VENIMUS, VIDIMUS, VICIMUS

PRAETORIAN

Team Survival Guide

Issue #10

FEATURED

- Ides of March – Chariot's Launch Day
- Best Places to Work
- Exploit Development Highlights
- Finding Secrets in Code Assets with Nosey Parker

Welcome

A mission. A meritocracy. A milestone. You wanted something a bit different than the standard cybersecurity experience. That's why you're here: we want that, too.

We want to make the world a safer and more secure place. We want a collegial community where people succeed based on the merit of their ideas and the degree to which they embrace our core values. We want the knowledge that we have pushed the envelope while following our passions, and in the process made craters in each other's lives, in our client's businesses, and in our industry.

You have a place here, in all of that. Is it chaotic at times? Sure. Meteors don't make craters without a fair amount of upheaval. But we struggle and celebrate together, and the charge we get from making the impossible possible? Indescribable. So, welcome. We can't wait to see the impact you make.

Nathan Sportsman
FOUNDER & CEO

praetorian

Table of Contents

Company / Essentials

Culture / Tech

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 **define 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.

The Survival Guide was deployed 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 content 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.

1 Monday

Monday you will meet with the IT team to get your laptops provisioned and have an initial intro into our systems. Reading the company magazine and starting your assembly challenge are both day-one activities. Today we answer the 'why' through an overview of the company and our strategy. You will also have lunch with your manager.

2 Tuesday

Tuesday you review a presentation covering People Operations. In addition, you can use Tuesday to complete your crossword puzzle and any onboarding 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.

3 Wednesday

Wednesday is for learning about Praetorian's Marketing and our current services offered. At Praetorian, we offer our clients outcomes and not hours billed - this is your opportunity to learn more about this approach.

4 Thursday

Thursday you will learn about our service delivery process, Chariot, and meet with our Finance team. Our PMO team will provide an overview of our delivery process, specifically focusing on the Engineer's responsibilities. You will learn about Chariot's value we deliver to customers. Our accountant will give an overview of Expensify and our reimbursement policy.

5 Friday

Friday is for learning about Praetorian's Sales offerings. While most company positions are technical, everyone needs to understand all aspects of the business at a high level.

Assignments for Week 1

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.

Recommended Reading

Throughout this Survival Guide you will find excerpts and a list of recommended reading.

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)*

Survival Guide

○ Complete crossword challenge

○ Complete "Assembly" challenge

○ Obtain signature from manager upon completion of this checklist

Readings

○ Read the Survival Guide

○ Obtain copies of recommended books

○ Begin month one readings from Box

Sign-in

○ Okta

○ Lattice

○ Box

○ Confluence

○ Expensify

○ Jira

○ 1 Password

○ Office 365

○ Salesforce (if applicable)

○ Slack

○ Pritunl VPN

○ Github (if applicable)

○ Google Mail/Calendar

○ Namely

Communication

○ Setup Praetorian email signature

○ Join rooms of interest on Slack

○ Connect with fellow Praetorians on your favorite social media platforms

○ Introduce yourself in **#company** channel on Slack

○ Create a bio in Namely

○ Update LinkedIn profile & post your new role *(be sure to tag Praetorian!)*

○ Complete first week company presentations

○ Attend meeting with manager

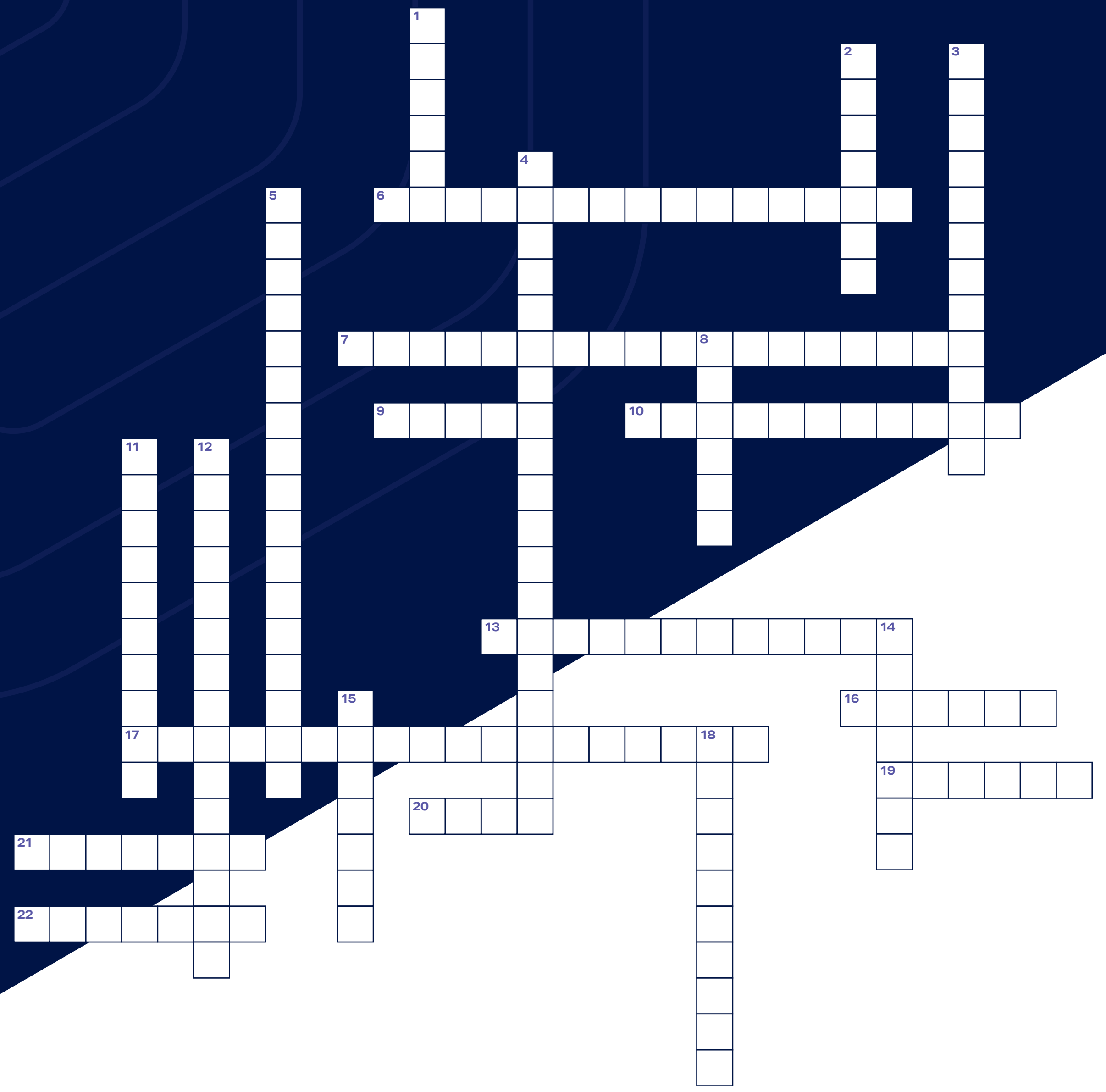
○ Attend meeting with mentor

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

TEAMMATE SIGNATURE

MANAGER SIGNATURE

DATE



Crossword Challenge

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

Across

6 Whose philanthropy system does the CEO follow?

7 Everything we do, we do as a team.

9 The mascot of the engineering team.

10 If you like dogs, join this Slack channel.

13 Find success and meaning through impactful work.

16 Open-source security scanner for Go.

17 If you like cats, join this Slack channel.

19 How do you save code changes to a source control management system in an engineering first culture?

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

21 To make the world a safer and more secure place.

22 Makes Praetorian more secure and sends unintentional and unintelligible Slack messages.

Down

1 To solve the cybersecurity problem.

2 Most advanced Offensive Security Platform on the planet.

3 Sniffs out secrets.

4 This is a small company trying to do big things. Every individual effort counts.

5 The biggest Lego set in the Austin office.

8 Similar to the Latin word tiger and a common Slack channel name.

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

12 Bias toward brutal truth over hypocritical politeness.

14 The world's first dedicated security scanner for Istio.

15 Lord of the Rings character inspired Praetorian's favorite party emoji.

18 Failure is inevitable, but fortitude will prevail. Nothing is impossible.

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.

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.

Lattice

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

Greenhouse Software

Greenhouse is our onboarding and recruiting system designed to help hire and onboard our new hires before their start date.

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!

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 employees' access to many applications and devices.

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.

GitHub

Our preferred continuous integration platform is where we develop internal capabilities, publish open-source tooling to the greater security community, and experiment with new ways to wow our clients.

Namely

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

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.

1 Password

1Password is used to generate, store, and retrieve complex passwords. 1Password is there when you need to log in, 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.

Mavenlink

Mavenlink is a professional services software that we use to optimize resources and boost operational performance. This includes project management and billable time management.

Resources List

Resources that have evolved our thinking as a company, and that we refer back to constantly.

Podcasts

DARKNET DIARIES

True stories from the dark side of the Internet. This is a podcast about hackers, breaches, shadow government activity, hacktivism, cybercrime, and all the things that dwell on the hidden parts of the network.

CYBER WIRE DAILY

The daily cybersecurity news and analysis industry leaders depend on. Published each weekday, the program also included interviews with a wide spectrum of experts from industry, academia, and research organizations all over the world.

SECURITY NOW

Steve Gibson, the man who coined the term spyware and created the first anti-spyware program, creator of SpinRite and ShieldsUP, discusses the hot topics in security today with Leo Laporte.

RISKY.BIZ

Published weekly, the Risky Business podcast features news and in-depth commentary from security industry luminaries. Hosted by award-winning journalist Patrick Gray, Risky Business has become a must-listen digest for information security professionals.

LAST WEEK IN AWS

Every week, listen to host Corey Quinn interview domain experts in the world of Cloud Computing to discuss AWS, GCP, Azure, Oracle Cloud, and how businesses are coming to think about the Cloud.

COMMAND LINE HEROES

Hear the epic true tales of how developers, programmers, hackers, geeks, and open source rebels are revolutionizing the technology landscape.

MALICIOUS LIFE BY CYBEREASON

Tells the unknown stories of the history of cybersecurity, with comments and reflections by real hackers, security experts, journalists, and politicians.

Technical 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.

IOS & ANDROID HACKER HANDBOOKS

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

MASTERING ETHEREUM

If you're looking to get started with the Ethereum protocol–or are among the many open source developers, integrators, and system administrators already working with this platform–Mastering Ethereum is the definitive book on the topic.

HANDS-ON GO PROGRAMMING

Praetorian is a Go shop! This book is designed to get you up and running as fast as possible with Go. You will not just learn the basics but get introduced to how to use advanced features of Golang.

THE CAR HACKER'S HANDBOOK: A GUIDE FOR THE PENETRATION TESTER

The Car Hacker's Handbook will give you a deeper understanding of modern vehicles' computer systems and embedded software. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems.

Technical Cont.

ADVANCED PENETRATION TESTING

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

NETWORK SECURITY ASSESSMENT

How secure is your network? The best way to find out is to attack it, using the same tactics attackers employ to identify and exploit weaknesses.

ADVERSARIAL TRADECRAFT IN CYBER SECURITY

This book will provide tips and tricks all along the kill chain of an attack, showing where hackers can have the upper hand in a live conflict and how defenders can outsmart them in this adversarial game of computer cat and mouse.

PENETRATION TESTING AZURE FOR ETHICAL HACKERS

Curious about how safe Azure really is? Put your knowledge to work with this practical guide to penetration testing. Develop practical skills to perform pen testing and risk assessment of Microsoft Azure environments.

RED TEAM DEVELOPMENT AND OPERATIONS

This book will provide you with the real-world guidance needed to manage and operate a professional Red Team, conduct quality engagements, understand the role a Red Team plays in security operations. You will explore Red Team concepts in-depth, gain an understanding of the fundamentals of threat emulation, and understand tools needed you reinforce your organization's security posture.

THE HACKER PLAYBOOK

Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing—including attacking different types of networks, pivoting through security controls, and evading antivirus software.

HOW TO HACK LIKE A GHOST (BE SURE TO CHECK OUT ALL OF THE SERIES BY SPARC FLOW)

Like other titles in the How to Hack series, this book takes you deep inside the mind of a hacker as you carry out a fictionalized attack against a tech company, teaching cutting-edge hacking techniques along the way.

UNIX AND LINUX SYSTEM ADMINISTRATION, 5TH EDITION

Excellent resource on general use and administration of *nix systems.

ARCH LINUX WIKI

Nominally specific to Arch Linux, but actually useful to many *nix systems. Great go-to resource!

THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE

True story in prose written by Cliff Stoll about detecting and responding to a Stasi intrusion at Lawrence Berkeley Lab in the 1980s. A great story that gives a good sense of the attacker/defender mindset.

HACKBACK! BY PHINEAS FISHER

This is a narrative account of Phineas Fisher's hacking of the Hacking Team. It is quite technical and pulls back the curtain on how attackers solve problems.

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.

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.

ONLY THE PARANOID SURVIVE

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

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.

THIS IS HOW THEY TELL ME THE WORLD ENDS: A CYBERWEAPONS ARMS RACE

An intrepid journalist unravels an opaque, code-driven market from the outside in – encountering spies, hackers, arms dealers, mercenaries, and a few unsung heroes along the way. As the stakes get higher and higher in the rush to push the world's critical infrastructure online, This Is How They Tell Me the World Ends is the urgent and alarming discovery of one of the world's most extreme threats.

THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS

An inside look at how governments, firms, and ordinary citizens can confront and contain the tyrants, hackers, and criminals bent on turning the digital realm into a war zone. The Fifth Domain delivers a riveting, agenda-setting insider look at what works in the struggle to avoid cyberwar.

A LEADER'S GUIDE TO CYBERSECURITY

Why Boards Need to Lead and How to Do It: Cybersecurity threats are on the rise. As a leader, you need to be prepared to keep your organization safe.

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 are 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 of things I haven't gotten used to yet. A few times before we were about to kick off 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.

Building a culture of excellence

Vision
To solve the cybersecurity problem.

Mission
To make the world a safer and more secure place.

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.

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 come 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 & celebrate together
Everything we do, we do as a team.

The Praetorian Way:

People First, Always.

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 are 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..."

These 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.

COMPANY

Developing the Red Team Practice

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's 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.

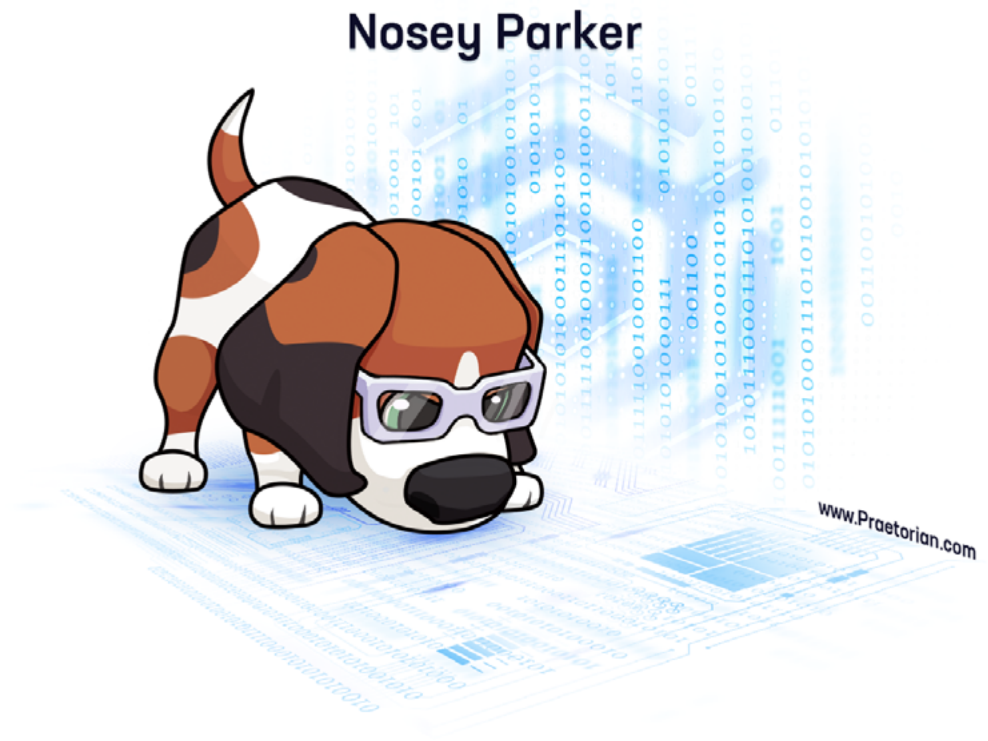
In addition to improving our capabilities, Praetorian began taking on **unique customers with atypical requirements**. Dallas and Weems conducted the company's first supply-chain operation scenario in 2019. Up to this point, Red Team operations were classic "Enter from the outside" scenarios. This operation was unique in that it simulated an adversary inserting a malicious package into a company's 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. 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, Nate Kirk, 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.



Finding Secrets in Code Assets with Nosey Parker

Time and time again in client engagements at Praetorian, we have discovered exposed secrets in source code repos, CI/CD assets, configuration files, and application and firmware bundles.

These secrets include things like credentials for cloud provider accounts, API tokens, and database connection strings. These exposed secrets have sometimes provided initial access to a client's systems in a Red Team engagement; at other times they have permitted complete bypass of a client's sophisticated access control rules.

To amplify the ability of security engineers at Praetorian to **find exposed secrets**, we developed Nosey Parker, a secrets scanner that uses machine learning techniques to produce high-quality results. In typical usage, more than **80%** of reported findings are true positives. This is just one example of how we combine machine learning with offensive security at Praetorian.

Nosey Parker can scan files, directories, and the history of Git repositories, identifying likely secrets. It operates in two modes:

THE FIRST uses regular expressions to detect secrets, followed by a machine learning-based denoiser that filters out things that look like noise (such as an AWS API key like **AKIA0000EXAMPLE10000**). This mode uses a high-performance regular expression engine and carefully chosen algorithms, resulting in **3-100x faster operation** than other regular expression-based secret scanners. Our development team performed a manual review of more than 15000 data points, optimizing for high signal-to-noise, before carefully choosing the set of regular expressions used for matching. We periodically update it based on real-world feedback from Praetorian security engineers, to improve its ability to detect secrets that it missed on recent engagements.

THE SECOND mode uses a cutting-edge deep learning model trained on source code to detect secrets. We used techniques published in the last 3 years to build it on top of a self-supervised deep neural network. This mode requires no explicit rules from a subject matter expert; it can detect secrets whose format we have not previously seen. This mode is much more computationally expensive than the regular expression-based scanner, and hence runs on GPUs in Google Cloud instead of on the laptop of a security engineer.

Beyond simply scanning for secrets, Nosey Parker reports its findings in JSON and human-readable formats. Unlike other secret scanners, it deduplicates its findings, reporting each detected secret once with a list of locations where it was detected. In practice, this deduplication results in a **5-10x reduction** in the total number of findings for a human to review.

Nosey Parker currently is available to Praetorian employees as a Docker image, and we encourage its use in client engagements when source code or other textual assets are available. It is also now available on GitHub Open-source here: https://www.praetorian.com/newsroom/open-sources-nosey-parker/.

GoKart: The First Year

At the time of this publication, Praetorian Labs had just celebrated the one year anniversary of releasing our first open source tool, GoKart. Our engineers review Go code in their day-to-day client engagements, and this tool has significantly improved the signal-to-noise ratio for them.

Outside of Praetorian, growth tracking data clearly demonstrates that we have made a crater in our industry with this tool in addition to increasing the efficiency of our own work. In just a year **we've seen 31,000 clones** of the repository and 8,907 downloads of the release binaries. More than **2,000 people have starred** the GitHub repository, and nearly 100 have forked it.

GoKart is a Game Changer

GoKart is a static application security testing (SAST) tool that finds security vulnerabilities in Go code. While neither the first nor the last tool was created for this purpose, GoKart stands out due to its lower false positive rate and its taint-tracking functionality. Taint tracking allows GoKart to determine code paths where user-controllable data has the potential to reach a vulnerable function, reducing the frequency of false positives. The net result is a more **user-friendly, more accurate, less noisy experience** for Go users, along with an increased ability to quickly understand full attack paths for high-impact issues.

How GoKart Works

GoKart works by using the Go analysis package to build a call graph. It puts Go code into single static assignment (SSA) form, structuring every value computed by the program as an assignment to a unique variable. In a security context, SSA can help us trace back to the source of input data. It also simplifies the GoKart implementation by allowing it to handle only SSA primitives. Use of SSA also enables constant propagation during analysis, which allows the analyzer to evaluate expressions that are not literals (e.g. misconfigurations or code vulnerabilities that only occur under certain conditions). By reasoning with constant propagation, GoKart is able to further reduce the frequency of false positives. ●

Coming Up Next for GoKart

We have seen such fantastic community involvement, including bug fixes and adding GoKart to Homebrew package management. We also have received many suggestions for improvements. Future work will include the addition of further analyzers to detect additional types of vulnerabilities, support for Go generics in version 1.18, and analysis improvements for properly handling the programmatic concurrency of Go channels.

Contact **careers@praetorian.com** if you would like to have a full time role making a significant impact on GoKart and other open source security applications.

Exploit Development Highlights

Our Labs team relishes an exploit development challenge. We are highlighting three from the past year.

ProxyLogon, March 2021

1. What is it? CVE-2021-26855 is a vulnerability on Microsoft Exchange Server that allows an attacker to bypass authentication and impersonate users.
2. How did we reverse engineer it? We examined the differences between the vulnerable version and Microsoft's patched version, then deployed a test environment of the vulnerable version to observe instrument deployment. This gave us knowledge of typical communication, which we then investigated until we had a full, working end-to-end exploit.
3. Why does it matter? We used the ProxyLogon vulnerability in conjunction with a common Active Directory misconfiguration to achieve organization-wide compromise.

Log4j, December 2021

1. What is it? CVE-2021-44228 is a vulnerability in Java that evaluates log statements for certain "lookups" before writing to the log file. The most dangerous of these performs a JNDI lookup on a user-controlled value.
2. Why does it matter? We built a Log4j scanner into Chariot, our Attack Surface Management tool, which has helped us detect the vulnerability for our clients. We have inadvertently discovered this vulnerability in adjacent systems that were not the direct target of our scans. Worse yet, these adjacencies were not obvious even to well informed defenders.
3. How do we suggest clients mitigate it? The best defense against this vulnerability is to patch all 2.x Log4j versions to 2.16.0. Clients also should disable Log4j Lookups, remove dangerous .class files, and add prefixes like **`${jndi:`** to a blocklist in a web application firewall to block exploit attempts.

Spring4shell, March 2022

1. What is it? CVE-2010-1622 is a vulnerability in Spring Core on JDK9+ that allows remote code execution. Exploitation requires an endpoint with DataBinder enabled (e.g. a POST request that decodes data from the request body automatically) and depends heavily on the servlet container for the application.
2. Why does it matter? This vulnerability allows an unauthenticated attacker to execute arbitrary code on the target system.
3. How can we detect successful exploits? The first option is to search for the pattern **`/.*\.?[Cc]lass\..*/`**, and the string `class.module.classLoader` in the request body or query parameters of HTTP requests followed by a 200 response code. That is costly in terms of retaining access logs, though, so a second option is to review files written to the webserver by the user under which the application is running.

The Voice of a Client:

NPS at Praetorian

Praetorian's singular focus on information security consulting means we deliver unbiased expertise. Our team also keeps our clients' bigger pictures in mind in order to help them understand both the ground truth about their security programs and the implications for each client's future. We are proud to have earned **the trust of Fortune 1000 companies** that return year after year confident that we will deliver honest, direct, innovative results in the most efficient way possible. In fact, they are so satisfied that their referrals account for 80 percent of our new business.

We take client feedback so seriously that we track our Net Promoter Score (NPS) on a weekly basis. NPS is a survey system that calculates client satisfaction based on their responses to a single question:

> ***How likely are you to recommend our company to a colleague?***

The scoring for this answer is based on a 0-10 scale. Clients who answer 9 or 10 count as "promoters," while those who answer 0 to 6 are "detractors." We subtract the percentage of detractors from the percentage of promoters to yield our NPS. The final score can be as low as -100 (everyone is a detractor) or as high as 100+ (everyone is a promoter). An NPS greater than 50% is considered excellent. Widely recognized organizations have the following NPS as of August 2022, for context: **Apple, 52%; Amazon, 54%; Costco, 60%; Netflix, 51%.**

In contrast, Praetorian has a **rolling two-year NPS of 93%**. We put a significant amount of weight into what clients tell us through NPS scores and take them very seriously. When we get feedback that is positive, we know to analyze what we did well on a particular engagement and try to model that behavior more widely. Similarly, when we get feedback that a client would not promote us to their peers, or even if they were neutral about our performance, we know to take a critical look at what we could have done better so as to improve in future engagements.

Our insanely high NPS is a testament to our culture and the synergy of our core values. We put the client first, trusting everything else will work out. However, we don't stop there. We own our mistakes, leaning into discomfort and learning what went wrong when we do get a "detractor" response. Then we continue trying harder, following our passion and adapting along the way to improve the experience for the client every time. Our NPS demonstrates that we are making craters not only in the realm of cybersecurity, but in the day-to-day security of our clients. We absolutely celebrate that success together! ●

CHARIOT
Beware the Ides of March
Don't end up on the wrong side of an attack.
Chariot security platform.
praetorian

Chariot's Launch Day

Advances in SaaS and DevOps that transform global business also expand the attack surface. Knowing the unknowns is the first step, but ransomware and talent shortages compound the risks organizations face from constantly changing attack surfaces. We have decided security needs to go on offense. What if organizations could cut through noise, extend their security teams, and reduce false positives to zero? Our all-in-one offensive security service helps our clients do all of that.

Chariot is the first all-in-one managed offensive security platform that comprehensively catalogs internet-facing assets, contextualizes their value, identifies and validates real compromise paths, and tests companies' detection response programs. This is not a traditional managed security service that provides staff augmentation or manages third party equipment. Instead, Chariot combines Praetorian's offensive security expertise with proprietary technology automation and AI to continuously focus and improve defensive investments for enterprises. Marty Garvin, the Head of Security at Rubrik, excitedly remarked "Praetorian's deep security experience as a continuous service? Yes please!" when we proposed Chariot to him.

CONTINUED ON NEXT PAGE . . .

Key Features

Chariot Identify provides comprehensive attack surface discovery by combining outside-in adversarial expertise with inside-out integrations for cloud systems, container registries, source code managers, and CI/CD pipelines.

Chariot Attack prioritizes risk with zero false positives. Our defensive operators exploit dangerous exposures to confirm risk and demonstrate impact using constant, automated mapping of the evolving attack surface.

Chariot Detect retraces compromise paths to ensure clients can detect and respond to real attacks. Using automation and **MITRE ATT&CK** expertise, we quickly identify gaps and benchmark each client's detection abilities.

Chariot Prevent enables client security teams to flag security policy violations and enforce compliance by defining policy as code.

Key Benefits

Comprehensive Attack Surface Mapping

Using AI-driven outside-in and inside-out mapping techniques, Chariot continuously and comprehensively catalogs each organization's external attack surface.

Modern and Advanced Threat Simulation

Praetorian's offensive security engineers rapidly adopt and codify new attacker tactics and techniques to pressure test each client's cybersecurity posture against the latest threats.

Zero False Positives

Our security experts validate vulnerabilities to remove false positives, confirm the criticality of potential security exposures, and demonstrate impact through compromise.

Beyond a Product, Chariot's Managed Service is a Partnership

Security experts operate as an extension of clients' security teams, working within their collaboration channels to alert them on critical risks, align on mitigation strategies, validate remediation, and improve detection and prevention controls. Praetorian delivers the only end-to-end security platform and managed service that acts like attackers to protect clients. As Adam Page, CISO for Zurich Insurance, remarked, "Chariot is so much more than a product. Chariot is a partnership that enables material improvement of our cybersecurity program through close collaboration with Praetorian's security experts."

As an extension of our client's security teams, Praetorian helps enterprises achieve business resilience by continuously discovering assets, contextualizing their relationship and import, pinpointing vectors of compromise, and personalizing protection to remediate future risk. Melody Hildebrandt, CISO at Twentieth Century Fox, noted,

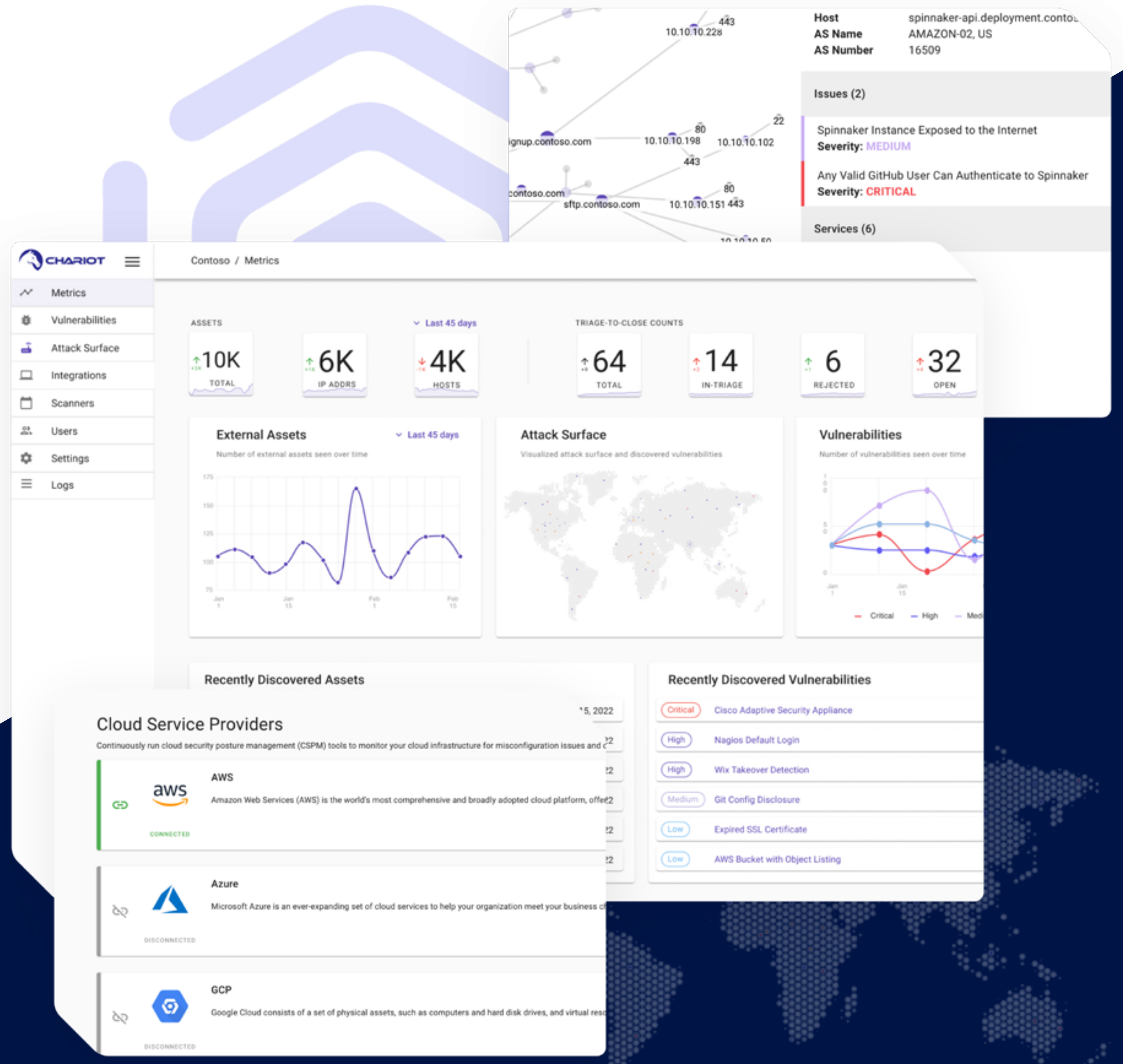
> **“**
>
> ***The Chariot platform pressure tests our cybersecurity program's effectiveness every single day***

Clients engage with Praetorian offensive security engineers and experts to locate their critical exposures and continuously validate their cybersecurity program. ●

References

1. Chariot Solution Brief / 2. Chariot EASM E-Book / 3. Chariot 23 Nuclei Template Release

> **“**
>
> ***Chariot is so much more than a product. Chariot is a partnership that enables material improvement of our cybersecurity program through close collaboration with Praetorian's security experts.***



Host	spinnaker-api.deployment.conto
AS Name	AMAZON-02, US
AS Number	16509

Issues (2)

Spinnaker Instance Exposed to the Internet
Severity: MEDIUM

Any Valid GitHub User Can Authenticate to Spinnaker
Severity: CRITICAL

Services (6)

External Assets: Number of external assets seen over time

Attack Surface: Visualized attack surface and discovered vulnerabilities

Vulnerabilities: Number of vulnerabilities seen over time

Recently Discovered Assets

Recently Discovered Vulnerabilities

Critical	Cisco Adaptive Security Appliance
High	Nagios Default Login
High	Wix Takeover Detection
Medium	Git Config Disclosure
Low	Expired SSL Certificate
Low	AWS Bucket with Object Listing

Cloud Service Providers

Continuously run cloud security posture management (CSPM) tools to monitor your cloud infrastructure for misconfiguration issues and c

AWS: Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offe

Azure: Microsoft Azure is an ever-expanding set of cloud services to help your organization meet your business c

GCP: Google Cloud consists of a set of physical assets, such as computers and hard disk drives, and virtual reso

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 increase diversity 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, inclusion, and belonging (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. Ad- vance 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/

Your "Assembly" Test

Be prepared to show off your lego set during our Friday celebrations call

ASM × LEGO

Assembly is a low-level programming language for a computer, microcontroller, or other programmable device.

Much like the programming language, our "Assembly" test is also very low-level. During your first day at Praetorian you will select a LEGO set and get to work.

Meet the Leadership Team

Guess Who?

Nathan

CEO

Juan

VP, Services

Alex

VP Product

Richard

CTO

Andy

COO

Amanda

Controller

Taylor

VP, Sales

Write the letter from the description under the person you think it matches. Each Praetorian member has listed 5 fun facts about themselves for you to learn more about them, as well as help you solve this puzzle!

A

- The US Navy once told me I was "negatively buoyant"
- I've been skydiving
- I'm a "New Yorker" but come from a part of the state that is populated by more dairy cows than people

B

- Met spouse at summer nerd camp in high school
- Lived on Oahu for 3 years and want to move back
- National champion fencer and arm wrestling enthusiast

C

- My left eye is half blue and half brown
- My first job was at Whataburger
- At 16, I chose to get a computer over getting a car

D

- Has 2 Siberian cats
- A 3 time winner of the National Flute Association Jazz Flute Competition (true!)
- Panelist at one of the first 5 DefCon's - but I'm not telling which one (!)

E

- Has held 4 citizenships and lived in 4 countries, currently living between Dubai and Miami
- Spent 6 years on the swimming world circuit
- Adopted a 3-legged Saluki named Rahrah

F

- I happen to think Nickelback is a great band
- I hold a Level 1 Sommelier certification
- My first sales job was pushing a lemonade cart

G

- Parent to an almost 2 year old Leukemia warrior
- Love to travel - Been to Everest Base Camp, 6 continents, 29 countries, and counting
- I do aerial silks, scuba diving, and outdoor rock-climbing

Best Place to Work

by Michelle Rhodes

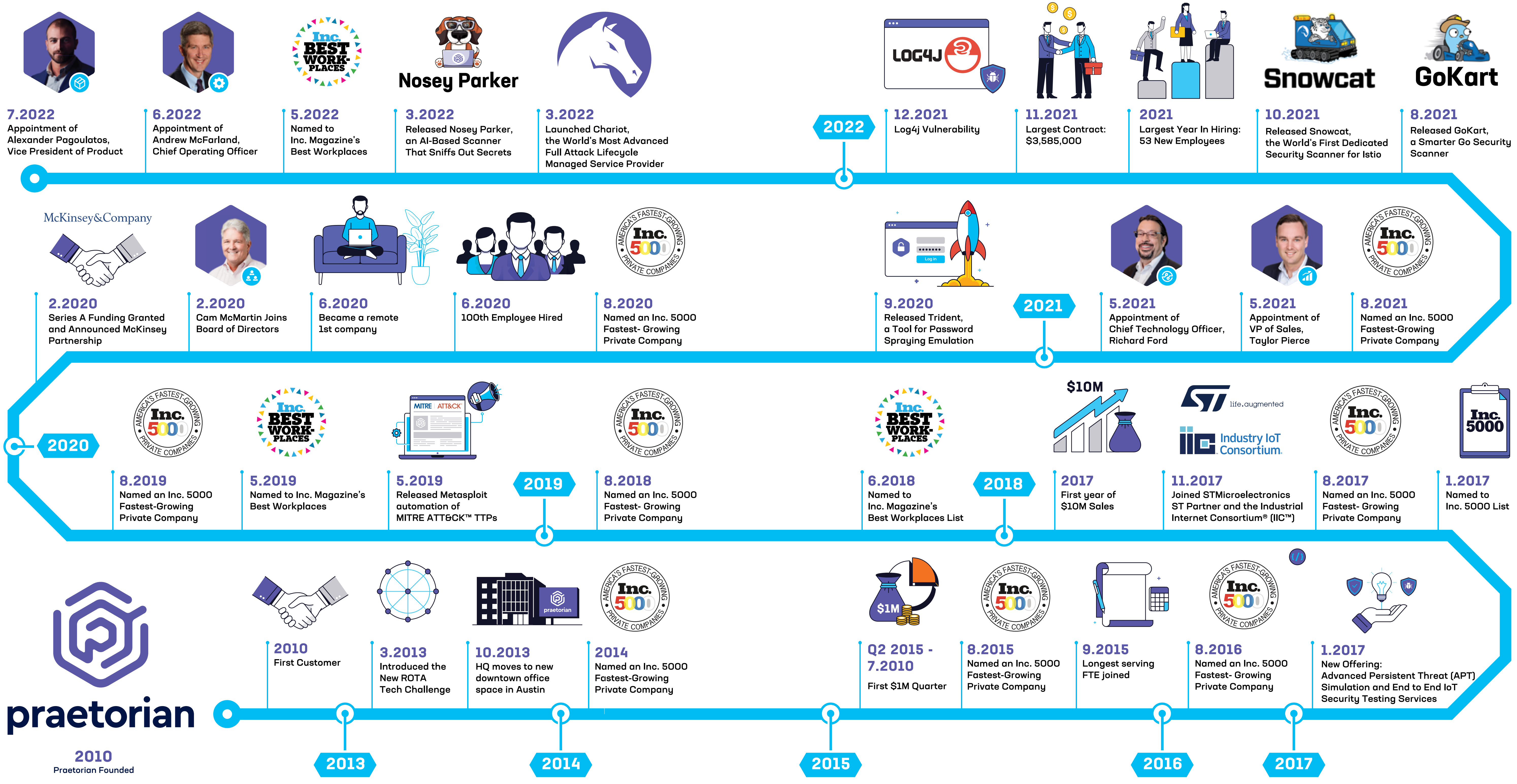
When Inc. Magazine named Praetorian on their Best Workplaces list for 2022, we were thrilled.

We love working here, and are incredibly proud that a nationally recognized publication agrees that we have an exceptional workplace and company culture. Our cultural focus on our core values has paired with a seamless transition to remote work that allows us to connect as a community from wherever we happen to be working. One response to the Inc. Magazine survey captured the feeling perfectly when they wrote, “My coworkers are brilliant, everyone is highly motivated, and there's constantly cool work being done by everyone at the company. This shop is exactly what I've wished some other places I worked at were like.”

Perhaps our most radical response to the pandemic–declaring ourselves permanently Remote First during Summer 2020–paved the way for our thriving virtual workplace in 2022. Since one of our core values is to struggle and celebrate together, we set a goal to grow a sense of connection despite not sitting next to each other. Leaning into the discomfort of change enabled us to reach for deep, long-lasting solutions and invest the energy in truly transitioning. We changed our onboarding process, mentorship and collaboration structure, and internal and client-facing communication methods. To facilitate all of these process shifts, we incorporated tools that prioritized virtual interactions, such as Slack, Google Meet, Namely, Lattice, Predictive Index, and Greenhouse Onboarding. No one likes limbo, and we didn’t sit in uncertainty for very long.

In fact, we realized instead that none of our core values requires seeing someone face-to-face to implement. Once we let go of what “always was” we found we were excited to embrace the potential for making craters for our clients while following our passions from our spaces at home. The emphasis on performance, hard work, and creativity persist, and every single person still matters. As one employee noted on the Inc. Magazine survey, “I am treated like an individual, valued person. I have massive flexibility in my hours and how I get my work done. The metrics for success are clear and fair. My compensation and benefits are extremely generous. The negatives are minor nit-picks relative to the benefits of working here.” ●

Praetorian in the years



2010
Praetorian Founded

2010
First Customer

3.2013
Introduced the New ROTA Tech Challenge

10.2013
HQ moves to new downtown office space in Austin

2014
Named an Inc. 5000 Fastest-Growing Private Company

Q2 2015 - 7.2010
First $1M Quarter

8.2015
Named an Inc. 5000 Fastest-Growing Private Company

9.2015
Longest serving FTE joined

8.2016
Named an Inc. 5000 Fastest- Growing Private Company

1.2017
New Offering: Advanced Persistent Threat (APT) Simulation and End to End IoT Security Testing Services

1.2017
Named to Inc. 5000 List

8.2017
Named an Inc. 5000 Fastest- Growing Private Company

11.2017
Joined STMicroelectronics ST Partner and the Industrial Internet Consortium® (IIC™)

2017
First year of $10M Sales

6.2018
Named to Inc. Magazine's Best Workplaces List

8.2018
Named an Inc. 5000 Fastest- Growing Private Company

5.2019
Released Metasploit automation of MITRE ATT&CK™ TTPs

5.2019
Named to Inc. Magazine's Best Workplaces

8.2019
Named an Inc. 5000 Fastest-Growing Private Company

2.2020
Series A Funding Granted and Announced McKinsey Partnership

2.2020
Cam McMartin Joins Board of Directors

6.2020
Became a remote 1st company

6.2020
100th Employee Hired

8.2020
Named an Inc. 5000 Fastest- Growing Private Company

9.2020
Released Trident, a Tool for Password Spraying Emulation

5.2021
Appointment of Chief Technology Officer, Richard Ford

5.2021
Appointment of VP of Sales, Taylor Pierce

8.2021
Named an Inc. 5000 Fastest-Growing Private Company

8.2021
Released GoKart, a Smarter Go Security Scanner

10.2021
Released Snowcat, the World's First Dedicated Security Scanner for Istio

2021
Largest Year In Hiring: 53 New Employees

11.2021
Largest Contract: $3,585,000

12.2021
Log4j Vulnerability

3.2022
Launched Chariot, the World's Most Advanced Full Attack Lifecycle Managed Service Provider

3.2022
Released Nosey Parker, an AI-Based Scanner That Sniffs Out Secrets

5.2022
Named to Inc. Magazine's Best Workplaces

6.2022
Appointment of Andrew McFarland, Chief Operating Officer

7.2022
Appointment of Alexander Pagoulatos, Vice President of Product

praetorian