys. Our customers are in trouble, and they need our help. Whether it's ransomware, theft, fraud, or a full network compromise, our customer needs accurate information and expert recommendations. They need to make informed decisions quickly.

by Andrew Cook

The aftermath of a cybersecurity incident always is chaotic. Everyone has questions, answers can be contradictory, and priorities clash. Successfully managing this phase is not about what forensics tools you can use, what log sources you can parse, or what malware you can reverse engineer. **It is, however, about your ability to discern the reality of the situation, prioritize competing concerns, ask good questions, and provide confident answers and recommendations based on evidence.**

That is where we find ourselves as incident responders. Where do you begin? Get your detective hat on, you'd better start investigating.

PERCEPTION VS REALITY

Investigations exist to uncover the truth. Everyone comes to an incident with biases and preconceived notions of what they think happened. Without an investigation, this interpretation is largely speculative and may not match reality. Without an understanding of the truth, our response could fail to stop the damage or even can make things worse.

Praetorian has been brought in on a few incidents after the victims' initial responses. In each case, the client had reacted based on what they thoughthappened rather than what they knewhappened. In one case, a client had spent days rebuilding from a ransomware attack only to be re-infected because they never remediated the backdoors. Our follow-on investigationensured they could restore their network with confidence.

Our first job as incident responders is to bridge the gap between people's perception of what happened and the reality of what actually happened. This increases our confidence that the actions we take thereafter are appropriate, measured, and effective. Responding to an incident based on guesses, hunches, or speculation is dangerous. Reactions based on fear, for example, can lead customers to take drastic and unnecessary actions that do more harm than the incident caused in the first place.Guiding people with different backgrounds, experiences, and motivations to converge on a shared understanding of reality is difficult, so Praetorian uses a model that everyone can understand. This is where the simple yet powerful concept of timelining comes in. A timeline of the incident's events, backed by evidence, is a powerful tool for describing reality and deciding what we need to do next.

ALWAYS BE TIMELINING

The most important model we have to represent our understanding of reality is a timeline of the incident. The idea is simple: add an entry for every event and tag it with the evidence. Be specific. Sometimes a difference of a few seconds can significantly alter our understanding of events.

The simplicity of a timeline makes it an important tool in managing complex incidents. Our confidence that our perception matches reality is backed by the rigor of our timeline. The timeline keeps us honest. For example, neither Praetorian nor a client's cybersecurity staff can claim the initially compromised system is a vulnerable and exposed Internet-facing server (an obvious choice) if another system was actually compromised four minutes prior.

When we start an investigation, our first task is to put what littlewe know on the timeline. These first events are largely drawn from interviews with the customer about their initial observations of the incident. This is our time to ask a lot of "When" questions about the events leading up to our arrival. When did the computer crash? When did you block the IP address? When did the alarm trigger? The customer typically does not have their answers down to the minute, and that is expected in the initial stages. We just need somewhere to start our analysis.

With our timelin begun, we then start asking questions. Questions are key to progressing our investigation, improving our timeline, and discovering the truth. But with so many possible questions, on which ones should we focus?

ASKING GOOD QUESTIONS

In forming good questions, we start with our timeline. Based on what we know so far, what would we expect to have happened before, after, and in-between? The more our questions are grounded in the truth and accuracy of our timeline, the more likely those questions will be well formed and worth answering. Conversely, questions that are not based on our timeline tend to be guesses that have no basis in reality and therefore are unlikely to give us any meaningful answers.

Each questions represents an investment and is expensive to investigate. Our goal is to "buy" the questions that give us the most significant return. The best questions are those that address the business concerns of the customer, mitigate damage, and resolve the incident. That generally means questions like "What was the first system compromised?" and "How many customers were affected?" are high priorities. These are questions that demand action and enable our customer to make informed decisions.

Low on the list of priorities are gee-whiz questions that, while interesting, have no impact on how our customer will respond or what we can do next. For example, a simple question with a complex answer is "Who did this?" For most incidents, the "who" questions tend to be expensive distractions. Regardless of the answer, they generally have no impact in how the customer responds or what can be done next.

The difference between a good investigator and a great investigator is the ability to ask and prioritize the right questions. But the second half of the battle is answering them. This requires evidence.

GETTING ANSWERS

Locard's exchange principle is a key concept in forensics. In short, it means that a criminal's interaction with the crime scene will leave evidence. This is the type of thinking that brought us Sherlock Holms. An investigator's is to find the evidence, analyze it, and draw accurate conclusions.

Digital forensics is the most technical piece of incident response. Not only does an engineer need to understand where traces of evidence may be, they must also know how to interpret it. Oftentimes the answers we need are hidden away in some complex data from logs, memory, forensics artifacts, security devices, malicious binaries, network captures, and more.

Interpreting evidence can be complicated. Worse, misinterpreting evidence can be dangerous. For example, minor differences in two systems' clocks may completely swap the order of events in our timeline causing us to misdiagnose the root cause. In some cases, a key answer comes down some esoteric knowledge of how a program works: misunderstand the data is tellingand risk leading the customer down the wrong path.

Therefore, whenever we tell a customer something based on evidence and analysis, we are very specific about what it means and how confident we are. Grandstanding and faux confidence have no place in incident response. Praetorian's clients want honest answers based on the evidence available, and nothing more.

CONCLUSION

An investigative mindset is key to a successful incident response. Without an investigation, we cannot be confident that our response was effective or appropriate. A skilled investigator is able to manage multiple priorities, know what questions are worth investigating, and understand what to do based on the answers. Remember: bad guys can be tricky, but evidence can be trickier.

** Want to learn more? Check out the online course **Investigation Theory** by Chris Sanders.*

The NIST CYBER SECURITY Framework as a Baseline for *Security Assessment*

by TrevorSteen

At Praetorian, we underpin our security assessment approach and product lines with a robust, methodical, defensible framework to ensure clients fully understand their security posture. The National Institute of Standards and Technology (NIST) originally published its Cybersecurity Framework (CSF) in 2014 as a guide for government organizations and entities that support critical infrastructure to develop and improve cybersecurity programs in a manner that was descriptive rather than prescriptive. In April of 2018, the NIST released version 1.1 of the framework, which makes the outcomes applicable to all industry sectors and all organization sizes. Praetorian uses the NIST CSF as our baseline because the framework provides a much more holistic view of an organization's cybersecurity posture by acknowledging the business components of cyber risk, and by addressing the full spectrum of cybersecurity activities.

The structure of the framework acknowledges the varying degrees of business risk clients are willing to tolerate in their cybersecurity programs. The CSF is composed of five discrete functions that represent the five aspects of an organization's security posture: Identify, Protect, Detect, Respond, and Recover. In order to determine the level of cyber risk, an assessment would consider 108 sub-categories representing discrete outcomes in cybersecurity, organized under 23 broader categories representing general outcomes that directly relate to one of the 5 key functional areas.

The alignment of functions, categories, and subcategories aid Praetorian in developing both a current state and target state profile for an organization. The target state profile distinguishes NIST CSF assessments by considering an organization's security shortfalls based on risk, rather than the minute detail of raw findings emphasized by more common approaches. In other words, an organization's target state profile will determine whether a low-scoring sub-category will even matter to an organization.

In order to best develop the target profile and provide actionable recommendations for customers, Praetorian's implementation of the NIST CSF includes a threat modeling phase where we seek to understand critical business activities, major risks to those activities, and the threats that might cause those risks to be realized. With these factors understood, we can develop an accurate target profile to ensure we are properly benchmarking the organization. This process ensures that we do not have the same cybersecurity expectations for a customer who offers employment assessments as we have for a customer who develops medical implant devices.

For example, the broadly used CIS CSC Top 20 dictates that inventories of physical assets should compile information from an active method, a passive method, and via DHCP logging. In most organizations, this level of redundancy is neither necessary nor warranted. The NIST CSF simply states "Physical devices and systems within the organization are inventoried." This generalization supports business driven definition of the required controls to evaluate this specific category and to bring the associated risk within an organization's risk appetite.

By layering the business-compatible flexibility of the NIST CSF with Praetorian's other service lines, our engineers have powerful tools to solve our clients' problems rather than simply completing a check list of security boxes. The Identify function equates to our defensive enablement offering where we help to build and deploy tools that specifically aid in creating a solid foundation for an organization. Protect and Detect each align with Purple Teams and penetration tests where we validate that both processes and tooling can defend against the most common attacks. Respond and Recover correlates to our Red Team offering where we emulate the attacker to fully understand how an organization will react to a realistic attack scenario. In addition to these direct alignments between functions and service lines, the NIST CSF assessment also gathers the necessary data to understand critical components and dependencies for an organization that then inform exception of our other service lines.

To further ensure precise ratings and assessments, Praetorian utilizes the Capability Maturity Model to assess each NIST CSF sub-category for people, processes, and technology. Furthermore, in cases of inconsistent resource application across an organization, "dimensions" can provide finer granularity beyond what the CSF provides natively. For example, inventories of physical assets may be different for servers, workstations, and virtual machines, each of which could be their own dimension. The ultimate result is a summary of ratings at the category and function levels. With the fine granularity of sub-category and dimension assessments and the broad summary of categories and functions, organizations can make smart, efficient, and appropriate decisions about their cybersecurity programs.

Our clients require a well-defined, defensible, and repeatable assessment construct to drive internal decision-making processes about what people to hire, what tools to buy, and what processes to spend time developing. By using the NIST CSF as a baseline assessment, Praetorian helps organizations identify the exact areas that require improvements without fear of superfluous resource allocation or a poor return on investment. Coupled with recommendations from our dense talent pool and deep breadth of experience, our clients can understand their current state and begin to improve their security posture in a meaningful way.

Problem Solving:

GRAPHS AND MACHINE LEARNING

by Matt Kindy

One of the most interesting things about working in machine learning is the wide range of problems that can be attacked. From natural language processing (NLP) to image recognition and malware detection, machine learning has been used to do it all -- and in so many different ways!

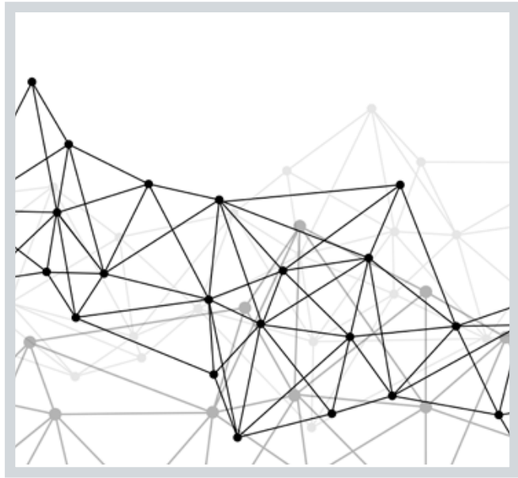
Applications exist for a broad range of interests, including convolutional or recurrent neural networks (CNNs/RNNs), attention mechanisms, or even more specialised things like denoising autoencoders. One type of data, however, seemed to consistently be outside the reach of machine learning: graphs! Until recently, no well-defined way of dealing with graphical information in neural networks (in particular) existed, despite the fact that machine learning technology had been able to deal with sequential and two-dimensional data for quite some time. In response to this gap, software engineers have developed graph neural networks (GNNs).

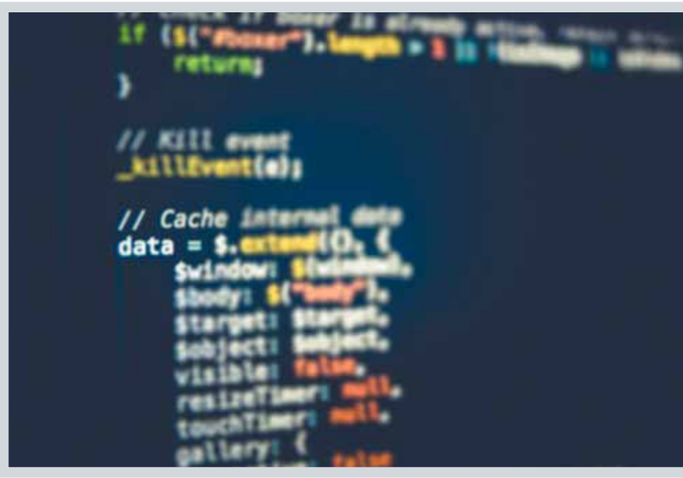
WHY USE GRAPHS?

At Praetorian, the machine learning team has been focused on the problem of finding certain classes of security vulnerabilities, like SQL injection, in source code. We had focused originally on an NLP-based approach from amongst the breadth of potential approaches to the problem. "Source code is meant to be read by machines, but it's also meant to be read by people," we reasoned, "so code is a form of natural language." During our experiments and interactions with security engineers, we found more evidence to support this idea.

One of the hard things about source code, though, is that it is not just natural language. Source code has a structure which is somewhat order-dependent (think of statements in a function) and somewhat not (think of the order of functions in a class or a file in some languages). Source code can be partially generated during build phases (e.g. Lombok annotations in Java), not to mention other forms of meta-language incorporated by other dependency injection frameworks. Finally, sometimes a word is not just a word: where that word comes from matters. Applied to our case, whether a function executeStatement came from a local logging class or a command execution library matters a lot.

Graphs provide a way to incorporate all of this messy and somewhat disparate information into a structured format. Whether the graphs are abstract syntax trees (ASTs), program or system dependence graphs (PDGs/SDGs), call graphs, or control flow graphs (CFGs), they all contains information that helps clarify the ambiguity of the "natural language" of code.





THE HARD PART

We spent the last several months developing the right graphs for the right data. For novel problems, data is certainly the hard part. Ultimately, we explored the experimental parts of some open source static analysis tools, extended upon them, and fixed some bugs along the way!

Now we face some engineering challenges: How do we train over large numbers of massive graphs efficiently? Maybe more importantly, how do we integrate this into a production pipeline? How will we iterate quickly on this idea, making sure to continuously deliver value to our clients and security engineers along the way?

Now that is the really hard part.

CLIENT COLLABORATION AT ATT&CKcon

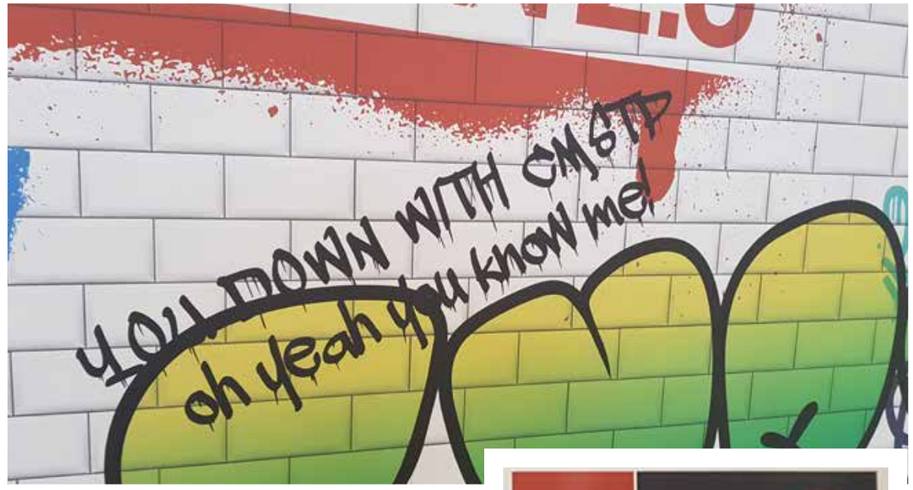
by Daniel Wyleczuk-Sterns

I had given presentations in my roles at the Air Force and at Praetorian but stepping onto the stage at ATT&CKcon 2.0 certainly felt different. First, I had never been live streamedacross the world before. At a second and deeper level, my previous talks had involved speaking to an inherently friendly and known audience.

My nerves did not strike until the event staff began hooking on my microphone. As I sat down in the "batter's box" my heart and stomach joined forces and shouted up at my brain, "What are you doing? Flee!" As I forced myself to walk to the stage, my thoughts turned to the relationship and email that had brought me to this point.

What felt like an eternity ago, I received a message from Matt Southworth, the CISO at Priceline. The travel company is well known for their old commercials with William Shatner. What I knew them for was their incredible security team. I have had the pleasure of working with Matt and his staff on a number of projects while at Praetorian, and during our Purple Team engagements we had established an extremely successful collaborative approach to identifying and improving detection gaps. Matt was proud of the progress that we had made, so he reached out asking if Praetorian wanted to co-speak with him at the SANS Purple Team Summit and at ATT&CKcon. Speaking at a conference appealed to me, so I took him up on his offer to collaborate in this new way.

After both conferences accepted our presentation proposal, we behaved like any speakers at an infosec conference—we procrastinated. We assembled an uninspiring first draft as the deadline for slide submissions approached, and at that point we realized that we lacked a cohesive theme. As we deliberatedamongst unifying ideas, Matt stated that the reason he kept returning to Praetorian was that our engineers do not come into a project trying to prove a point or flex intellectual muscles. Rather, we begin with a genuine interest in solving the client's toughest problems, which leads to an environment where we work together. And thus, we had our theme: collaboration.



In a trip to NYC, Matt and I drafted a far more cohesive set of slides, then sent it to Praetorian's marketing guru for polishing. As a finaltouch, I incorporated some much-needed pictures of cats. We then rehearsed until we felt comfortable enough to wing it if all the technology failed while we were on stage. The entire process gave a new meaning to collaborative preparation for the worst-case scenario, but we were more than prepared.

When I stepped onto the stage at ATT&CKcon, my mind went fairly blank. Fortunately, Matt had the first slide so I had a few seconds to compose myself. As soon as the first few words came out, the content began coming back to me, even more naturally than in practice. I was not just reading words off a slide; I was speaking about a methodology in which I firmly believe.

Together, we introduced a tested and successful method to consider when planning multi-organization security efforts. At the end of the day, I hope our presentation led others to adopt a more collaborative approach to make the world a safer and more secure place. I am incredibly thankful to Matt and Praetorian for making this incredible opportunitya reality.

PUBLISHER

Matthew Kindy
Andrew Cook
Daniel Wyleczuk-Stern
Thomas Reburn
Alex Ionscu
Thomas Hendrickson
Trevor Steen
Sarah Kalmbach

EDITOR'S OFFICE

Praetorian
98 San Jacinto Blvd.,
Suite 500
Austin, TX 78701
www.praetorian.com
info@praetorian.com

CROSSWORD KEY:

Handlebar / Despite this bar's name, you don't actually need a mustache to get in

Sword / Praetorian pooled their arcade winnings to get this prize, which resides in the office

Tigres / Standard last word for Slack channels

Fairground / Food court catty-corner from the Austin office. A frequent destination for lunch trips

Clean / The carbonated energy drink of choice for Praetorian

Atomibomb / If you hear this William Onyeabor song, Schneider is probably the culprit

Concept / Board game where a person must convey an idea to the rest of the players using only tokens and pictures on a board

Yubikey / Makes Praetorian more secure, but also can send unintentional and unintelligible Slack messages

MillenniumFalcon / The biggest Lego set in the Austin office

Cats / If you forget to lock your computer, everyone will know about your professed hate of this animal

Confluence / Names of the service that Praetorian uses for its Wiki

MondayPunday / At the beginning of each week, a new pun of these gets released

OneTimePad / The only existing mathematically un-breakable encryption technique

Teamzerowing / Nickname of the Corporate Security team

Obsidianpresence / Metamorphic APT designation acquired during a red team engagement

pleasehold / cGxlYXNlaG9sZA==