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 #09

Nathan Sportsman
Editor In Chief

Start with *Why*

Perspective:
Cloud and Beyond

A Day in the Life:
Labs

DEI: Reflecting
the World We Want
to Protect

Building Culture in
a remote world

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.

Nathan Sportsman
FOUNDER / CEO

praetorian

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 AT PRAETORIAN

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 you will meet with the People Ops and IT teams to get your laptops provisioned and an initial intro into our systems. 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 and our strategy. You will also meet your manager and mentor today to begin getting the lay of the land.

02

Tuesday you review presentations covering Operations and People Operations. In addition, you can use Tuesday to complete any on-boarding paperwork and sign-in to the various solutions that form our tech stack. Today you will also have a company-sponsored lunch with your team.

03

Wednesday is for learning about Praetorian's Marketing and Sales offerings. 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.

04

Thursday is an opportunity to learn about Product and Engineering. You will learn about Chariot and the value we deliver to customers. You will have the opportunity to learn more about our current R&D efforts on the product side and Chariot's longer term roadmap.

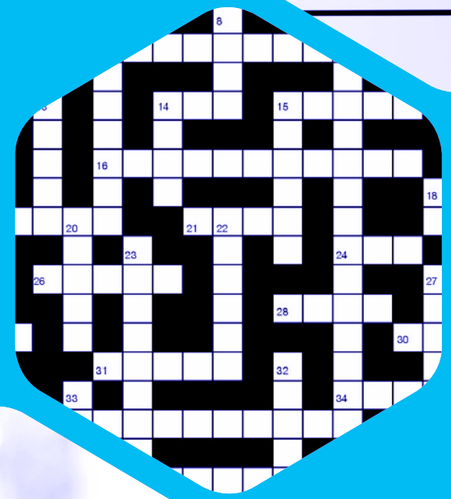
05

Friday is for learning about Praetorian's current service offerings and the value that we deliver to our customers. At Praetorian, we are offering our clients outcomes and not hours billed - this is your opportunity to learn more about this approach.

WEEK 1 ASSIGNMENTS

Get Started Checklist

Complete the items outlined in Greenhouse Onboarding.



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

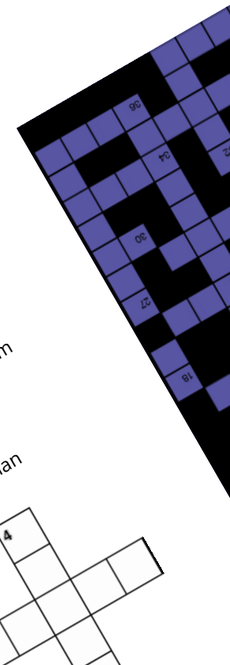
I have completed the requirements assigned to me during my first week of employment.

Teammate signature _____ Manager signature _____ Date _____

CHALLENGE

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

CROSSWORD



DOWN

1. The cow in the Austin Office is covered with graphics from this song
3. The reporting CLI tool that allows us to edit reports
4. Praetorian's product that helps secure our client's software through continuous security analysis
6. a governance model that helps evaluate cybersecurity practices, establish or improve a cybersecurity program, and inform your security roadmap and buying decisions
8. Integrating security into the entirety of software's lifetime, from plan to monitor
9. _ SRF
12. Carbonated yerba mate drink for all your energy needs
14. New hires build these during their first week at Praetorian

ACROSS

2. This tool graphs relationships in AD environments
5. Our Friday retroactive meeting where we take a look at all of the exciting things we accomplished that week
7. The open source tool that Diana uses to identify flaws in containers
10. This AWS service sometimes allows you to fetch API credentials from instances
11. Publicly known exploits and weaknesses often get designated one of these
13. The protocol used in TLS to exchange keys
14. Each services team's name starts with this

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.

Namely

Namely is our HRIS, used for payroll, benefits, anniversaries, and birthdays.

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.

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.

Chariot

Chariot brings all application security program activities into a single view, giving visibility into the breadth of coverage and opportunities to improve across the entire CI/CD lifecycle

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.

The Five Dysfunctions of a Team
Lencioni reveals the five dysfunctions which go to the very heart of why teams even the best ones-often struggle. He outlines a powerful model and actionable steps that can be used to overcome these common hurdles and build a cohesive, effective team.

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

by Nathan Sportsman

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

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.

01 **Default to open.**
Bias toward brutal truth over hypocritical politeness.

02 **Orient to action.**
Make decisions. Make mistakes. Just take the initiative.

03 **Lean into Discomfort.**
Growth and innovation comes from tension and change.

04 **Be humble.**
Constantly pressure test your opinions, convictions, and believability.

05 **Yes, and...**
Start with yes by encouraging new ideas and expanding on them.

06 **Follow your passion.**
If your vocation is your avocation, you will never work a day in your life.

07 **Put the customer first.**
Everything else will work itself out.

08 **Make craters.**
Find success and meaning through impactful work.

09 **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.

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 Praetorian Way: People First, Always

by Nathan Sportsman, CEO

We firmly believe that a small group of exceptional people can do great things when we put those people first. We are the security *experts*, and we are privileged to employ the top one-percent of minds in our industry. Each individual's well-being, success, and growth is vital, and when combined yields an organization that is far greater than the sum of its parts. Yet, employing the brightest in our field is not itself a unifying factor or a force multiplier. How we treat each other is our "secret sauce," and we take pride in the fact that thriving relationships drive our organization because our core values allow us to prioritize people over process.

Anyone smart can do something interesting, but at Praetorian we do more. We accomplish amazing things because we do them together. Whether it's celebrating a massive new account or successful pilot project, or struggling through an obstacle or professional growth area, no one is alone. Core values such as Be Humble, Default to Open, and Lean into Discomfort interweave to create an environment where your colleague is as invested in helping you solve a tough problem as they are in achieving their own objectives. We expect people to admit they do not understand or know something, and then seek help and ask questions. Not knowing is not a problem; not learning is. Communication in all directions is clear and honest, even on hard topics, because every human deserves the truth and also because speaking directly leads to deeper trust and more meaningful growth. A mindset that Performance Matters means we as individuals constantly work to improve ourselves, each other, and our services and products.

We encourage people to take risks, make mistakes, and achieve the improbable. After all, Without risk there is no change, and change is the engine that drives greatness. Try Harder, Orient to Action, Follow Your Passion, and "Yes, and..." are entrenched values that have paved the way for engineers to produce initiatives, practices, products, and service lines. Everyone is empowered to be the catalyst of change, and leadership is possible at all levels. Our barometer is simple, really: leaders must take radical ownership. Ownership of their failures, subject matter, projects, role, and growth, their team's success, and the company's reputation. We accept that some failure is inevitable. We applaud those who take the initiative, and if they fail we are invested in their comeback.

When the empathy for and camaraderie with one another combine with our high tolerance for risk and failure, magic happens. We know that we have the capacity to Make Craters in our own field, and in our clients' industries. We have done so in the past, and will continue to do so, because we put our people first. When we all are content in our work and trust each other, we have the mental space to focus on evolving our relationships with clients. Praetorian's foundation of Core Values ultimately supports each employee in their effort to Put the Customer First.

We Will Stand in the Gap:

Building a Defensive Service Line at Praetorian

by Stanley Parret

Globally, we as a society will spend $160-170 billion in the next year to protect ourselves from cybersecurity threats. Yet despite this colossal investment, analysts anticipate an estimated $6 trillion worth of damage will result from cyber crime and other cyber threats during 2021 alone. The threat is real and orders of magnitude larger than our industry's effectiveness in protecting against it. The range of causes is broad—organizations invest money in suboptimal solutions, cast too wide of a net, or fail to optimize their existing capabilities. Regardless of the reasons contributing to this trend, one fact remains: few want to accept the responsibility of standing in the gap. Security professionals—both internal teams and external consulting firms—seek to pass the buck to a nebulous "they" in order to avoid taking ownership of the problem. Until now.

At Praetorian, we view security as a first-person problem, so that "we" and "I" are responsible for making things better. Orienting toward action on so vast a problem is scary and challenging, but making craters always involves leaning into discomfort. We as the security experts have looked at the global security problem as it has manifested across our diverse client base, and we say "no more." We will confront this problem, protect our customers, and "make it better." We will stand in the gap.

We fundamentally believe that developing a defensive capability is the next phase of evolution for us to best serve our clients. It makes absolute sense, especially when viewed through a superhero lens. Superheroes? Yes! Read on!

Superheroes and the skirmishes along the way

The issue, of course, is that by and large organizations do not care about security until they have been compromised, and then it becomes an all-consuming problem for which no one wants to accept responsibility. How can Praetorian, a small company, protect the entire world from a skulking supervillain and save it before the cataclysm? This dynamic parallels that in superhero stories wherein the hero is a ghost until the world is about to explode, and then they arrive to save the day. We all know there will be a climactic battle scene, where the scrappy superhero leverages their power and knowledge to defeat a villain that seemed unstoppable.

What people forget amidst the awe and splendor of that epic victory is the fact that the superhero has confronted the villain multiple times beforehand. They have jumped in to rescue individual citizens who were experiencing harm at the hands of the villain long before the villain unleashed the fullness of their evil plan. In a world where no one wants to address the full scope of the cybersecurity problem, we have learned that most people will not care about our "villain" until they are hurt. So, we help those who are hurting. Every engagement is an opportunity to understand the cybersecurity threat further in hopes that we can not only forestall the cataclysm for a client or industry, but also gradually close the gap between the global threat and our ability to protect against it.

A framework to defy the odds

Historically, Praetorian has taken an offensive posture in countering the threats our clients face. After thousands of engagements with diverse clients we now are poised to leverage our deep technical expertise in a defensive way. Stepping into this role will happen over time, but we are structuring our Defensive Service around the NIST CSF framework, which in our experience is the most comprehensive framework for defensive enablement. Every step is crucial to the service's overall effectiveness, and we are approaching our internal development in this order:

1. **Response:** Help those who are in need now. Our team comes in, determines what is happening, ejects the hostile entities, and outlines what the client needs to do to remain safe after the engagement.
2. **Detection:** Find and Remediate invaders. The entire purpose of our Detection service line is to determine if there are invaders in your environment and eject them as quickly as possible.
3. **Protect:** Develop the client's ability to defend themselves. Being able to respond to a threat generally means that the attack got past this step of the attacker kill chain. Our aim is to stop the attacker before they get in leveraging the capabilities that our customers possess in their environments.
4. **Strategic goals:** determine what has the most potential impact for clients. We identify future threats to our clients' industries based on analysis of patterns emerging in the Incident Response Program and Detection Spaces.
5. **Recover:** clean up following incidents. We use our robust, effective defensive capability to make things better after an incident.

A common theme throughout this program is the idea that we must meet the client where they are. Every aspect will be tool agnostic and cloud first, because we believe every client deserves world class service regardless of the tools they do or do not use. After all, to carry our analogy a bit further, superheroes never say that they will only rescue people in runaway trains but not speeding buses or crashing planes.

Our goal is to be the one company that will not pass the task or responsibility on to someone else. Rather, we will stop the threat. We will find the hostile actors in whatever guise they adopt, and eject them from our clients' environments. We will protect our customers. We will stand in the gap. ⬢

Developing the RED TEAM PRACTICE

by Samuel Pezzino

Inception

The Red Team service line began with a leap of faith by Thomas and Dallas in Praetorian's early days. The company was fully capable of conducting internal and external network assessments but simulating an advanced threat was new territory. Remotely compromising a corporate network and reaching a predefined objective without being detected by a well-funded blue team is hard. Additionally, there was no precedent for executing these assessments for the company at this time. Dallas and Thomas developed the original Red Team playbooks on the fly and ultimately were successful. The team compromised a financial institution and demonstrated the ability to move significant amounts of money.

Learning on the fly

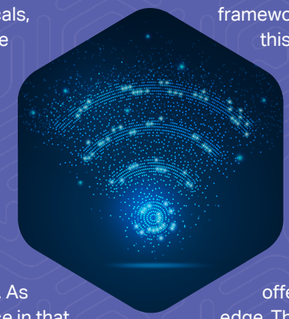
The prior Red Team success gave Praetorian the motivation to step up our game and take on more advanced customers. The addition of Adam Crosser as a summer intern was a significant multiplier to the team. Even as a college student, Adam developed malware capable of evading EDRs and AVs we saw on customer networks. These tools were crucial for our success in the beginning stages.

The major chip manufacturer Red Team assessment of 2018 was a major trial by fire for the newly formed group within Praetorian. Initial access took weeks, and repeated failure to achieve a foothold produced doubt on if we would be successful.

Ultimately, the team compromised an employee through social engineering, and the op took off. Over two weeks, the team operated in the environment, hitting our objectives while remaining undetected. Success on this assessment was a defining moment for the Praetorian Red Team. This op showed that we could target the same organizations as a Nation-State adversary and be successful.

Hitting our stride

Given the previous success, Praetorian took on more and more Red Team assessments across many business verticals. Financial institutions, defense contractors, pharmaceuticals, and others were among the customers engaged in these assessments. The team began running these operations concurrently and achieved overwhelming success leading to long-lasting partnerships with some of the most well-known and respected companies. As the team gained experience in that first year, it became clear we needed to evolve our Tactics, Techniques, and, Procedures (TTPs) to remain successful. At this point, everything was manual and time-consuming. Payload generation, infrastructure provisioning, external enumeration, and OSINT all took significant time and preparation to execute. Adam developed the first version of Praetorian's payload generation framework known as Pilum, which leveraged the malware he developed as an intern. Pilum led to the successful compromise of countless phishing victims and was critical to the team's success as a whole.



At the same time, Dallas pulled in open-source DevOps projects and adapted them to fit the Red Team need for automated infrastructure provisioning. This work would become the internal project known as "Red Box" and is used on essentially all assessments at this point.

In addition to improving our capabilities, Praetorian began taking on unique customers with atypical requirements. Dallas and Weems conducted the company's first supply-chain operation scenario in 2019. Up to this point, Red Team operations were classic "Enter from the outside" scenarios. This operation was unique in that it simulated an adversary inserting a malicious package into a companies build pipeline. Dallas and Anthony created an agent and C2 framework from scratch to execute this assessment and ultimately were successful in hitting their objectives.

Taking it to the next level

In 2021 Praetorian Labs was formed to act as an R&D center to support services and keep our offerings at the bleeding edge. The team consisted of Dallas, Anthony, Michael Weber, and Ian Spiro early, with rotations from services engineers to support development. In addition to developing long-term solutions such as C2 frameworks, malware, and sandbox evasion techniques, they also serve as a rapid development team to support complex assessments as needed. For example, the team developed one of the first working PoCs for the Exchange ProxyLogon vulnerability within days of the disclosure to support an ongoing Red Team.

The future

The Praetorian Red Team is continuing to evolve its capabilities past "classic" ops. Significant investment is being placed on improving our capabilities to target SaaS platforms, microservice architectures, cloud. and non-Windows environments. The Red Team Practice Manager, Thomas Reburn, continues to refine our Assumed Breach offerings to provide valuable scenarios for customers and unique opportunities for Red Team operators. The Praetorian Red Team will continue to grow and take on the hardest challenges out there. ⬢

From Chip to Cloud:

Praetorian's Methodology to Hacking IoT

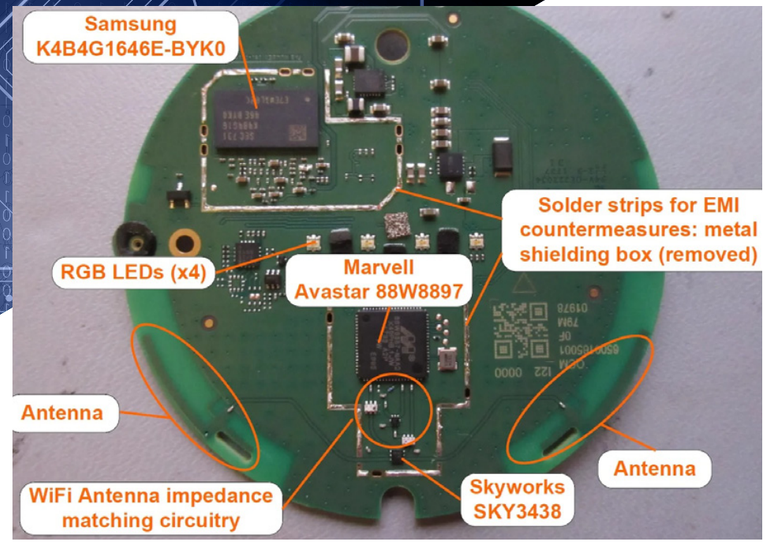
Welcome to the wonderful world of IoT (Internet of Things) security testing, where no two devices are the same yet there are similar themes in security problems that arise. Praetorian has tested a wide range of embedded systems, such as autonomous vehicles, medical devices, critical infrastructure, and smart consumer devices. In this article, we will go through Praetorian's methodology to hacking IoT systems, starting with hardware and ending with cloud communications.

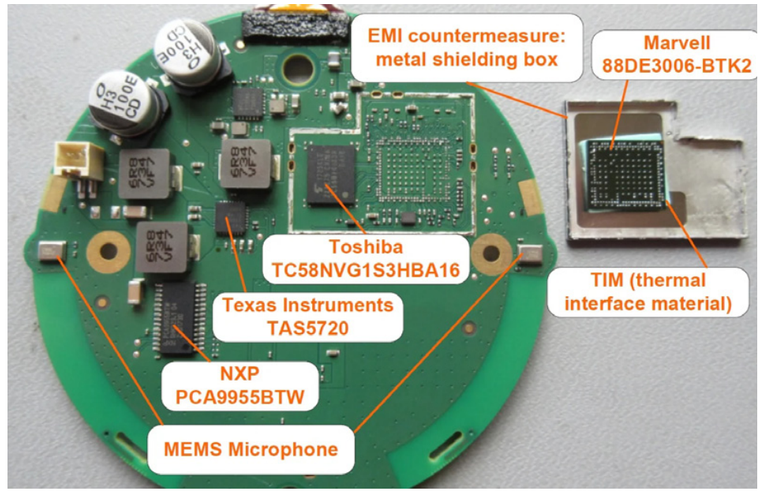
Once you start testing an IoT device, the first thing to do is map out its possible attack surface. Since there are significant differences between embedded systems, there are always new attack paths to consider. For example, testing a smart doorbell could include a camera, microphone, and Wi-Fi interfaces, whereas testing a Kiosk machine could include a touch screen and USB slots. Regardless of the device, there will be some form of interface in the underlying system than an attacker could attempt to abuse. One common denominator is the printed circuit board (PCB) within each device.

Hardware

The above images are taken from an extracted PCB of a Google Home Mini (credits to https://www.allaboutcircuits.com/news/teardown-tuesday-google-home-mini/). When you first take apart a device, the very first thing to do is write down the chip packages (the black boxes with markings) and look up their datasheets. The next thing to do is rank the packages by level of importance: microcontrollers, memory, and peripherals. For the examples above, the two Marvell chips are the main microcontrollers on the PCB but used for different purposes (top is for application logic, bottom is for Wi-Fi). The main memory components are the Toshiba chip for long term memory, and the Samsung chip for DRAM. The peripherals, such as the MEMS microphone, are important to note but will not be the main focus of hardware testing.

Once you have an understanding of the hardware components, the three main areas to focus for hardware security testing are interacting with debug pins, extracting data from memory, and monitoring data over interesting buses (such as between the main microcontroller and the Wi-Fi microcontroller). Some of the tools you will need to perform your testing are a multimeter, a logic analyzer, and an on-chip debugger (OCD) such as a J-Link. Additionally, things like a power supply unit (PSU), a soldering bench, and jumper cables are essential to connect to the PCB components.

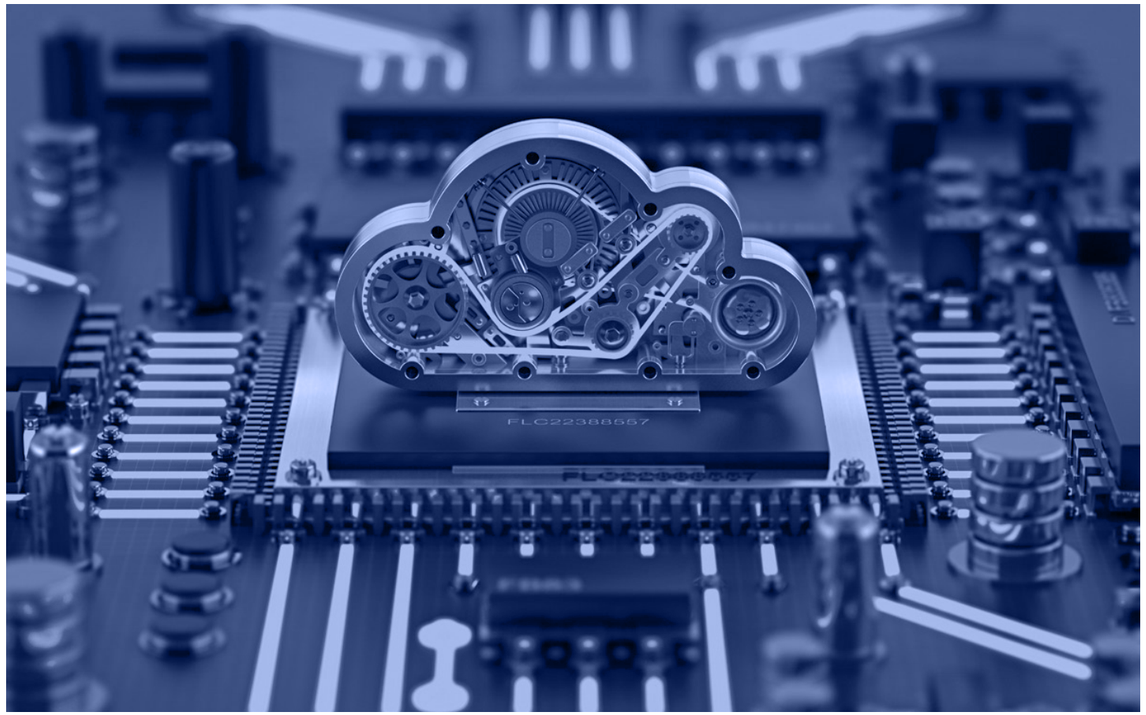




Almost all microcontrollers contain a debugging interface, and the most common are JTAG and SWD. When these interfaces are enabled, it is very easy to connect a J-Link to extract onboard memory from the chips or re-flash the memory with malicious firmware. To prevent this debug access, companies should set the eFuse on the chip or add security controls like JTAG password protection to prevent easy access to the underlying microcontroller. Another common debug interface occurs over UART. Since UART is generic by design, this could be a console terminal to the device or a debug application with a custom protocol. Praetorian often gains terminal access over UART with a password that was extracted using some of the techniques described here.

Extracting data from memory can also occur in dedicated chips on the PCB. For example, it is very common to have an additional SPI flash chip used to store larger amounts of data such as a filesystem. In these cases, it is important to find the pads corresponding to the SPI interface. In the event the pads are not exposed, it is feasible to attach to metal scrapped from the PCB, or remove the flash chip entirely from the board using a heat gun and attaching wires directly to the chip (dead bug method). Once the pads are identified, you can use a tool such as a J-Link to interact with the flash chip and read/write data.

When devices use dedicated Wi-Fi / BLE / ZigBee chips for network processing, data is often sent to the main microcontroller over an unencrypted bus. In this case, using a logic analyzer to monitor traffic can be an interesting attack path to obtain privileged information. For example,



the bus could contain the stored Wi-Fi credentials it uses to connect to the user's home network. In that case, an attacker without previous knowledge of the user's home network could capture that information and access their Wi-Fi network.

Network Interfaces

IoT devices are connected in many different ways, and for our purposes we will look at Wi-Fi, BLE, and ZigBee network interfaces. Typically, an IoT device communicates with the internet over Wi-Fi, however how does the device get connected to the right Wi-Fi network? The most common ways are either the device exposes its own access point (AP), or a mobile device communicates over BLE. When a device hosts its own AP, it is important to use some type of encrypted channel. For example, Praetorian often finds that devices expose an open AP but also passes application data between a mobile device via cleartext HTTP. In this case, the device should use HTTPS to ensure the information is encrypted and the TLS certificate is signed by a trusted certificate authority.

As time has passed, BLE has become more mainstream to provision IoT devices to the internet. BLE communications occur via GATT characteristics, which can be loosely understood as a key-value pair that devices can read/write depending on the characteristic's permissions. The most important permissions are whether a characteristic needs encryption or authentication to access. If neither of these permissions are set for sensitive characteristics, it can be easy for an attacker to sniff BLE communications using an UberTooth and capture sensitive information over-the-air.

Another common network protocol is ZigBee (802.15.4), and it is most commonly used in smart home communications due to its low frequency. There are more technical details in ZigBee due to the separation of application and network layers, however one of the pitfalls Praetorian commonly sees is neglecting to pre-configure a ZigBee network. In the event Praetorian is able to trick other devices into thinking it is a Coordinator device, it is possible to take over the entire network. Additionally, network keys are often not encrypted and sent over plaintext. Tools such as the RZ Raven Stick are good to interact with ZigBee networks.

Firmware Analysis

Hardware and network interfaces are only one piece of the bigger IoT picture, and most of the security vulnerabilities within devices can be found in its running firmware. Praetorian's clients typically provide firmware source code for in-depth analysis, however knowing how to test extracted firmware is a good skill to know. Once firmware is extracted via a debug interface or flash chip, running a binwalk over the binary will give clues as to what the binary contains of and which components can be further analyzed using reverse engineering tools such as Ghidra. Regardless if you have source code or not, some of the most important things to analyze are the over-the-air (OTA) update process, device authentication/authorization, and input handling.

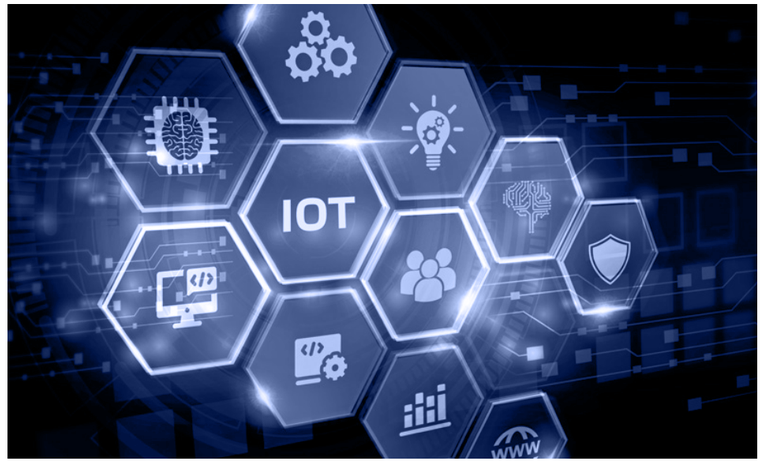
Most consumer IoT devices have some sort of OTA update process that is initiated remotely or by a mobile device. During the OTA process, it is important to check that firmware signatures are properly validated and the communication channel is encrypted. This will prevent a man-in-the-middle attacker from modifying the OTA update package and performing a malicious firmware update.

Other security controls to test are commonly found in the OWASP top 10, such as authentication, authorization, and input handling. Given the number of hardware and network interfaces, there are many injection points where user input could cause undefined behavior or even fully compromise the device by remote code execution. For example, Praetorian has performed buffer overflow attacks against unauthenticated BLE characteristics that handled input incorrectly. It is again important to stress that most security vulnerabilities are found in firmware source code.

Cloud Communications

So far, we have mainly focused on hacking a single IoT device. However, IoT consists not only of the end device, but the mobile applications, gateway devices, and Cloud backend services that communicate with it. There are two common ways that devices communicate with Cloud services: HTTPS and MQTT. For both of these protocols, you should attempt to proxy communications between the IoT device and services. There are often problems in how an IoT device validates server TLS certificates that allow man-in-the-middle attack scenarios.

For developed services like AWS IoT Core, communication typically occurs over MQTT. This publish/subscribe protocol makes



it easy for many devices to subscribe to one topic and receive information all at the same time, such as new OTA updates. However, MQTT authorization controls quickly become important to prevent one device from publishing/subscribing to other device topics. In a worse case scenario, a single device could update all other devices with malicious firmware at once!

Conclusion

In this article, we went through Praetorian's methodology to hacking IoT systems. First, perform a thorough enumeration of attack surfaces to create plausible attack vectors against the system. Next, disassemble the device and categorize hardware components that are interesting to inspect, such as microcontrollers or external memory. After extracting the firmware, analyze how the device handles external input and attempt to identify attacks such as buffer overflows. Finally, proxy communications between the device and cloud services and test the backend service's authentication and authorization controls to prevent cross-device attacks.

Perspective: Cloud and Beyond

Back in the early 1990's, while working as an engineer with the Networking and Distributed Systems Group at Sun Microsystems, our rally cry was "global, mobile, simple". Yes, ladies and gentlemen, that was circa 1992. Fast forward almost 30 years, and these words seem to be so apt and relevant for anything driving the evolution of the cloud or its adoption. This walk down memory lane is to help reinforce the point that the Cloud is still a pit stop on the ever maturing continuum for the technology industry at large. The Cloud is not revolutionary, but evolutionary.

Praetorian's service offerings as well as our product Chariot, require us to be well versed with an incredibly broad array of technologies. We engage with customers at all stages of the Cloud evolution. Some of our customers are startups on the bleeding edge of the technology curve and some large customers are just getting started with modernizing their legacy applications.

This article is intended to share our perspective on where we see this continuum heading. These points along the technology curve may seem a bit further out for some, but for all engineers at Praetorian it is something we think about every day and prepare for weaving competencies into our service offerings and our product Chariot.

Self Sovereign Identity

We are all too familiar with "Login with Google". This has been both a blessing (ease of use) and a curse (violating least privilege access). On the business side companies like Okta, Ping Identity and Auth0 have hidden the complexities of the underlying OIDC, OAuth and SAML protocols to provide a seamless SSO experience. So to stay true with the earlier assertion that the Cloud is just a pit stop in the ever evolving continuum, where do we think IAM is heading? At Praetorian, we like to keep an eye on Self-Sovereign Identity. The concept of an individual protecting and managing their identity as their personal property rather than allow an organization or third-party provider manage it. By keeping the individual's information protected by encryption in a permanent blockchain across a distributed network system, this concept offers complete individual control over identity data. Through the Self-sovereign identity system, the idea is to replace centralized identity providers and instead let each individual take control and decrypt the data only when required. The evolution of this space is something we are watching closely at Praetorian.

Redefining Perimeter Security

While human to machine interactions have been greatly assisted with technologies like OIDC, OAuth, the one area that we think about a lot at Praetorian is how traditional perimeter security anchored on firewalls is (or should be) likely to break down. Service to service interactions, across organizations with strong security presents the next frontier for security technologies in general. Presently, major cloud providers offer service account identities based on X.509 certificates. However, getting these service identities to interoperate across organizations, hosted on different public cloud providers is where evolving standards like SPIFFE and SPIRE come into play. We believe it is not too long until we witness a widespread adoption of these technologies redefining the present perimeter security model and allow secure service to service interactions that transcend organizational boundaries.

Extensible service mesh

Today, microservices architecture is considered the de facto standard when it comes to leveraging architectural patterns. The anchors of a microservices architecture: single responsibility principle, services own their data, externalized non-functional capabilities amongst others is well suited to deal with the complexities of an overall cloud adoption strategy. Open source products like Istio are the equivalent of "Login with google" from the standpoint of leveraging microservices, seamlessly packaging them for mutual TLS and embracing other important anchors of a microservices architecture as briefly alluded to above. With that said, what we find the most interesting at Praetorian is how these service meshes can be extended to cross organizational boundaries and in the process opening up possibilities of "secure industry meshes", "supplier meshes etc."

Declarative Primacy

Sun microsystems introduced Solaris containers back in 2000. They introduced renting a machine by the hour in 2004. But unfortunately, in the technology industry, the hockey stick inflection point requires consumer participation for things to go viral. Cloud Computing had a certain panache and buzz and created the hockey stick that Sun microsystems could not achieve with its utility computing model. Cloud won over utility. Similarly Docker won over Solaris containers. But the real winner today is Kubernetes. A ginormous declarative control loop for managing distributed resources. We at Praetorian like to think of Kubernetes as the "Hypervisor for the data center", a term we believe captures and conveys the true power of this platform. There are many aspects of Kubernetes that interest us:

- A ubiquitous platform that can provide the next higher level abstraction from one of many different public cloud platforms. This paves the way for multi-cloud solutions.
- Kubernetes implements a zero trust model internally and when combined with open source platforms like Istio also extends this zero trust model to customer services deployed on Kubernetes
- Kubernetes operators are a significant asset when dealing with large scale deployments.

For all the reasons outlined above, we decided to build Praetorian's Chariot product entirely on Kubernetes.

Hybrid Cloud - Interoperability focus

Consistent with the theme that technology evolution is on a continuum, the question is what is the next abstraction over a public cloud platform ? While the most definitive and authoritative answer will only become obvious in highsight, we do believe the single most important factor driving this next higher level abstraction will be interoperability across cloud platforms. We draw a distinction between integration and interoperability. The latter goes deeper and broader and will pervade many constituent technologies that are likely to collectively define this new abstraction. Kubernetes, extensible service meshes with Istio, Hyper-Converged Infrastructure (HCI), cloud deployment patterns, container patterns are all contributing to defining this next stop on the continuum curve. We can assure you that the term Cloud will seem archaic in a few years and will be replaced with something else. My personal favorite contender is Spaces. Imagine a giant Kubernetes swarm hosted by a provider that is carved up into multi-tenant Spaces. Similar to the experience with Google App Engine or AWS Elastic Beanstalk, adequate tools, abstractions are available to provide full engagement and consumption of these Spaces.

Authorization Primacy

Authentication gets far too much love, Authorization does not. When dealing with large monolith systems the distinction between the two seems to blur, primarily because as authorization gets more and more coarse grained, it starts to meld into authentication. But as these monoliths are strangled into loosely coupled services and the distributed footprint starts to get larger, the distinction between Authentication and Authorization starts to stand out. While a human or service may be authenticated once, authorization will likely see many points of enforcement even during a single distributed transaction. Consequently, fine grained authorization is an imperative for building modern cloud based platforms leveraging microservices. As you move along the technology continuum with higher level abstractions, as organizational boundaries get broken down, authorization is likely to play an even bigger role in the overall architectural fabric. At Praetorian, we are huge fans of Open source frameworks like OPA (Open Policy Agent). OPA supports many different POE (Points of Enforcement) and offers a rich DSL for implementing authorization policies.

Praetorian's Chariot product leverages OPA for its authorization policies.

Gross Margins - the new engineering metric

AirBnB blew up the fragmented vacation rental industry with its platform and how incredibly easy it was to use. Stripe blew up the payments industry with its really easy to use REST API. There are numerous case studies of the importance of ease of use. How you navigate a website is clearly important but equally important is how the website performs under load. For SaaS providers to provide what we call "performant ease of use", the cost of delivery is paramount. While Cloud Computing has fulfilled many expectations, it has failed miserably on the cost front. At first blush, inclusion of cost of delivery in this article may seem out of place, but at Praetorian we believe this is an important dimension to consider for various reasons:

- It elevates the architectural challenge and consequently has a direct impact on how we secure the architecture.
- Cost of delivery has a direct impact on the choices around Scalability, Availability etc. and these in turn are right in the cross hairs of Praetorian's security lens.

Gross margins were once an esoteric financial term not commonly considered by engineering teams. But now we believe it is front and center (or perhaps should be) for all engineering teams.

Security - above and beyond

At Praetorian, we live and breathe security. But the term "security" has a very wide footprint and canvas. It touches all aspects of an enterprise or product. It encompasses and impacts choice of protocols, standards, development patterns, integration patterns, architectural patterns, cloud platforms.

As this continuum evolves further, the role of security and its impact will only increase. As the future platforms and abstractions get more loosely coupled, the higher the security implications.

Working at Praetorian offers you well more than just working with security technologies. While we specialize in Security, we look at the forest first before the trees.

Closing

We started this article talking about the technology continuum and how the adage "global, mobile, simple" continues to drive the evolution of this continuum. We did not talk about another popular adage within the technology industry driving this evolution: "Break down silos". If you examine the various forward looking trends we have referred to here, the theme that is evident is "Break down Cloud Silos". Whether this be eliminating perimeter security, extending secure corporate digital boundaries or using technologies to enable the above, this clearly is going to define how the technology continuum evolves over the next decade. ⬢

A Day in the Life: Labs

One of the Praetorian core concepts is that if you truly love your job, then you will never have to work a day in your life – to paraphrase Mark Twain, your vocation becomes your vacation. In this article, we want to share a little bit about Praetorian Labs, a place where that vision is realized and our work aligns with our passions. While it's not all glitter and unicorns – research, especially vulnerability research, can be really frustrating – in general each assignment in Labs is interesting, because "interesting" is basically our mission statement. Yep, Labs is a good place to be.

Let's convert that into something that's a bit more formal: Labs is a standalone organization with Praetorian that is designed to help drive innovation in both the Services and Product sides of the business. Within Services, we're looking out to the horizon, figuring out where we need to be in a year or two. That, and providing "advise and assist" services on engagements. This is really interesting, because we get to focus on the aspects of the job where we as a company still have room to grow.

On the product side of the house, it's also pretty intense work, as we own and drive the scanner infrastructure our product (Chariot) leverages. This is a good fit with the Red Team and ProdSec work we support, as we have a good understanding of what tools work in practice… and which ones don't. Work is pretty varied; one week, we might be advising on a security assessment, another might be building out our own C2 infrastructure or browser implant. It's technically challenging because of this, but it's also what keeps it interesting.

Introducing Hafnium

One of our more interesting recent adventures has been research on CVE-2021-26855. It's an important vulnerability because it was so pervasive and let attackers into the very heart of the company infrastructure. Moreover, it was a so-called 0-day, as the vulnerability was actively being targeted before defenders became aware of it. From timelines, it appears that state-sponsored attackers (most notably China) were using the vulnerability to achieve complete control of victims' Exchange infrastructure, followed by lateral movement.

The situation was serious enough that the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) published a Microsoft Exchange Server joint advisory (AA-21-069) on the topic, and we are painfully aware that the weakness continues to be exploited – now with the added challenge of criminal groups joining the party (as well as continued use by Nation States).

For a truly deep dive, it's best for you to stop and go read our Blog on the subject. However, we did want to share the approach we took here, as it's something that can be applied to many different vulnerabilities. After that, we'll share some as-yet unpublished work that actually took us to a working POC.

First, because Microsoft had issued a patch for the vulnerability, we had a huge head start: we could look at the patch and determine what had been fixed. This is the next best thing to having details on the vulnerability itself, because by examining what has been changed, it's a short hop to determining why it has been changed. From there, building an exploit is easy (where perhaps putting the word easy in inverted commas might have been smart – it's all relative!).

To this end, we went through the following steps to allow us to perform both static and dynamic analysis of Exchange and its security patches:

- **Diff:** review differences between vulnerable version and patched version
- **Test:** deploy a full test environment of the vulnerable version
- **Observe:** instrument deployment to gain knowledge of typical network communication
- **Investigate:** iterate over each CVE, connect patch diff to network traffic, and fabricate proof-of-concept exploits

We'll take a look together at the individual steps here as a recap.

Diff

By examining the differences (diffing) between a pre-patch binary and post-patch binary we were able to identify exactly what changes were made. These changes were then reverse engineered to assist in reproducing the original bug.

Microsoft's update catalog was helpful when grabbing patches for diffing. A quick search for the relevant software version returned a list of security patch roll-ups that we used to compare the latest security patch against its predecessor. For example, by searching for "Security Update For Exchange Server 2013 CU23" we identified patches for a specific version of Exchange. Exchange 2013 was chosen here because it was the smallest set of patches for a version of Exchange vulnerable to CVE-2021-26855 and therefore easiest to diff.

To begin, we downloaded the latest (3/2/2021) and the previous (12/2/2021) security update rollup. By extracting the .msp file from the .cab file, and unpacking the .msp file using 7zip, we were left with two folders of binaries to compare.

Because most of the binaries were .NET applications, we used dnSpy to decompile each binary to a series of source files. To speed up analysis we automated decompilation and leveraged the comparison functionality of source control by uploading each version to a GitHub repository as separate commits for comparison.

An alternative diffing option that we also found helpful was Telerik's JustAssembly. It was a little bit slower for observing the actual file differences but was helpful in immediately identifying where code had been added or removed.

With this preparation complete, we needed to spin-up a target Exchange server to test against.

Test

To begin, we set up a standard domain controller using the ADDS-Deployment module from Microsoft. We then downloaded the relevant Exchange installer (ex: https://www.microsoft.com/en-us/download/details.aspx?id=58392 for Exchange 2013 CU23) and performed the standard installation process.

For an Azure-based Exchange environment, we followed the steps outlined here, swapping the installer downloaded in step 8 of `Install Exchange` with the correct Exchange installer found in the above link. Additionally, we modified the PowerShell snippet in the server provisioning script to spin up a 2012-R2 Datacenter server instead of the 2019 Server version.

This allowed for a quick deployment of a standalone Domain Controller and Exchange server, with a network security group in place to prevent unwanted Internet-based exploitation attempts.

Observe

Microsoft Exchange is composed of several backend components which communicate with one another during normal operation of the server. From the user perspective, a request to the frontend Exchange server will flow through IIS to the Exchange HTTP Proxy, which evaluates

mailbox routing logic and forwards the request on to the appropriate backend server. This is shown in the diagram below.

We were interested in observing all traffic sent from the HTTP Proxy to the Exchange Back End as this should include many example requests from real services to help us better understand the source code and from requests in our exploit. Exchange is deployed on IIS, so we made a simple change to the Exchange Back End binding to update the port from 444 to 4444. Next, we deployed a proxy on port 444 to forward packets to the new bind address.

The Exchange HTTP Proxy validates the TLS certificate of the Exchange Back End, so for our proxy to be useful, we wanted to dump the "Microsoft Exchange" certificate from our test machine's local certificate store. Since this certificate's private key is marked as non-exportable during the Exchange installation process, we extracted the key and certificate using mimikatz:

With the certificate and key in hand, we used a tool similar to socat, a multi-purpose network relaying tool, to listen on port 444 using the Exchange certificate and relay connections to port 4444 (the actual Exchange Back End).

With our proxy configured, we began using Exchange as normal to generate HTTP requests and learn more about these internal connections. Additionally, several backend server processes sent requests to port 444, allowing us to observe periodic health checks, Powershell remoting requests, etc.

Investigate

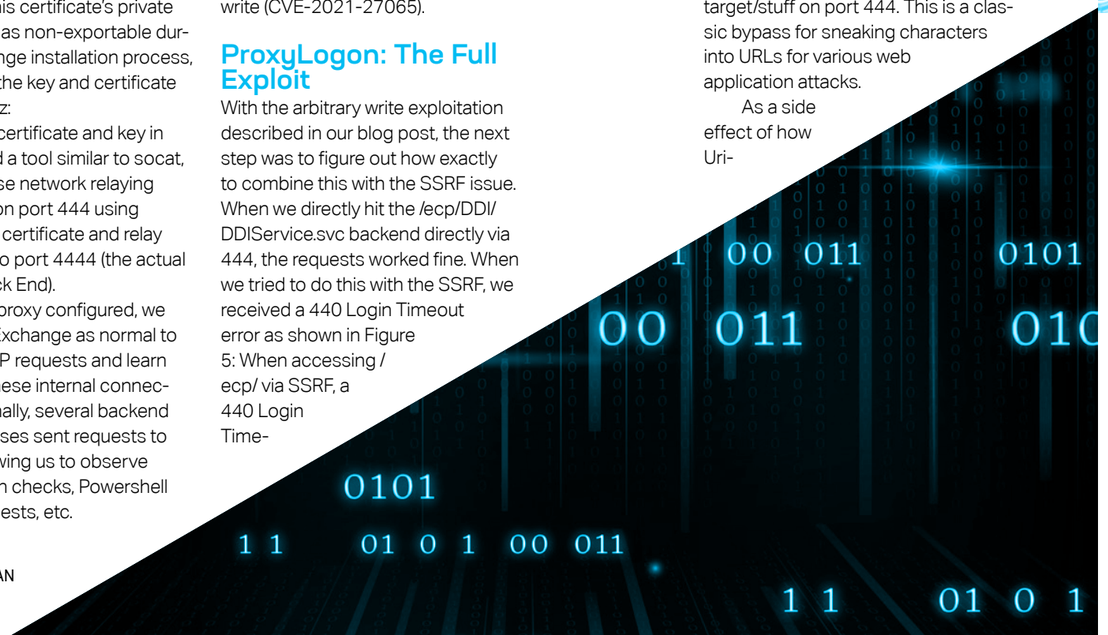
While each CVE is different, our general methodology for triaging a particular CVE was composed of five phases:

1. Reviewing indicators
2. Reviewing patch diff
3. Connecting the indicators to the diff
4. Connecting these code paths to proxied traffic
5. Crafting requests to trigger these code paths
6. Repeat

From here, things get a bit in the weeds. Once again, we refer you to the original blog post for the play-by-play, but by the end of this, we had the ability to exploit this vuln. Read on for what we decided we couldn't share in the original post. Thus, without more ado, here are the missing details of how we chained the SSRF bug (CVE-2021-26855) to trigger the arbitrary write (CVE-2021-27065).

ProxyLogon: The Full Exploit

With the arbitrary write exploitation described in our blog post, the next step was to figure out how exactly to combine this with the SSRF issue. When we directly hit the /ecp/DDI/DDIService.svc backend directly via 444, the requests worked fine. When we tried to do this with the SSRF, we received a 440 Login Timeout error as shown in Figure 5: When accessing /ecp/ via SSRF, a 440 Login Time-



out is returned, even for valid requests..

Given that we had control of the hostname that was sent to UriBuilder, we modified the request slightly to try relaying our payload directly to 444 to see if this bypassed the 440 error. This turned the response into a 500 error which was a sign of progress. After enabling verbose error messages on the server and replaying the request we were given a stack trace to further triage what was stopping us.

After attaching dnSpy to the MSExchangeECPAppPool w3wp.exe process (which we identified by trial and error) and re-triggering the 500 error, we realized that UriBuilder, on assigning our exvm.corp.contoso.com:444/path/to/target URL to the Host property, was detecting the ':' and deciding to wrap our string in square brackets to convert it to IPv6.

Because the host was still being parsed as a URI, we were able to bypass this issue by prepending an '[:[@' to our SSRF host. When URIs are parsed, any value after the protocol but before the @ symbol is considered a username and password which can contain any character. So [:[@exvm.corp.contoso.com:444/target/stuff# would be interpreted as having a username of '[', a password of ']', and accessing exvm.corp.contoso.com/target/stuff on port 444. This is a classic bypass for sneaking characters into URLs for various web application attacks.

As a side effect of how UriBuilder works, we only needed to prepend the '@' symbol, since we were already appending a '#' to the end of the SSRF attack. Even if the square brackets wrapped our host, it would still look like [@exvm.corp.contoso.com:443/target#] which would also be a valid URI.

Interestingly, once requests were made on 444 via the SSRF, they appeared to be authenticated as NT AUTHORITY\SYSTEM. After examining our back-end traffic logs were found that all proxied requests achieved this authentication via the addition of an Authorization: Negotiate header. For example, a SSRF'd request to the MAPI NSPI API returned the eyebrow-raising response shown in Figure 8:

A response like this is normally an indication that full compromise has been achieved..

Armed with this new highly privileged SSRF, we attempted to access the arbitrary write endpoint again.

ProxyLogon is Go!

At this point, we had the ability to send requests to arbitrary backend endpoints and the ability to write a webshell to an arbitrary location on disk. However, when we sent a DDI request through the SSRF, it returned an interesting error.

This is due to the fact that the Exchange server's machine account has no roles in Exchange. It is possible that an administrator might have granted this machine account permissions, but we cannot rely on that in our exploit. Therefore, we must find a mechanism to tell the backend ECP service which user we should authenticate as. In this case, our hint comes from the domain registered by DEVCORE for this series of vulnerabilities: https://proxylogon.com. We also notice that in their exploit video, their script obtains an ASP.NET_SessionId and msExchEcpCanary, both values which are needed to make authenticated requests to the DDIService in ECP. Unfortunately, these properties didn't immediately lead us to a new endpoint to target.

After searching through various

blog posts online for more indicators we noticed that the Crowdstrike blog showing logs of exploitation contained another clue:

In the exploitation logs, the request before invoking /ecp/DDI/DDIService.svc/GetObject returns a 241 response code. Taking a look at our logs we can see that there is only one endpoint that seems to return 241s.

Given that DEVCORE literally named the bug ProxyLogon it seemed like this was probably the correct path of inquiry. Replaying this type of request returned a redirect to an http 500 with the error Microsoft.Exchange.Clients.Owa2.Server.Core.OwaADUserNotFoundException

We spent hours attempting to replay some of these requests to /owa/proxylogon.owa but continued to encounter errors until after discussions with another researcher, we determined that the likely candidate for exploitation was actually /ecp/proxyLogon.ecp.

In contrast to most of our previous research, proxyLogon.ecp was missing some of the helpful time savers like patch diffing. Instead, our main path to understanding was to simply read as much code related to ProxyLogon as possible. We discovered that the backend ECP service loaded a module, RbacModule, which referenced proxyLogon.ecp. We tracked user input through the RbacModule down to RbacSettings, and which ultimately seemed responsible for creating the user identity and setting session cookies.

As shown in the code snippet above, the ProxyLogon request body is used to create a SerializedAccessToken. This token used a custom XML serializer/deserializer to encode the user's domain, username, SID, and groups.

We used the serialization code to construct a sample XML token with an admin username and SID. However, calling proxylogon with a valid XML token was not sufficient to authenticate as our target user. Further code review revealed a dependency on the msExchLogonMailbox header, which is used when constructing the Server and EcpLogonInformation. This header is undocumented and did not appear in our observed traffic logs. However, this header was responsible for setting the logonUserIdentity, which was required to spoof our authentication to proxylogon.

The full request to spoof authentication via SSRF to proxylogon is included below:

SID Retrieval

Fully abusing the ProxyLogon bug required that we use a valid SID for the machine. In some cases, using the SSRF automatically leaked the SID, but in single server environments this was not the case.

Unfortunately, the patch diffs didn't appear to offer many hints how this could be obtained. Thanks to a suggested approach from Rich Warren (@buffaloverflow) we started digging into MAPI requests made to the server. Similar to the RPC over HTTP mechanism that we abused to leak the server backend name, MAPI is also historically an abuse vector.

The MAPI API is one of Exchange's binary protocols that is tunneled over HTTP requests. Often, with these kinds of requests, half the battle is building something that will not trigger a 400 bad request response. In order to save time on generating test requests by hand, we observed the existing traffic sent and then attempted to replay payloads.

Searching through our default Exchange installation for any interesting MAPI calls revealed a series of health check calls that repeatedly invoked /mapi/emsmdb?mailboxId=de2b5eb0-e4db-403e-9b54-2a6163a0afc3@hafnium.local.

The payload posted to the /mapi/emsmdb endpoint was a CONNECT request defined in the MS-OXCMAPIHTTP open specification. Most of the content in the CONNECT request was fixed or unnecessary, but the userDn property was needed to successfully invoke the API. When we attempted to use just an email address, which appeared to be the only necessary parameter in public proof of concepts, we received an error message from the server.

Fortunately, while testing the earlier SSRF, we had already discovered a way to leak the userDn field: the autodiscover endpoint. It already returned the userDn value in the LegacyDN field - this allowed us to use the SSRF to convert valid email addresses into a userDn value.

When we initially were trying to call the /mapi/emsmdb endpoint, it was just to see if we could invoke ANY MAPI endpoint. In an incredible stroke of luck, it turned out that this API threw an incredibly verbose error that leaked the SID we needed!

Apparently when the NT AUTHORITY\SYSTEM attempted to access another user's mailbox it didn't own, an error was thrown explicitly listing the SID of that user when explaining why the MAPI request failed. The final step was to take this SID and use it to invoke the proxyLogon.ecp endpoint and then trigger the arbitrary write bug.

Unfortunately, the user whose SID we used didn't have permission to access the administrator functionality we wanted to abuse. However, due to a small quirk in how SIDs work, we were able to transform our user SID into an admin SID. The final digits of a SID are associated with specific roles, which are described in Microsoft's documentation.

We simply replaced the last digits at the end of the SID we recovered with 500 and invoked the proxyLogon call. With this simple change, the SSRF can be used to successfully execute CVE-2021-27065.

The final pieces of information necessary to execute this attack are an exposed Exchange frontend server and any valid email on the domain. Given that most corporate email names are predictable or can be harvested via OSINT gathering, this is not unlikely.

Even without any foreknowledge of existing emails, an attacker looking to hit as many machines as possible would simply be able to brute force a number of common email aliases and names via the autodiscover endpoint until one returned a valid userDn. You can likely see this behavior in some logs posted on the sysadmin subreddit back on March 6th, 2021. We didn't become aware of this post until after we had completed our proof-of-concept, but the server logs give a number of hints which could be used to determine further implementation details of the exploit chain.

Closing Thoughts

Hopefully, you enjoyed our run through the Hafnium exploit as much as we enjoyed building it. As you can see, it wasn't easy, but by working together and making good use of 3rd-party resources we got there in the end.

Our intent as a research team is to keep working on this type of research, so we can find and help fix vulnerabilities before they impact our customers. As we do that, we'll keep building out our offensive and defensive tooling. Yesterday's 0-day is patched and done. What tomorrow will bring is still a mystery, but we know that we'll be ready. It's our job.

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 91.7%.

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	"From the get go Praetorian had a great process in place that kept the twitter team informed and filled in what to expect. The team was able to provide what we had in mind and even beyond what we expected. The issues found will help prevent any loss in trust in the product. Looking forward to many more engagements!!"- Twitter
NPS 10	"As usual, loved both the service and the value we got out of the testing." – Palo Alto Networks
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." - Zoom
NPS 10	"The Praetorian team provided a well organized security assessment. They were professional and responsive." - VMWare
NPS 10	"Always a pleasure to work with you. Best in class security professionals providing an expert service." – Priceline
NPS 10	"Praetorian was very professional in handling the engagement. The quality of work was excellent, and the team was in constant touch with us to ensure that everything was in order." - Salesforce

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.

The Best Kind of Group Project: Developing Chariot at Praetorian

by Harry Wallace

At Praetorian, we believe that everyone deserves a simple, cost-effective way to find, fix, and manage vulnerabilities in their software products regardless of budget and irrespective of whether they maintain a dedicated security team. Yet, current open-source security products are not adequately meeting users' product security needs. Over our years of working with diverse clients, our Services and Sales arms have noticed that available automated solutions have serious downsides for clients such as noisy false positives, exorbitant subscription fees, and complicated configuration and implementation. We set out to develop a product that captures all the positives of an automated security solution while eliminating the negatives, and we are approaching product development in a uniquely Praetorian way. Our pools of security expertise and development experience have merged to solve a major problem in product security. This is the best kind of group project. This is where we will make our mark.

All engineers at Praetorian are called to contribute to Chariot. From hackers extraordinaire to developers with no security experience, all have a valuable perspective to add. The engineers working on Chariot fall into one of three main groups: software engineers, security engineers, and machine learning researchers.

Praetorian's talented team of software engineers holds primary ownership over Chariot's development. Our software engineers are driven by our mission and see firsthand the positive impact of the code they are writing, all while getting to work with cutting-edge technologies. Chariot is built on a modern, event-driven architecture that makes use of microservices written in Golang and deployed with Kubernetes to drive a React-based single-page application. The product development team maintains a devout focus on quality and scalability while operating around shared values of passion, drive, and technical excellence.

Our security engineers, whose teams provide direct services to clients, can take advantage of Sapporo time (wherein they are not billing) to work with the product development team on both Chariot and other open-source security tooling projects. Security engineers who contribute to Chariot have the opportunity to pull themselves out of the weeds of customer interaction and apply their experience in an actionable way with far-reaching impact. Our commitment to releasing what we develop here as open-source software serves to extend the reach of our talented engineers' security expertise. We commit to highlighting our engineers' contributions and accomplishments through blog posts and other means, as we work toward providing the security community with high-quality and reliable security tooling. Our engineers will continue to make a name for themselves as authors of notable open-source software projects. These contributions to Chariot and other open-source security projects amplify the good that members of our Services team do to protect the world and solve the security problem.

Finally, Praetorian's machine learning team is working to revolutionize the world of static analysis. Their primary focus is on deep learning, paying particular attention to an assortment of advanced NN-based techniques and leveraging research and tooling from around the world. Their moonshot project demonstrates Praetorian's lofty ambitions and shows how important we believe it is to invest in creative and ground-breaking security solutions.

Chariot embodies Praetorian's core values of putting the client first, following our passion, struggling and celebrating together, and orienting toward action. In the end, we have the very great privilege of being able to offer our clients a simple, cost-effective automated solution to their product security problems. We commit to making security simple, signaling only when it matters, offering technical expertise on standby, and providing full-stack security support. This caliber of final product is what happens when we begin our approach to problem-solving by saying "yes, and…," then draw equally on the depth and breadth of intellectual talent and cutting-edge technical resources available to us. Chariot will make a crater in the cybersecurity industry, and we, the talent propelling it onward, get to shape its positive and far-reaching impact.

Diversity, Equity, Inclusion, and Belonging at Praetorian: Reflecting the World We Want to Protect

At Praetorian, our mission is to make the world a safer and more secure place. Literally: all our work comes down to protecting the vulnerable from those who would harm them in the realm of cybersecurity. We fundamentally believe that if our staff is all one type of person (cisgender, heteronormative, neurotypical, affluent white men as with most of our industry) then we limit that mission. We need to represent the world we are trying to save, and all the beauty and struggles that come along with it. Our goal to reach 50% diversity by the end of 2021 reflects a layered intention: To put our people first by creating a safe, inclusive, welcoming environment in which anyone can thrive. To put our clients first, also, by representing our world in all its complexity. And to set an example for diversity, equity, and inclusion (DEIB) that other cybersecurity companies can emulate.

Steps in the right direction

Praetorian was founded on the philosophical ideal of making craters: that we would change the landscape of our industry by finding solutions to problems rather than simply identifying them and accepting them as status quo. We recognize that the status quo in cybersecurity is neither diverse, equitable, nor inclusive. This problem is unacceptable, and we have a responsibility not only to find a solution but to influence change in our industry. And so we begin here, where we strive daily to build a psychologically and physically safe environment for all people. We intentionally engage with institutions, groups, and individuals that help us identify, access and engage applicants that represent the diverse talent we are looking to support. We celebrate our colleagues' differences and embrace them as they are. We have hard conversations with staff who make comments that are unacceptable, and we let people go who have not taken that coaching on board.

Over the past year, we have made significant improvements in more quantifiable DEIB areas, specifically with recruiting and compensation-leveling efforts. As a result, our staff is 35% diverse (an 84% increase over the past year) in contrast to global industry diversity averages of 11% female and 26% minority, as reported by the National Technology Security Coalition[1]. We are proud to partner with Girls Who Code and Women in Cybersecurity, and are seeking a partnership with My Brother's Keeper. These organizations help us identify underrepresented talent and provide guidance on internal policies so that we design an equal, inclusive, and safe space for all our staff. Longer term, we plan to reach out to high schools and colleges to sponsor programs that encourage women and minorities to consider cybersecurity as a viable career choice.

We also are proud of our equity-focused policies of interview loops and pay band transparency. For each new job posting, staff who will conduct the interviews hold a kick-off call with the purpose of defining the needs for the role. They use those clear requirements to design interview loops and create score cards using Greenhouse. The resulting interview process is equitable for every applicant.

Our pay bands are likewise designed to maximize equity. A study by the Applied Psychology Association[2] showed white males are more likely to negotiate successfully than their female counterparts, which when coupled with policies of compensation confidentiality leads to inequitable compensation for the same work. On average, women in the US workforce make between 10-24.4% less than their similarly qualified and experienced male counterparts, not accounting for any racial differences, according to the Institute of Women's Policy Research[3]. At Praetorian, though, our staff do not have to negotiate themselves into being paid at a rate equitable with their peers. We simply ensure that it happens. Our posted pay bands align with our core value of defaulting to open: transparency regarding salary leads to equal compensation across roles, regardless of any differences in gender, race, physical ability, or sexuality.

Moving forward

We almost certainly will make missteps as we move forward, but we will humbly acknowledge those and will seek to do better. That drive aligns directly with our core value of trying harder. We don't stop when things are hard or when we fail. We simply try again, and our approach to DEIB is no different. We will listen to voices of marginalized communities in an effort to understand and connect, design policies that have long-term effects across our organization, and view the results through a lens of humility. We will be proud of our successful efforts to increase our DEIB and acknowledge when we take a misstep. And we will reassess and try again, over and over, because the first step in shifting the status quo of the cybersecurity industry is building a company that reflects and is safe for the world we are driven to protect. ⬢

1. Patton, H. (2021). Cybersecurity diversity cannot be solved by tools or policy, but by the way we think. National Technology and Security Coalition Blog. https://www.ntsc.org/resources/ntsc-blog/cybersecurity-diversity-cannot-be-solved-by-tools-or-policy,-but-by-the-way-we-think.html

2. Dannals, J. E., Zlatev, J. J., Halevy, N., & Neale, M. A. (2021). The dynamics of gender and alternatives in negotiation. Journal of Applied Psychology. Advance online publication. https://doi.org/10.1037/apl0000867

3. Hegewisch, A., & Mefferd, E. (2021). The gender wage gap by occupation, race, and ethnicity 2020. Institute for Women's Policy Research Blog. https://iwpr.org/iwpr-issues/employment-and-earnings/the-gender-wage-gap-by-occupation-race-and-ethnicity-2020/

Tools and Core Values: BUILDING CULTURE IN A REMOTE WORLD

by Christopher Frakes

Historically, Praetorian Security has not been a remote organization. In fact, we have an office in downtown Austin with a pretty sweet view of the river. Like many other companies faced with the pandemic in 2020, we had to find a way to operate remotely while continuing to build and sustain our "secret sauce" culture. In learning to do precisely that, we have disproved the old idea that a virtual environment cannot foster camaraderie. While the trial and error has not been easy, we have adapted and continue to do so, struggling and celebrating together.

Our initial response looked like many others', incorporating systems like Slack and Google Meets to accomplish everything virtually from couches, kitchen tables, and home offices. We changed our onboarding process, what mentorship and collaboration look like amongst our teams, and how we communicate amongst ourselves and with clients. The underlying goal: to grow a sense of belonging when you are not sitting next to your coworkers.

Fortunately, Praetorian already had an environment of collaboration that adapted well to the virtual word, at least in part. Team members knew that they could reach out to one another for help in solving problems. The harder part was in recreating the sense of spontaneously turning around to ask a question, or catching up over a snack in the kitchen with people working on different projects. We also recognized the equally important need to ensure newly hired employees could integrate to the dynamics of--and build relationships with--team members who previously had worked face to face.

Our immediate approach to the first of these two particularly difficult problems was to further incorporate tools that enable employees, teams, and managers to communicate effectively. We forged an entirely new, remote first path wherein an environment of collaboration is integral to success. Among our tactical solutions are Namely for HRIS, Lattice for engagement, 1:1s, and performance, Predictive Index for better understanding baseline behaviors and team dynamics, Slack for constant communication, and Greenhouse Onboarding for facilitating an engaging remote onboarding experience.

The second hard problem--cultivating camaraderie--is an ongoing task with a multipronged approach much as it would be were we in-office. We offered games nights, poker night, lunch and learns, and fireside chats, with mixed success. We introduced Donut, which pairs employees to have coffee, eat lunch, and engage one another outside of work. We have dedicated Slack channels devoted to employees' personal passions. Each of us is equally responsible for fostering camaraderie, so we will continue working at it using the results from an employee survey to guide us toward what might be fun to try. Just like an impromptu happy hour leaving from the office, employees will drive this conversation.

Adapting our culture to a fully remote workforce entailed a year of learning on the fly, but the experience has prepared us well for a future hybrid model wherein employees can work remotely or from the office in Austin. Perhaps our greatest lesson has been the reminder that our culture is defined by our values. As we move forward, we will continue to ensure our core values are at the foundation of what we do.

What does that look like in practice?

- Our CEO, Nathan, defaulting to open about the vision he has for the company and having the difficult conversations about why decisions are made.
- Our security engineers, constantly putting the customer first.
- Our VP of Operations, Neil leaning into the yes, and…jumping in Day 1 to help solve hard problems across the organization

When a company's employees understand and exemplify its values, that "secret sauce" culture will grow stronger. None of our core values requires seeing someone face-to-face to implement. We align performance reviews and after-action reviews to values-based behaviors. We celebrate our wins together and tie them back to the mission in our all-hands celebration call each Friday. Most importantly, we practice humility every day when we log on to work intending to learn from colleagues with different perspectives than ours. The manner in which we go about collaborating and engaging with one another will develop more over time, but our pledge is to keep building an environment grounded in our core values!

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