

# TEAM SURVIVAL GUIDE

## FEATURED

**Our North Star**

**What is Chariot?**

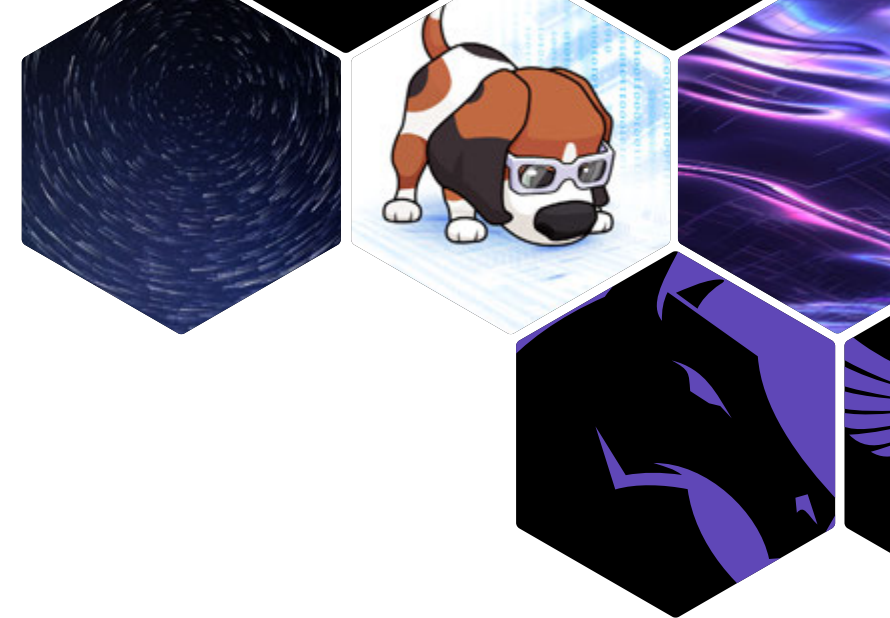
**Your First Week at Praetorian**

**Your First Assembly Challenge**





**To all those who have historically contributed to cyber and those who have yet to make discoveries.**



# Contents

<b>One Metric That Matters: Our North Star</b>	Page 04
<b>Social Media</b>	Page 06
<b>Praetorian By The Numbers</b>	Page 07
<b>What is Chariot?</b>	Page 08
<b>NPS at Praetorian</b>	Page 12
<b>The Trust Behind Our Success</b>	Page 13
<b>The Quest for Cyber Excellence</b>	Page 14
<b>Attack Surface Management</b>	Page 18
<b>Mercury AI: The Future of Reporting is Here</b>	Page 20
<b>Finding Secrets in Code Assets with Nosey Parker</b>	Page 22
<b>The Evolution of Red Teaming: Past, Present, and Future</b>	Page 24
<b>Unity Across Continents</b>	Page 26
<b>A Milestone of Excellence</b>	Page 30
<b>Your First Week at Praetorian</b>	Page 34
<b>Your First Assembly Challenge</b>	Page 38
<b>Praetorian Leadership</b>	Page 42
<b>Recommended Reading</b>	Page 46
<b>Where Warlocks Stay Up Late</b>	Page 50

# One Metric That Matters: Our North Star



by **Charlie Gelatt, Vice President of Operations**

At Praetorian, our quest for cybersecurity excellence is fueled by a North Star Metric (NSM) that aligns every team effort with our ambitious goals. This guiding principle, combined with our Objectives and Key Results (OKRs) framework, shapes our path to success.

## The Centaur Approach: A Unique Business Breed

Embracing the “Centaur” model, Praetorian blends the scalability of unicorns with sustainable profitability. This unique approach is essential in cybersecurity, where rapid change requires both adaptability and robust solutions. By focusing on repeatable and scalable operations, we ensure growth without sacrificing innovation or service quality.

## Explaining our North Star Metric, All Stars Align

At Praetorian, our NSM—“Number of uncovered material risks that were successfully mitigated”—directly supports our mission and vision.

By prioritizing this metric, we not only achieve our mission of preventing breaches, but also advance our vision of a culture of exceptional security standards.

## Driving Progress with OKRs

Our OKR framework helps us set high-reaching objectives with clear, measurable key results. This approach ensures alignment across the company, fosters transparency, and drives collective progress toward our NSM.

By integrating these principles, Praetorian ensures a unified direction and a culture of collaboration and transparency—vital for our growth and innovation.

## Strategic Insights



### Scalability and Repeatability:

Focus on processes that accelerate growth.



### Unified Direction:

The NSM provides a singular, clear target.



### Structured Progress:

OKRs establish quarterly metrics that drive our goals.

Our NSM isn't just a goal; it's the beacon guiding our rise to leadership in the cybersecurity industry. For more on our journey and achievements, visit [praetorian.com](https://praetorian.com).

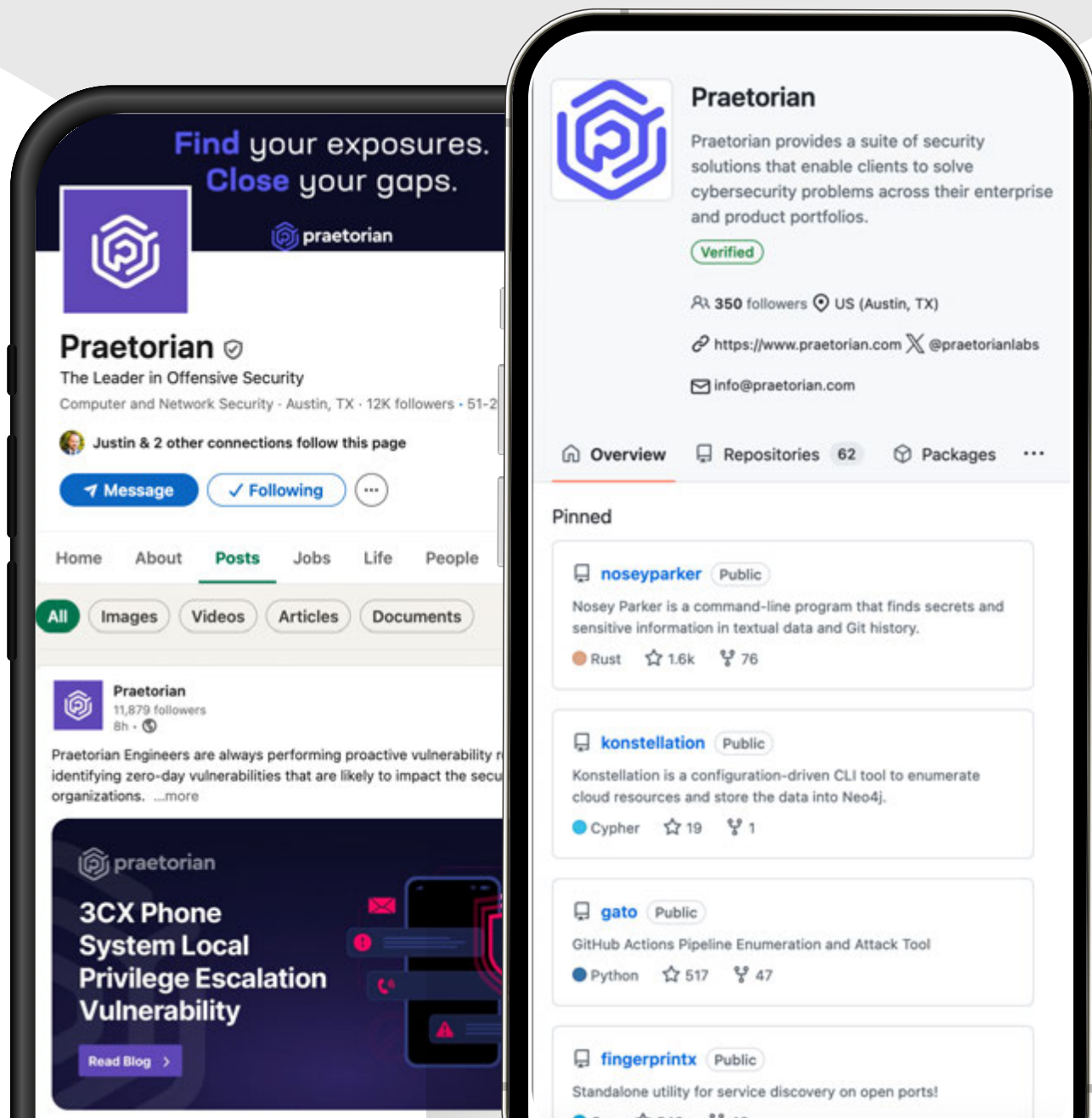
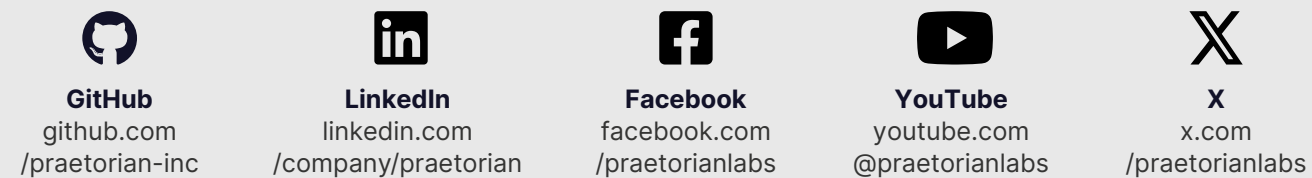
**Mission Alignment:** Our mission is to “prevent breaches before they occur.” By focusing on identifying and addressing material risks, we proactively strengthen defenses and prevent potential breaches, ensuring our clients are safeguarded against emerging threats.

**Vision Alignment:** Our vision is to “create a culture without compromise.” This metric reflects our commitment to maintaining the highest security standards. By consistently uncovering and mitigating risks, we embody a culture of uncompromising excellence and proactive security.

**Company-Wide Impact:** Tracking this metric drives company performance and continuous improvement. It keeps us aligned with our mission and vision, ensuring that we deliver superior results and enhance our clients' security posture.

# Social Media

Here at Praetorian, we are protecting the vulnerable through bleeding edge offensive technology. Keep up with our work through our social media and blog. Follow us for the latest.



# Praetorian by the Numbers

A snapshot of our people, accomplishments, and milestones across the world.





# What is Chariot?

Chariot, Praetorian's Continuous Threat Exposure Management workhorse, provides comprehensive attack surface discovery, outside-in adversarial engagement, inside-out attacker simulation, cloud integrations, source code protection, CI/CD pipeline coverage, and synchronization with trusted workflow management systems. Chariot is Praetorian's all-in-one security tool that never sleeps. It's like having a team of expert hackers constantly checking your digital world for weak spots.

## Key Features

### Attack Surface Management

Using tools like subfinder, Assetfinder, Massscan, WHOIS, and others, Chariot seeks, finds, and presents a picture of your Assets.

### Cyber Threat Intelligence

Chariot monitors emerging threats, providing detailed analysis of new vulnerabilities, exploits, and attack vectors from a variety of trusted sources.

### Breach & Attack Simulation

Breach & Attack Simulation (BAS) safely mimics real-world attacks to find weak spots before hackers do. It's like a fire drill for your digital defenses.

### Managed Service Provider

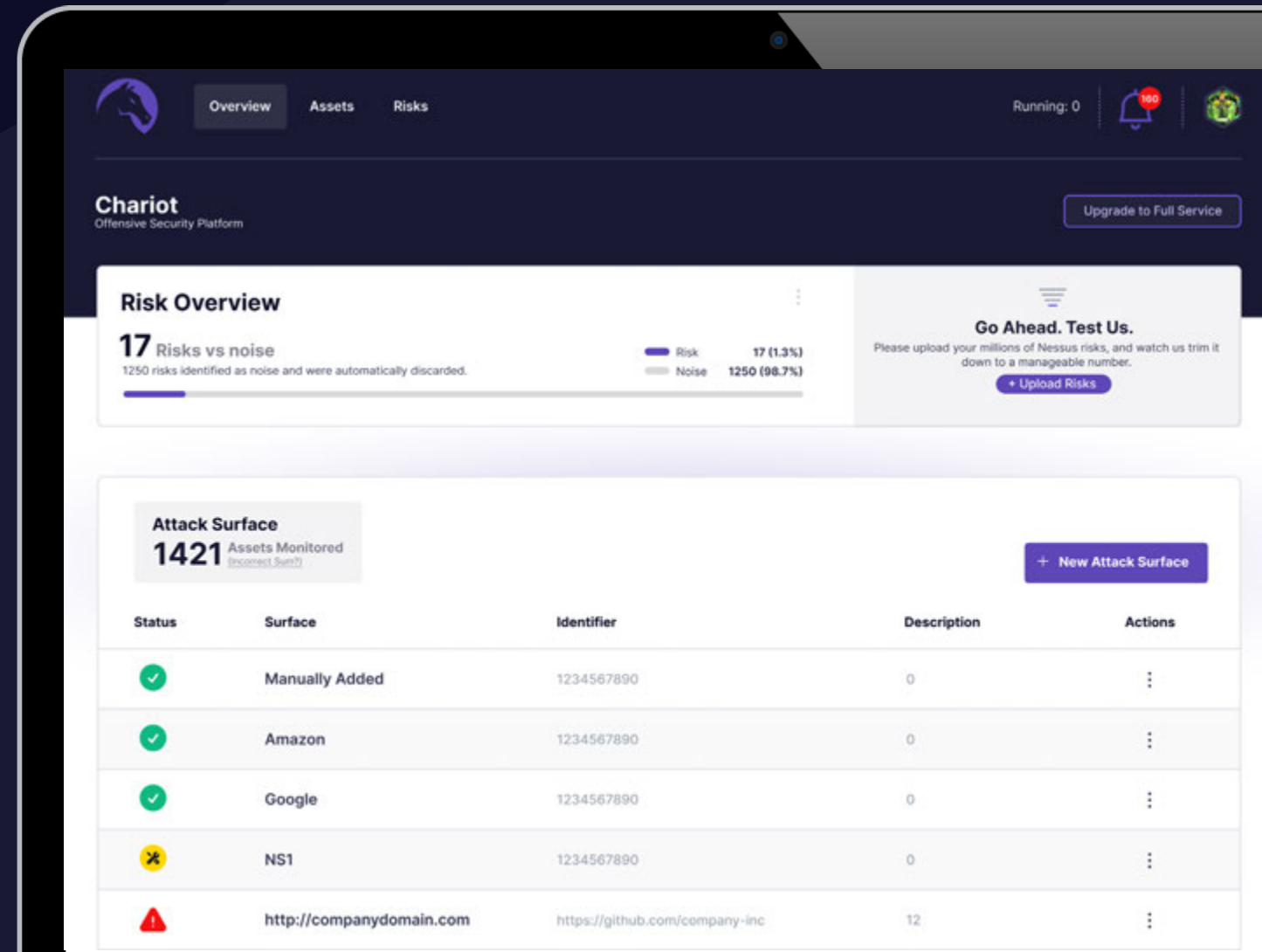
Our Managed Service Provider (MSP) is your organization's dedicated threat exposure management team.

### Vulnerability Management

Our Vulnerability Management (VM) services identify, assess, and mitigate security vulnerabilities across your digital infrastructure.

### Endpoint Detection & Response

Endpoint Detection & Response (EDR) acts as a vigilant digital guard, continuously monitoring your devices for suspicious activities.



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.

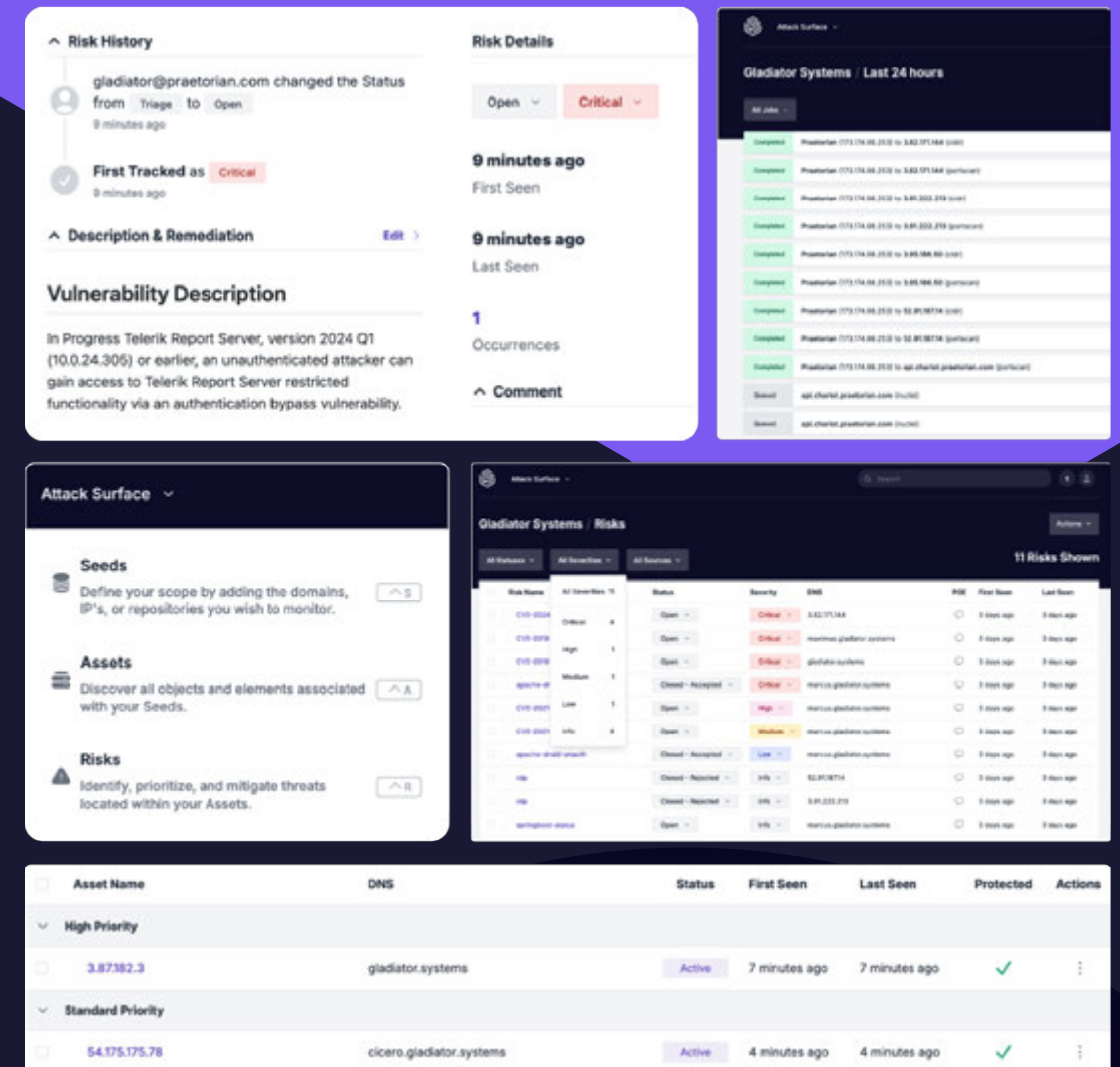
-Adam Page, CISO for Zurich Insurance

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

Security experts operate as extensions 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 extensions of our clients' 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.



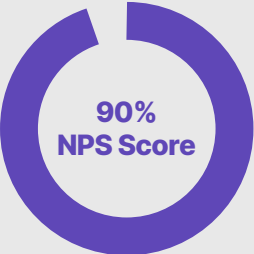
# NPS at Praetorian

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 their futures. We are proud to have earned the trust of Fortune 1000 companies who 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% 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: 61%, Amazon: 73%, Costco: 79%, Netflix: 67%



**90% NPS Score**

**Customers are so satisfied that their referrals account for 80% of our new business.**



In contrast, Praetorian has a rolling two-year NPS of 90%. 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 Exceptionally 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 try 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!

# The Trust Behind Our Success

## SAMSUNG

"We chose Praetorian primarily for the domain expertise, which is IoT in our case, and the security expertise in general."



"From the get-go Praetorian had a great process in place that kept the X team informed and filled in what to expect. The issues found will help prevent loss in trust in the product. Looking forward to many more engagements."

## Nielsen

"I think of Praetorian as one of only a handful of trusted partners in the security space. I feel confident that the things that are most likely to cause my team to drop everything are going to be more likely to be found by Praetorian than anyone else."



"Praetorian brings an expertise that my team just doesn't have. They come in with a different perspective."

NETFLIX

HBO

The New York Times

AP

THE WALL STREET JOURNAL

amazon

Google

Microsoft

salesforce

intel

vmware

servicenow

Qualcomm

APPLIED MATERIALS

stripe



# The Quest for Cyber Excellence

How Praetorian Engineers Lead the Way



by **Mande Blackwell**

BlackHat and DEFCON are crucial events in the cybersecurity world, where innovation and collaboration drive the future of digital defense. These conferences are not just showcases of technical prowess, but vital forums where new tools, techniques, and findings are shared for the greater good. At Praetorian, our engineers are deeply involved in this ecosystem, using their expertise to advance the field and address emerging cyber threats.

## The Significance of BlackHat and DEFCON

At these conferences, cutting-edge research and tools are unveiled, shaping the industry's approach to security. For example, John Stawinski's presentation on self-hosted GitHub CI/CD runners highlighted critical vulnerabilities in these increasingly complex systems. As Stawinski notes, "CI/CD pipelines are getting more and more complex, which creates more room for errors and misconfigurations." His insights underscore the importance of addressing these issues proactively to prevent security breaches.

Similarly, Matthew Jackoski and Mitchel Jordan introduced Vishline, a tool designed to mimic the voice and tone of an internal help desk bot, gaining sophisticated access via social engineering and showcasing these security challenges. Their work exemplifies how new tools can set new standards and enhance our ability to defend against emerging threats. Jackoski, along with Mason Davis, also developed GitHub Attack Toolkit (Gato), an enumeration and attack tool that has significantly advanced our understanding of identifying and exploiting pipeline vulnerabilities with Githubs public and private repositories.

### Vishline

A tool designed to mimic the voice and tone of an internal help desk bot

### Gato

An enumeration and attack tool that has significantly advanced our understanding of identifying and exploiting pipeline vulnerabilities with Githubs public and private repositories

[/praetorian-inc/gato](#)

## Praetorian Engineers at the Forefront

Our engineers are not just participants at these conferences; they are leaders in the cybersecurity community. They apply their findings from BlackHat and DEFCON directly to their work at Praetorian, enhancing our ability to tackle complex security issues.

Matthew Jackoski shared his experience from a challenging Red Team engagement with a financial services company, noting, "Getting that initial foothold was painful. It was a test of perseverance. Always try harder, don't stop trying." This perseverance is critical in offensive security, where success often requires innovative approaches and relentless effort.

Mitchel Jordan highlights the collaborative spirit of these conferences, saying, "A rising tide lifts all boats. We're all trying to make each other's companies more secure through offensive security." This ethos of mutual support and shared knowledge is central to advancing cybersecurity as a whole.

These events are essential for growth and leadership. Mark Rowlands emphasizes the importance of helping engineers transition from practitioners to leaders. By fostering an environment where engineers can step out of their comfort zones and engage in thought leadership, we support their development and contribute to the future of cybersecurity.

**"A rising tide lifts all boats. We're all trying to make each other's companies more secure through offensive security."**

- Mitchel Jordan

## The Demand for Top Cyber Talent

The need for top cybersecurity talent is more intense than ever. The field is highly competitive, with the demand for skilled professionals far exceeding the supply. As our Technical Director, Anthony Paimany, points out, “Remaining relevant for over 15 years is a big time commitment. It’s almost a full-time job to stay up to date with the latest developments.” This relentless pace underscores the importance of hiring the best talent and fostering a culture of continuous learning and adaptation.

At Praetorian, our approach to hiring reflects the brutal realities of the cyber talent market. We prioritize candidates who are not only technically proficient, but also aligned with our mission to advance the field. Our guiding principles are a direct reflection of how we select and develop our talent, ensuring they are equipped to handle the complexities of modern cybersecurity challenges.



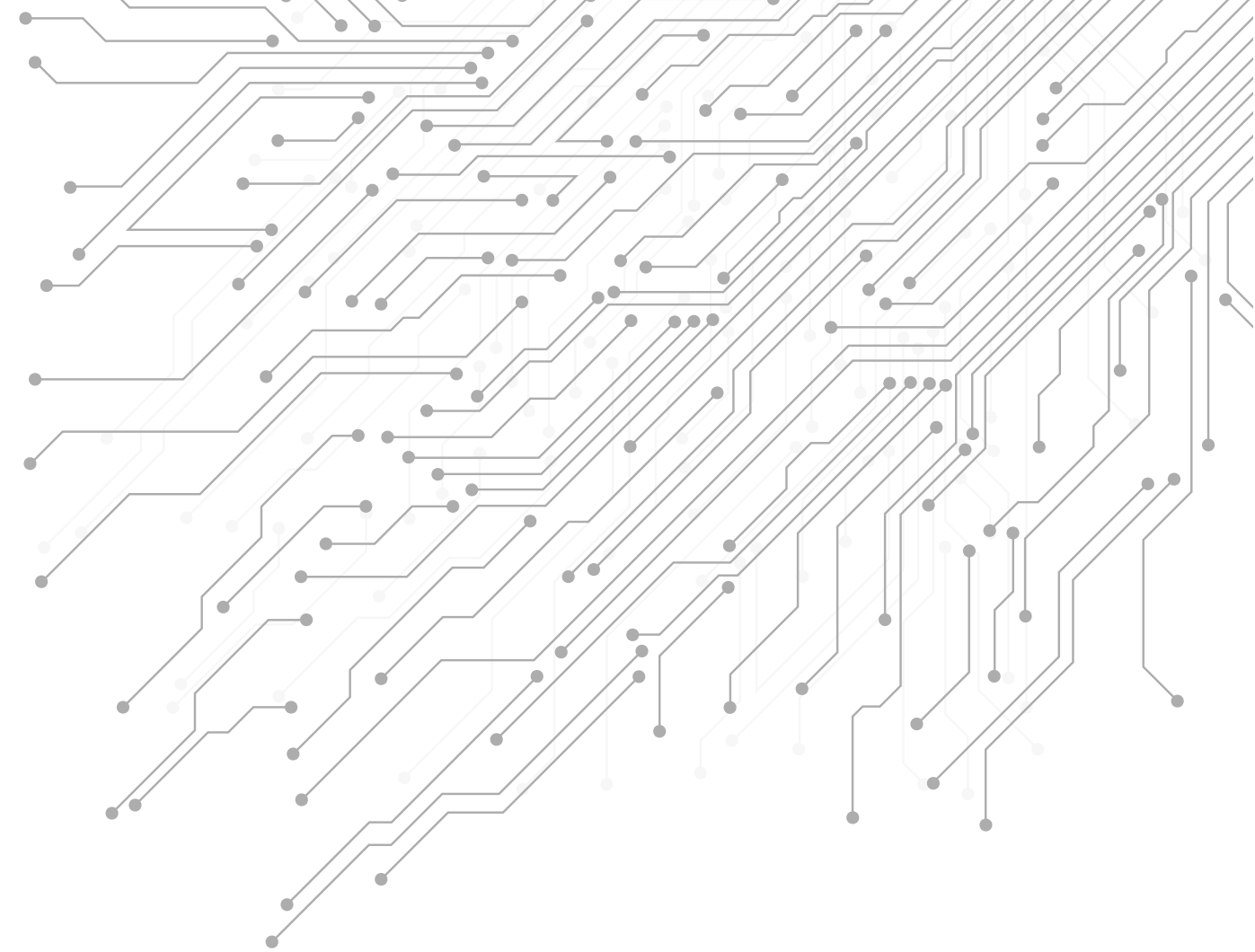
## Red Team Analogies and the Offensive Security Landscape

In offensive security, red team engagements are akin to a high-stakes chess game. Our engineers think several moves ahead to anticipate and counteract potential threats. The evolving landscape, with increasing complexity in systems like CI/CD pipelines, requires this strategic mindset to stay ahead of adversaries.

The future of offensive security will likely involve more automation and continuous monitoring. Anthony Paimany envisions a shift toward using platforms like Chariot and leveraging large language models to enhance our capabilities. “We need to be continuous,” he says, “and to do that, we need to leverage automation.”

Risk Name	Severity
<input type="checkbox"/> CVE-2019-11248	Critical
<input type="checkbox"/> CVE-2007-3010	Critical

Class	Count
<input checked="" type="checkbox"/> All Classes	138
<input type="checkbox"/> Weakness	110
<input type="checkbox"/> Exposure	19
<input type="checkbox"/> Misconfiguration	9



## Conclusion: “Stay Curious”

BlackHat and DEFCON are pivotal in shaping the future of cybersecurity, offering a platform for sharing knowledge and driving innovation. At Praetorian, our engineers contribute significantly to these discussions and apply their expertise to advance the field. The demand for top cyber talent is fierce, and our commitment to hiring and nurturing the best ensures that we remain at the cutting edge of cybersecurity. By staying engaged with the latest developments and fostering a culture of excellence, we continue to make a substantial impact in the fight against cyber threats.

## Are you ready to join our Mission?



# Attack Surface Management

A Free Enablement Technology for Effective Continuous Threat Exposure Management



by Nathan Sportsman

As digital threats evolve, organizations must stay vigilant about their attack surfaces. However, a troubling trend has emerged: companies often end up paying bug hunters for vulnerabilities discovered through surface-level scans, leading to costly and reactive security measures.



At Praetorian, we offer a solution that challenges this norm. Our Chariot platform now features a free Attack Surface Management (ASM) module, empowering organizations with crucial tools to proactively manage risks.

## The Problem with Current Practices

Relying on bug bounty programs and external researchers can lead to significant expenses and a reactive security stance. Paying for each vulnerability discovered promotes a piecemeal approach to cybersecurity, where immediate threats are addressed, rather than managing overall risk systematically. This method can also incentivize attackers to find and exploit weaknesses for financial gain.

## Praetorian's Vision: Free ASM

We believe ASM should be a foundational capability accessible to all. By providing our ASM module at no cost, we shift the focus from reactive vulnerability discovery to proactive risk management. This module includes:



**Exposed Secrets in Code:** Automatically detects sensitive data inadvertently exposed in repositories



**Repository Status Changes:** Monitors changes to repository visibility to prevent accidental exposure



**New Public Repositories:** Alerts on newly public repositories to manage potential risks



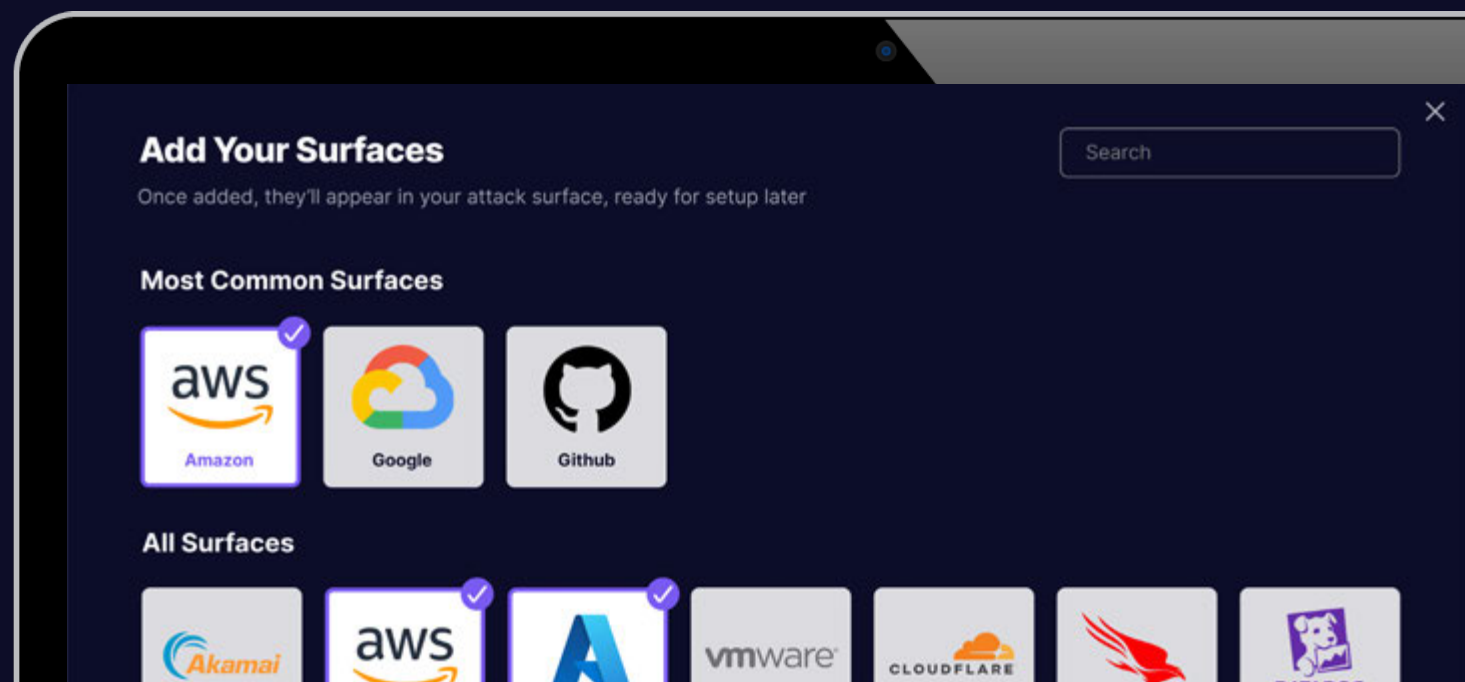
**GitHub Self-Hosted Runners:** Identifies vulnerabilities in CI/CD pipelines

## Shifting Focus to Material Risks

ASM offers visibility into potential attack vectors, but the real value lies in how this information is used. A comprehensive CTEM program should prioritize vulnerabilities based on impact, employ continuous monitoring, and integrate threat intelligence to anticipate and mitigate threats effectively.

## Conclusion

Attack Surface Management is a critical component of a robust cybersecurity strategy. By offering our ASM capabilities for free, Praetorian aims to democratize essential security tools, enabling organizations to focus on proactive risk management rather than reactive vulnerability patching.





# Mercury AI: The Future of Reporting is Here



by **Janani Mukundan**

In the dynamic world of cybersecurity, reports are more than just documentation—they are a pivotal communication tool that bridges the gap between technical teams and top executives, CISOs, and engineers. These reports offer a critical snapshot of a client's security landscape, spotlighting both strengths and vulnerabilities. They serve as a chronological record, tracking progress and pinpointing areas needing attention, which is essential for maintaining a proactive cybersecurity stance.



To ensure clarity and professionalism, consistency in report formatting and language is crucial. Uniform formats make reports accessible and understandable, regardless of the reader's cybersecurity expertise. Consistent language minimizes ambiguity and enhances Praetorian's credibility, enabling stakeholders to swiftly grasp critical insights and make informed decisions.

Enter Mercury, our cutting-edge reporting tool powered by an advanced Large Language Model (LLM). This revolutionary technology leverages sophisticated neural networks and transformer architecture to generate human-like text with unprecedented accuracy and context. Trained on a rich dataset of past reports, Mercury encapsulates the collective wisdom of Praetorian's engineers, delivering high-quality, actionable reports with exceptional speed and consistency.

Mercury and other LLMs excel at language tasks through complex algorithms and extensive computational resources. They understand context, relationships, and nuances in text, producing coherent and relevant content. Mercury benefits from a mix of open-source and proprietary models, enriching our reports with the latest insights and ensuring relevance to our clients' unique needs.

This integration of machine learning into our reporting process marks the beginning of a new era in offensive security engagements. Mercury sets the stage for more advanced and effective cybersecurity solutions, transforming how we deliver insights and drive proactive security measures.

# Finding Secrets in Code Assets with Nosey Parker



by **Brad Larson**

Time and time again in client engagements at Praetorian, we discover exposed secrets in source code repos, CI/CD assets, configuration files, and firmware bundles. These secrets include credentials for cloud provider accounts, API tokens, encryption keys, database connection strings, and more. These exposed secrets sometimes provide initial access to a client's systems in a red team engagement; at other times they enable pervasive lateral movement within a client's environment.

To augment 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.

Nosey Parker has been used to scan hundreds of terabytes of content and has produced findings in more than 200 reports from security engagements at Praetorian.

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



**Nosey Parker operates in Two Modes:**



Regular Expressions followed by Machine Learning



Learning Model trained to detect Secrets



The first mode uses regular expressions to detect secrets, followed by a machine learning-based denoiser that filters out things that look like noise (e.g., an AWS API key like AKIA0000EXAMPLE10000). Our development team performed a manual review of more than 15,000 data points, optimizing for high signal-to-noise, before carefully choosing the set of regular expressions used for matching. We periodically update the rules 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 past 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 runs best when a GPU is available. 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 5-100x reduction in the total number of findings for a human to review.



**5-100x reduction in findings for human review**



**Can detect secrets whose format has not been previously seen**

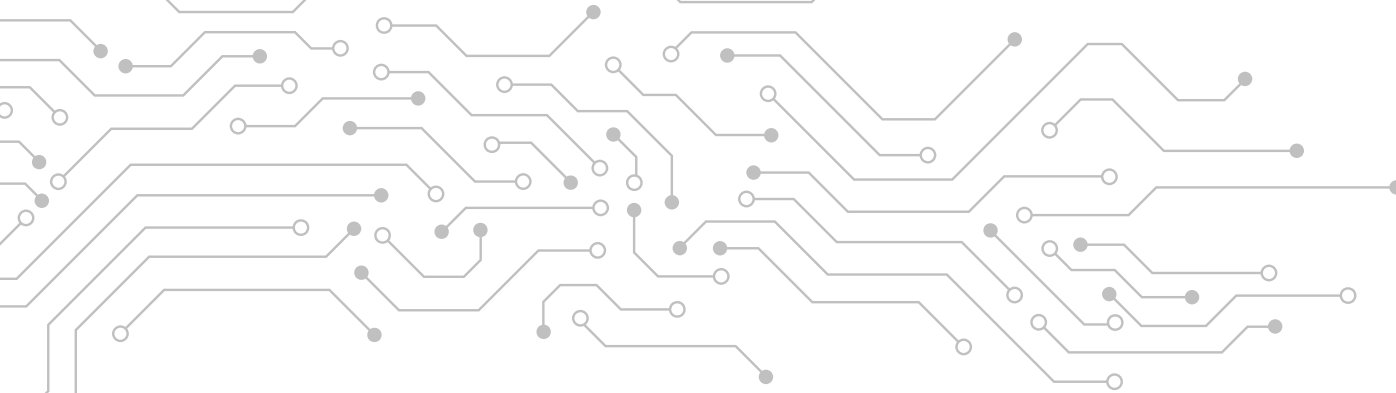


**Reports findings in JSON and human-readable formats**



**Nosey Parker is available as an Apache-licensed project on GitHub.**

An internal version with additional machine-learning features is available to Praetorian employees as a Docker image, and we encourage its use in client engagements.



# The Evolution of Red Teaming: Past: Present: and Future



by **Anthony Paimany**

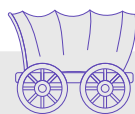


## Past, The Wild West of Cybersecurity

In its early days, cybersecurity had rudimentary Standard Operating Procedures (SOP) and Tactics, Techniques, and Procedures (TTP). Formal accreditation was almost nonexistent, and the field resembled the “Wild West”—unpredictable and full of unknowns.

Hackers of this era, often called the first and second generations, relied on limited knowledge from niche forums, Bulletin Board Systems (BBS), mailing lists, and IRC channels. This was before comprehensive cybersecurity literature, meaning much of what was known came from hands-on experience and shared insights. These hackers typically operated in environments dominated by Novell and Active Directory (AD), using systems with legacy stacks riddled with vulnerabilities. The attack surface was broad, and initial access was often gained through the external perimeter with relative ease. Attackers only needed to be right once to succeed, as detection and response capabilities were still underdeveloped.

Despite the potential for breaches, the overall impact of cyberattacks was relatively low, primarily due to limited reliance on technology and connectivity. Typical threat actors were often seen as “kids in basements,” motivated by curiosity and the thrill of hacking, rather than malicious intent.



### The Wild West

Attackers only had to be right once



### Iron Sharpens Iron

Attackers need to “think in graphs” and devise creative methods to breach increasingly mature environments



### Iron Sharpens Iron

Attackers will need to delve deeper into understanding SOPs and business processes to conduct successful attacks



## Present, The Maturation of Cybersecurity

Today, cybersecurity has evolved into a well-defined and crucial industry. The “iron sharpens iron” concept is evident with the rise of dedicated blue and red teams, often collaborating in a purple-team approach to enhance security.

The introduction of Endpoint Detection and Response (EDR) systems and the growth of Managed Security Service Providers (MSSP) have driven the need for advanced offensive research. Standard operating procedures (SOPs) and tactics, techniques, and procedures (TTPs) have become more sophisticated, adapting to improved defensive capabilities. Clients now demand higher standards from providers, with frameworks like MITRE ATT&CK, and regulatory standards such as CBEST, solidifying the industry.

While many environments remain AD-focused, there’s a rapid shift toward Software as a Service (SaaS) and cloud-based solutions, reducing the external attack surface. Today, attackers target appliances, hypervisors, and non-generic systems to evade detection. Defenders now hold an advantage, forcing attackers to “think in graphs” and develop creative ways to breach mature environments equipped with prevention, detection, and response capabilities.

The sources of knowledge have also changed. Platforms like X, Discord, blogs, podcasts, and Learning Management Systems (LMS) are now key resources for professionals. The profile of threat actors has also shifted, with Advanced Persistent Threats (APT), cybercriminals, and malicious individuals replacing the “hackers for fun” of the past.



## Future, The Next Frontier in Cybersecurity

Looking ahead, cybersecurity will likely embrace automation and continuous monitoring, moving away from today’s snapshot-based methods. The rising costs of research and development may lead to reduced information sharing as companies protect their investments in new technologies. Outsourcing aspects of cybersecurity, like command and control (C2) and initial access, may become more common, while regulatory mandates will continue shaping the industry.

The defense stack will mature further, with Extended Detection and Response (XDR) and a stronger focus on identity management. Attackers will need to evolve beyond traditional payloads and identity-based attacks, learning SOPs and business processes to conduct successful attacks. There’s concern that overemphasizing certifications and the ability to do the job without a deeper understanding could weaken future cybersecurity professionals, especially as the field becomes more accessible.

As the industry continues to evolve, knowledge sources will shift again, with video content and new platforms playing a larger role in education. While the defense market may consolidate, specialized offensive security services are likely to grow. With society’s increasing dependence on technology, the potential for more impactful attacks grows, especially with nation-state actors and the volatility of global security. The future of cybersecurity will be shaped by these challenges and opportunities, requiring ongoing innovation and vigilance to stay ahead of evolving threats.

# Unity Across Continents

## Building Culture in a Remote Startup



by Michelle Rhodes

In today's dynamic world, where the boundaries of geography and time zones blur, fostering a cohesive company culture and unity becomes paramount. At Praetorian, we take immense pride in being a remote-first startup that spans across 11 countries, with the exciting addition of a 12th in just a few months. Our global footprint is not just a testament to our growth but also to the rich diversity and unique skill sets that each of our team members brings to the table.

### Embracing Diversity

Diversity is the heartbeat of innovation. At Praetorian, our team members come from different corners of the world, each bringing their unique perspectives, experiences, and expertise. This diversity fuels creativity and innovation, allowing us to approach challenges with a wide array of solutions. Our commitment to hiring from various backgrounds ensures that we not only represent a global market, but also harness the best talent available, irrespective of location.

We understand that a diverse team is a strong team. It is through our differences that we find our strengths, and it is through our collective efforts that we achieve our mission of making the world a safer and more secure place. At Praetorian, every voice matters, and every perspective is valued.

As Mario Bartolome, Lead Security Engineer in Spain, shares:

**"I joined Praetorian almost two years ago. Until a month ago, I was the only Spaniard in the company, and recently, I was asked, 'How is that? Feeling lonely at times?' No. Not at all. Being alone is not the same as being lonely. And how could I feel alone, to begin with, in a company that believes in the remote-first principle so deeply? I've never felt alone or lonely in Praetorian because I have a team of more than a hundred people caring about me and what I do. In Praetorian, we make sure to have the tools and practices that keep us in touch in a meaningful way. When joining a company where everyone is welcome, the only differences you can tell are the time zones in the calendar events."**



## Building Unity in a Remote-First Environment

Creating a unified culture in a remote-first environment requires intentionality and dedication. At Praetorian, we prioritize communication, collaboration, and connection. Regular virtual meetings and check-ins help bridge the gap of physical distance, ensuring that our team members can connect on both professional and personal levels. We leverage state-of-the-art collaborative tools and platforms for seamless communication and project management, enabling our teams to work efficiently across time zones.

Understanding and respecting cultural differences is crucial in a global team. We promote cultural awareness and sensitivity through training and open dialogues, ensuring that every team member feels understood and valued. Additionally, regular team-building activities, both virtual and in-person, help strengthen bonds among our team members, creating opportunities for connection beyond work roles.

As Anthony Paimany, Technical Director in the UK, puts it:

**“At Praetorian, our remote-first culture is a core part of who we are. With colleagues from around the world, we benefit from diverse perspectives that enhance our work. We value an ego-free environment and prioritize openness and transparency in our communication. We are committed to supporting learning and development at all levels, keeping curiosity alive and well. Additionally, we make it a point to come together weekly to celebrate our achievements and build stronger connections.”**

## Harnessing Diverse Skill Sets

At Praetorian, we believe that our strength lies in our diverse skill sets. Our team comprises experts in cybersecurity, software engineering, data analysis, and more. This multidisciplinary approach allows us to tackle complex problems with a holistic perspective, delivering comprehensive and innovative solutions to our clients.

We encourage continuous learning and professional growth, providing our team members with opportunities to expand their skill sets and stay at the forefront of industry advancements. By investing in our people, we ensure that Praetorian remains a leader in the cybersecurity field.

Anthony further elaborates:

**“From my own experience, working from home allows me to maintain a healthy balance, facilitating my ability to keep fit and healthy, tend to family needs, and work without distraction. Leveraging a combination of regular webcam-enabled calls, Slack war room huddles, and engaging Slack channels, I feel connected and see my colleagues as they are—individuals.”**

## Looking Ahead

As we prepare to welcome our 12th country to the Praetorian family, we are excited about the new perspectives and expertise that will join our team. Our commitment to fostering a diverse, inclusive, and unified culture will remain unwavering, driving us toward greater innovation and success.

Praetorian's remote-first, globally diverse team is our greatest asset. By embracing diversity, building unity, and harnessing unique skill sets, we create a workplace where every team member can thrive and contribute to our shared mission. Together, we are not just a company; we are a global community united by a common purpose.

If you're passionate about making a difference and want to be part of a vibrant, inclusive team, explore the exciting career opportunities we offer, not only, in the US but around the world. Discover more on our [Careers page](#). Join us on this journey and be a part of something extraordinary. Together, we are Praetorian.





# Inc. Best Workplaces

2024

## A Milestone of Excellence

### Praetorian Named to Inc.'s Best Workplaces

This recognition is more than just a badge of honor; it is a testament to what makes Praetorian an exceptional place to work. The dedication exhibited daily by each team member truly sets us apart, highlighting the organic culture shaped by our people and the unwavering support from everyone at our company.

#### Why This Matters

This recognition is a testament to the vibrant and supportive environment we've cultivated. It not only celebrates our current achievements but also propels us toward future successes. At Praetorian, we lead by example, emphasizing the trust we place in our people to pioneer solutions that push boundaries and set new industry standards. Our company is defined not by our building, address, or logo, but by the people who make up our team.

#### A Word from Our Team

Elgin Lee, a seasoned Staff Security Engineer at Praetorian, was asked which song reminds him of Praetorian. Elgin picked the Pokémon theme song, "Gotta Catch 'Em All."

**"I wanna be the very best  
Like no one ever was  
To catch them is my real test  
To train them is my cause  
I will travel across the land  
Searching far and wide  
Teach Pokémon to understand  
The power that's inside"**

At Praetorian, we're committed to staying ahead of the game, capturing every opportunity to advance our skills and ensuring top-tier security across all operations. Each challenge is an opportunity for victory. We trust each other to lead initiatives that enhance our capabilities and drive us forward.

#### Looking Ahead

As we celebrate this recognition, we see it as just the beginning of our journey. With the strength and innovation of our people, we are not aiming to meet expectations, but to exceed them—10x, not just 10%. This is both a motivation and a call to action for those seeking a career driven by continuous improvement and bold innovation across the cybersecurity landscape. Together, we're not just securing the future; we're redefining it with the strength of our technology and the integrity and trust we cultivate within our talented team. Together, securing the future starts now!



**The Praetorian Way:  
Our company is defined not by our  
building, address, or logo, but by the  
people who make up our team.**

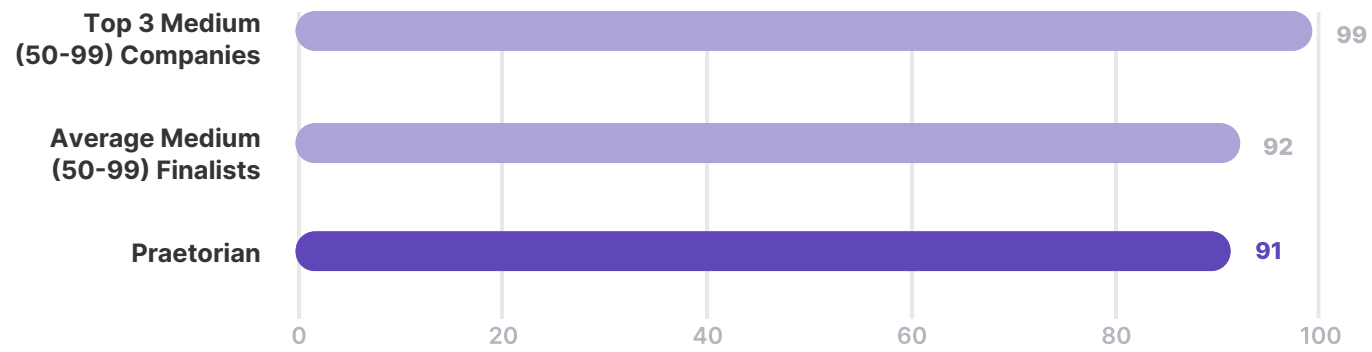
# Inc's Best Workplaces

Praetorian has won Inc's Best Workplaces award five times in the past seven years.



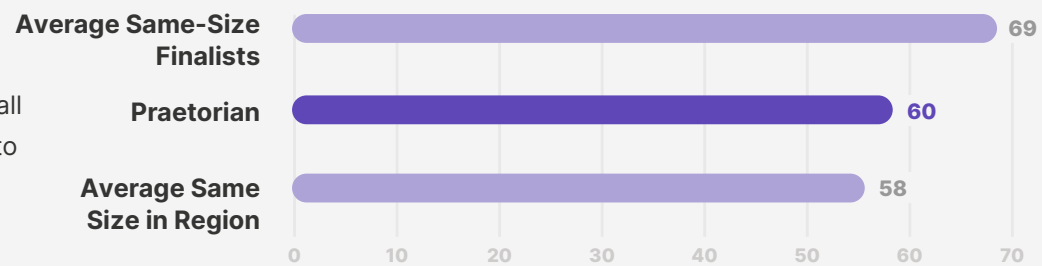
## Overview

73 Employees completed the survey, giving Praetorian an overall score of **90.68**.



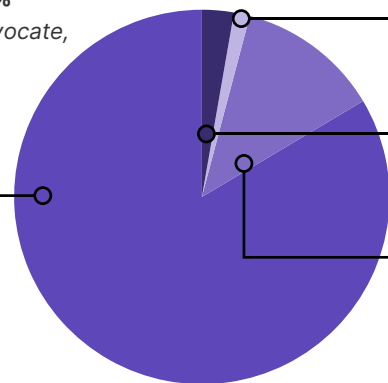
## Benefits

A comparison of all benefits offered to employees.



## Highly Engaged / 84%

Highly Favorable, Advocate, Intend to Stay, High Discretionary Effort



## Disengaged / 1%

Negative, Lacks Commitment, Impacts the Productivity of Other Employees

## Barely Engaged / 3%

Indifferent, Lack of Motivation, At-Risk for Retention

## Moderately Engaged / 12%

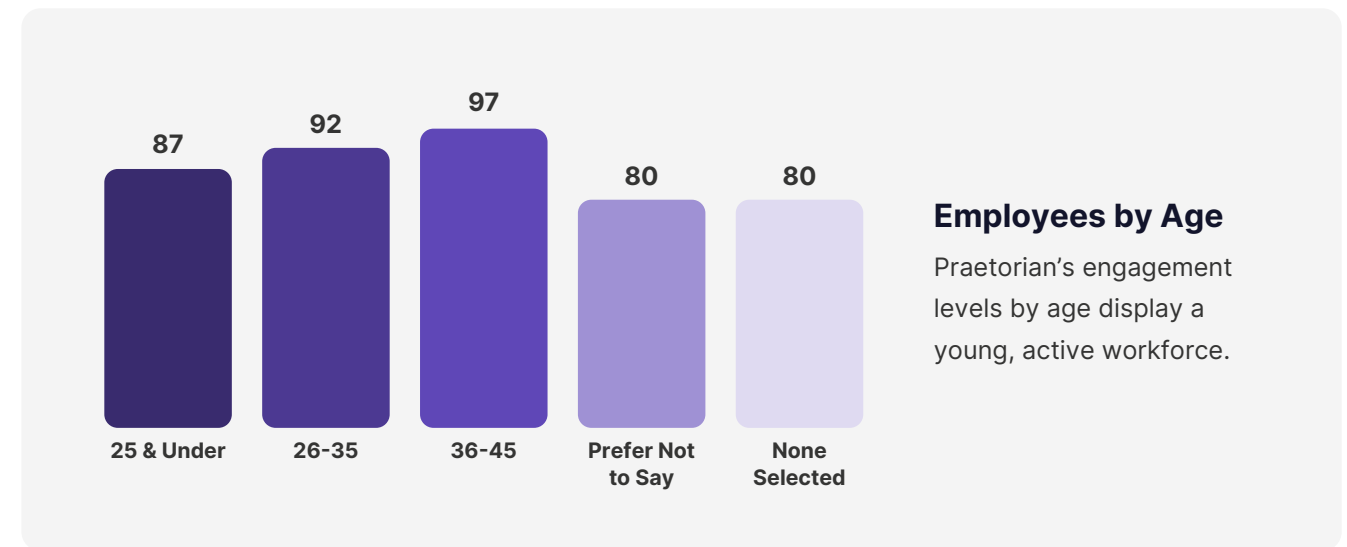
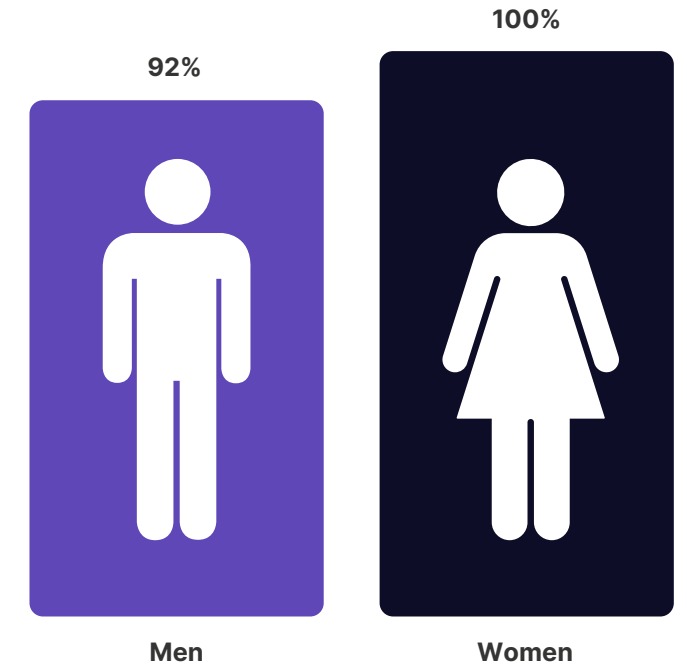
Moderately Favorable, Held Back, Opportunity for Increased Performance

## Employee Engagement

Looking at the attitudes and outlook of each employee.

## Employee Value

Employees understand how their contribution contributes to Praetorian's overall success.

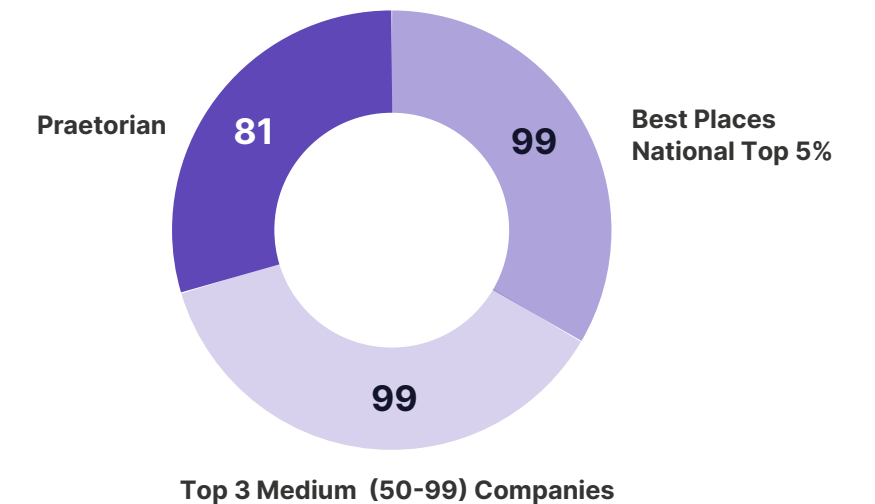


## Employees by Age

Praetorian's engagement levels by age display a young, active workforce.

## Leader Recognition

When asked if senior leadership recognizes their value, employees confirmed positively.



# Your First Week at Praetorian

An Opportunity to meet the Leadership Team and deep dive into the Company.

## IT & People Operations

On your first day you will meet with the IT team to get your laptops provisioned and have an initial intro into our systems. By the end of day 2, you should be able to answer the 'why' through an overview of the company and our NSM. There will also be a presentation covering People Operations to learn about our unique culture, recruiting, plus perks and benefits.

## Fun Your First Week

Throughout your first week, you can expect a company-sponsored lunch with your manager and team, along with opportunities to connect through various sessions. Be sure to join the Commitments call, the first of many, and get familiar with the company magazine as you start your assembly challenge. You'll have the chance to complete a crossword puzzle with fellow onboarders, wrap up onboarding tasks, and access our tech stack. You'll also meet your mentor and explore exciting topics like Car Hacking. Don't miss the water-cooler chat to connect with the company, and join the Celebrations call where we recognize the impact of our people and celebrate company-wide achievements.

## Professional Services & Chariot

During these sessions, you will learn about our service delivery process, and Chariot, our CTEM platform and how it delivers value to customers. Our teams will provide an overview of our delivery process, specifically focusing on the Engineer's responsibilities. You will also learn about our 10X Learning and Delivery training for our technical teams and how you can achieve the next level here. At Praetorian, we offer our clients outcomes and not hours billed. This is your opportunity to learn more about this approach.

## Sales, Marketing & Finance Overview

Later in the week is for learning about Praetorian's Sales offerings as well as deep dive into Praetorian's Marketing strategy. While most company positions are technical, everyone needs to understand all aspects of the business at a high level. In addition, you will meet our finance team who will give an overview of Expensify and our reimbursement policy.

# Getting Started Checklist

## Communication

- Set up your Praetorian email signature
- Join rooms of interest on Slack
- Connect with coworkers on social media
- Introduce yourself in the #company channel on Slack
- Create a bio in Namely
- Update your LinkedIn profile and post your new role (be sure to tag Praetorian!)
- Complete first week company presentations
- Attend meeting with Manager
- Attend meeting with Mentor

## Survival Guide

- Complete Crossword Challenge
- Complete Assembly Challenge
- Obtain signature from manager upon completion of this checklist

## Readings

- Read the Praetorian Survival Guide
- Obtain copies of recommended books
- Begin Month One readings from Box

## Sign-in

- Okta
- Lattice
- Box
- Confluence
- Expensify
- Jira
- 1Password
- Office 365
- Salesforce (if applicable)
- Slack
- Pritunl VPN
- GitHub (if applicable)
- Google Mail/Calendar
- Namely

## Enroll

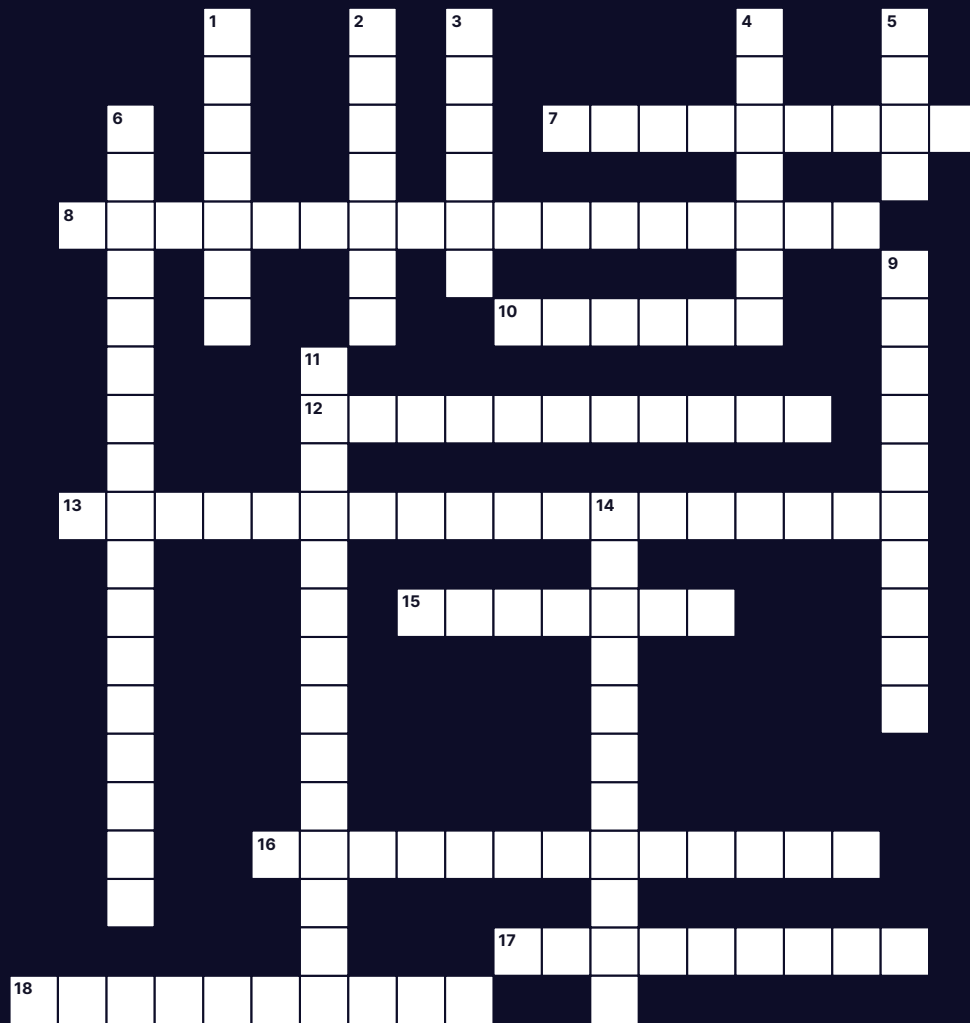
- Complete I-9 and W-4 forms
- Enroll in Direct Deposit
- Enroll in 401k Plan (Optional)
- Review Employee Benefits
- Opt-in to Health Insurance
- Obtain Capital One Card (if applicable)

### SERVICES TEAM

- By the end of your first week, you will have identified and pushed your first vulnerability to a customer.

### PRODUCT TEAM

- By the end of your first week, you will have submitted your first pull request.

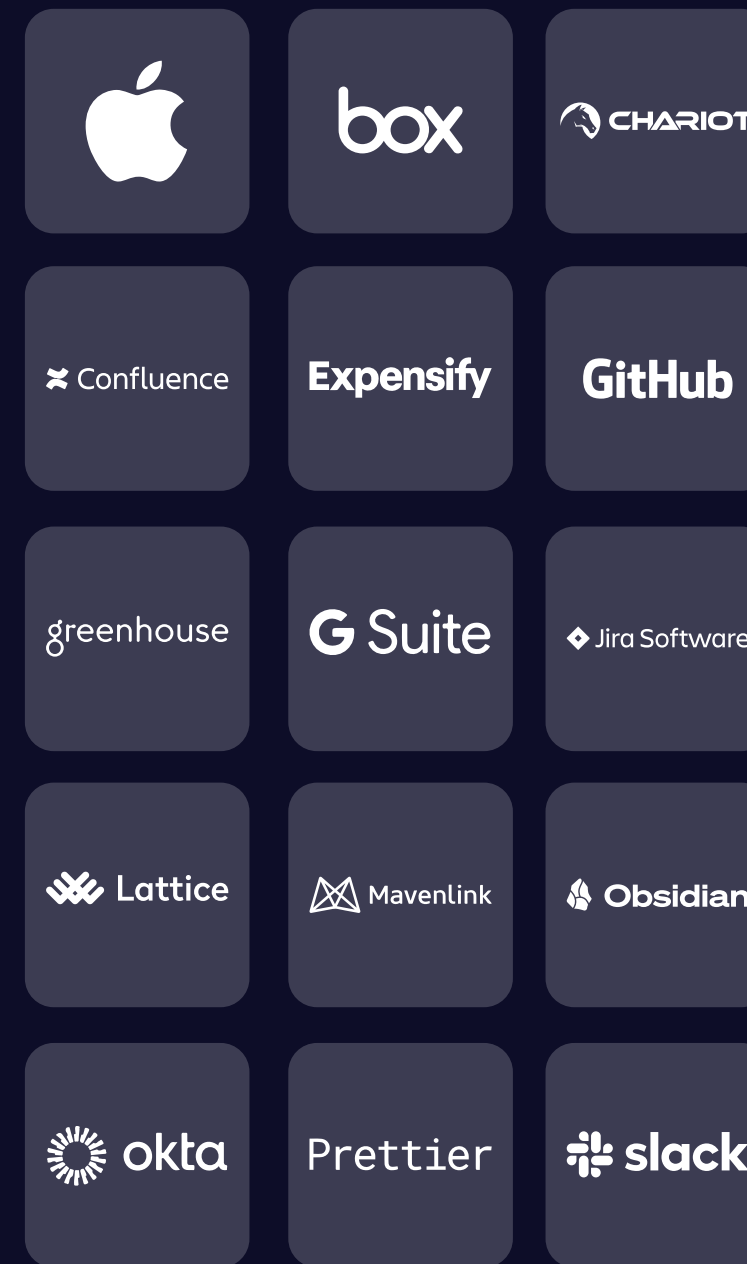


**Across**

- 7. Failure is inevitable, but fortitude will prevail.
- 8. Nothing is impossible.
- 10. By eliminating the material risk you...
- 11. How do you save code changes to a source control management system in an engineering-first culture?
- 12. Sniffs out secrets.
- 13. This is a small company trying to do big things. Every individual effort counts.
- 15. Makes Praetorian more secure and sends unintentional and unintelligible Slack messages.
- 16. Bias toward brutal truth over hypocritical politeness.
- 17. To solve the cybersecurity problem.
- 18. Name of the service that Praetorian uses for its Wiki.

**Down**

- 1. Gotta Catch `Em All.
- 2. Lord of the Rings character who inspired Praetorian's favorite party emoji.
- 3. Similar to the Latin word tiger and a common Slack channel name.
- 4. Most advanced Offensive Security Platform on the planet.
- 5. What category does Chariot sit within?
- 6. Everything we do, we do as a team.
- 9. To make the world a safer and more secure place.
- 11. Whose philanthropy system does the CEO follow?
- 14. Find success and meaning through impact.



# Tech Stack Essentials

Get familiar with these tools and 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.



# Your Assembly Test

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 low-level. During your first day at Praetorian, you will select a LEGO set and get to work.

## Your First Assembly Challenge

Crafting Connections One Brick at a Time at Praetorian



by **Michelle Rhodes**

At Praetorian, we embrace the power of 10x—driving tenfold results through relentless effort, innovation, and execution, all while having a bit of fun along the way. During your first week at Praetorian, every new hire, regardless of their role, embarks on a unique challenge: building a LEGO set. But this isn’t just a LEGO set—it’s your introduction to our culture of continuous self-improvement and unyielding pursuit of excellence.

Our tradition of the assembly challenge starts even before you’re officially part of the team. During the interview process, our engineer candidates tackle an “assembly challenge” designed to test their lowlevel programming skills. This technical assessment ensures our hires possess not only essential skills, but also the ability to solve complex problems creatively and effectively.

Once you’re part of the team, the assembly challenge shifts to the symbolic LEGO build. This playful yet meaningful activity reflects our commitment to building strong foundations and continuous growth. It’s a hands-on way to welcome you into the Praetorian culture, where each brick represents our values, mission, and the innovative spirit that defines who we are.



### The Tradition of Building Together

Throughout the years, each new hire orientation group has spent their first week constructing a large LEGO set together. This unique tradition, known as the First Assembly Challenge, ignites creativity, teamwork, and a sense of triumph. As you strolled through our Austin office prior to being fully remote, you encountered around 50 completed LEGO sets, each narrating its own story.

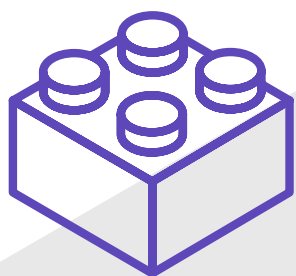
These sets embody growth, camaraderie, and the journey of our employees. They are more than just LEGOs—they are a testament to our company's transformation from a one-person operation, run by our CEO, to a global team spread across 11 countries with a worldwide footprint.

### Adapting to a Remote World

With the transition to remote work, we've preserved this cherished tradition. Now, every new hire receives a LEGO set, and we host a virtual assembly challenge via Google Meet. This allows everyone in the company to join in, extend greetings, and partake in the experience. It's a way to bring our remote team together, fostering the same spirit of unity and creativity that has always been at the heart of Praetorian.

### A Custom Touch

Today, we're thrilled to introduce our very own custom Praetorian LEGO set. This exclusive set is more than just a collection of bricks—it symbolizes our commitment to innovation and the enduring bonds within our Praetorian family. As you assemble your set, we hope you feel connected to our rich history and vibrant future. Each brick reflects our value of making craters by creating impact through our mission, and serves as a reminder to follow your passion in everything you do. This tradition is part of our legacy and a staple of our orientation process, embodying the foundation Praetorian is built upon.



**These sets embody growth, camaraderie, and the journey of our employees. They are more than just LEGOs—they are a testament to our company's transformation.**

### Once a Praetorian, Always a Praetorian

Our First Assembly Challenge is a tradition that honors our past, while paving the way for new beginnings. It's a way to welcome new members into our family and remind us all of the innovative spirit that drives us forward. At Praetorian, every brick you touch is a piece of our collective journey. Once a Praetorian, always a Praetorian.



# Praetorian Leadership

Write the letter from the description under the person you think it matches. Each member has listed 3 fun facts about themselves for you to learn more about them, as well as help you solve this puzzle!



**Charlie Gelatt**  
VP OF OPERATIONS



**Fahim T**  
VP OF FINANCE



**Juan Bocanegra**  
VP OF SERVICES



**Kabir Mulchandani**  
MANAGING DIRECTOR



**Michael Jordan**  
DIRECTOR OF IT



**Michelle Rhodes**  
DIRECTOR OF PEOPLE OPS



**Nathan Sportsman**  
CHIEF EXECUTIVE OFFICER



**Peter Kwan**  
VP OF ENGINEERING



**Taylor Pierce**  
VP OF SALES



**Thomas Reburn**  
VP OF MANAGED SERVICES

## A

- ✔ I love to travel and have visited 29 US states & 24 other countries
- ✔ I used to be a singer and have recorded on several albums
- ✔ I recently decided to start playing ice hockey (after not skating for 20 years)

## B

- ✔ I am a twin
- ✔ I'm a DIY enthusiast and power tool pro
- ✔ A passionate waterskier

## 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

- ✔ 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

## E

- ✔ I was an extra in the movie Spy Kids
- ✔ I enjoy rock climbing
- ✔ I enjoy cooking

## F

- ✔ Allergic to cats. Also, has 4 Siberian cats
- ✔ Was an extra in a football movie starring James Van Der Beek
- ✔ Was in both band and orchestra growing up

## G

- ✔ I have traveled to over 20 countries
- ✔ My set of twins are in college
- ✔ I am a Certified Public Accountant (CPA)

## H

- ✔ I have face-to-face angered every Apple CEO since Scully, not including Tim Cook and was never fired
- ✔ I have met Tom Selleck & Tom Clancy in person at the same time and have photographic evidence
- ✔ I am secretly a furniture maker at heart

## I

- ✔ 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

## J

- ✔ I nerd out on classical music
- ✔ I coach robotics
- ✔ I am still struggling with third person singular in my verbs

## Answers

- J - Peter Kwan
- I - Juan Bocanegra
- H - Michael Jordan
- G - Kabir Mulchandani
- F - Fahim T
- E - Thomas Reburn
- D - Taylor Pierce
- C - Nathan Sportsman
- B - Michelle Rhodes
- A - Charlie Gelatt

# Over the Years



Fahim T Joins as VP of Finance



Thomas Reburn VP of Managed Services



Kabir Mulchandani Managing Director



Michelle Rhodes Director of People Ops



Largest Year in Hiring: 53 New Employees



Largest Contract: \$3,585,000



Log4j Vulnerability



Michael Jordan Director of IT



Release: Chariot, the Most Advanced Attack Managed Service



Release: Nosey Parker, an AI-Based Secret Scanner



Named to Inc.'s Best Workplaces List



Juan Bocanegra VP of Services



Peter Kwan VP of Engineering



Charlie Gelatt VP of Operations

2022

2023



Release: Snowcat, the First Security Scanner for Istio



Release: GoKart, a Smarter Go Security Scanner



Named on Inc. 5000 Fastest Growing Private Companies



Michael Jordan Director of IT



Released Trident, a Password Spraying Emulation Tool



Named on Inc. 5000 Fastest Growing Private Companies



100th Employee Hired



Praetorian Becomes Remote-First



Named to Inc.'s Best Workplaces List



Cam Martin Board of Directors

2021



Named on Inc. 5000 Fastest Growing Private Companies



Named on Inc. 5000 Fastest Growing Private Companies



Joined the Industrial Internet Consortium (IIC)



First Year of \$10M Sales



Named to Inc.'s Best Workplaces List



Named on Inc. 5000 Fastest Growing Private Companies



Released Metasploit Automation of MITRE ATT&CK TTPs



Named to Inc.'s Best Workplaces List



Named on Inc. 5000 Fastest Growing Private Companies



Series A Funding with McKinsey Partnership

2018

2019

2020



Release: Advanced Persistent Threat (APT) & IoT Testing



Named on Inc. 5000 Fastest Growing Private Companies



Longest Serving FTE Joined



Named on Inc. 5000 Fastest Growing Private Companies



First 1M Quarter



Named on Inc. 5000 Fastest Growing Private Companies



HQ Moves to Downtown Austin



Introduces ROTA Tech Challenge



First Customer



Praetorian Founded

2017

2016

2015

2014

2013

2010





In a rapidly evolving world, staying ahead means continually expanding your knowledge. This curated collection of must-read books offers insights into leadership, innovation, and the cutting edge of cybersecurity. Whether you're facing complex challenges or seeking to spark new ideas, these reads will equip you with the tools to excel. From strategic thinking to navigating the future of technology, these books provide the inspiration and expertise needed to drive your next breakthrough.

**HACKER LORE**

**Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell**  
Phil Lapsley

**Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World**  
Joseph Menn

**This Is How They Tell Me the World Ends: The Cyberweapons Arms Race**  
Nicole Perlroth

**Cyberpunk: Outlaws and Hackers on the Computer Frontier**  
Katie Hafner & John Markoff

**Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon**  
Kim Zetter

**Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers**  
Andy Greenberg

# Recommended Reading



**The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage**

Clifford Stoll

**Where Wizards Stay Up Late: The Origins of the Internet**

Katie Hafner & Matthew Lyon

**The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats**

Richard A. Clarke & Robert K. Knake

**Hacker Crackdown: Law and Disorder on the Electronic Frontier**

Bruce Sterling

**Masters of Deception: The Gang That Ruled Cyberspace**

Michelle Slatalla & Joshua Quittner

**TECHNICAL READING**

**The Web Application Hacker's Handbook**

Dafydd Stuttard & Marcus Pinto

**The Art of Software Security Assessment**

Mark Dowd, John McDonald, & Justin Schuh

**Hands-On Go Programming**

Suraj Patil

**A Burglar's Guide to the City**

Geoff Manaugh

**UNIX and Linux System Administration Handbook**

Evi Nemeth, Garth Snyder, Trent Hein, & Ben Whaley

**The Tangled Web: A Guide to Securing Modern Web Applications**

Michal Zalewski

**Testing and Securing Deployments**

Various Authors

**Windows Security Internals**

Mark E. Russinovich, David A. Solomon, & Alex Ionescu

**The Hacker Playbook**

Peter Kim

**How to Hack Like a Ghost**

Sparc Flow

**Arch Linux Wiki**

Community Maintained

**PODCASTS**

**Where Warlocks Stay Up Late**

Nathan Sportsman

**Security Now**

Steve Gibson & Leo Laporte

**Malicious Life**

Ran Levi & Cybereason

**Command Line Heroes**

Saron Yitbarek

**CyberWire Daily**

Dave Bittner

**Risky.Biz**

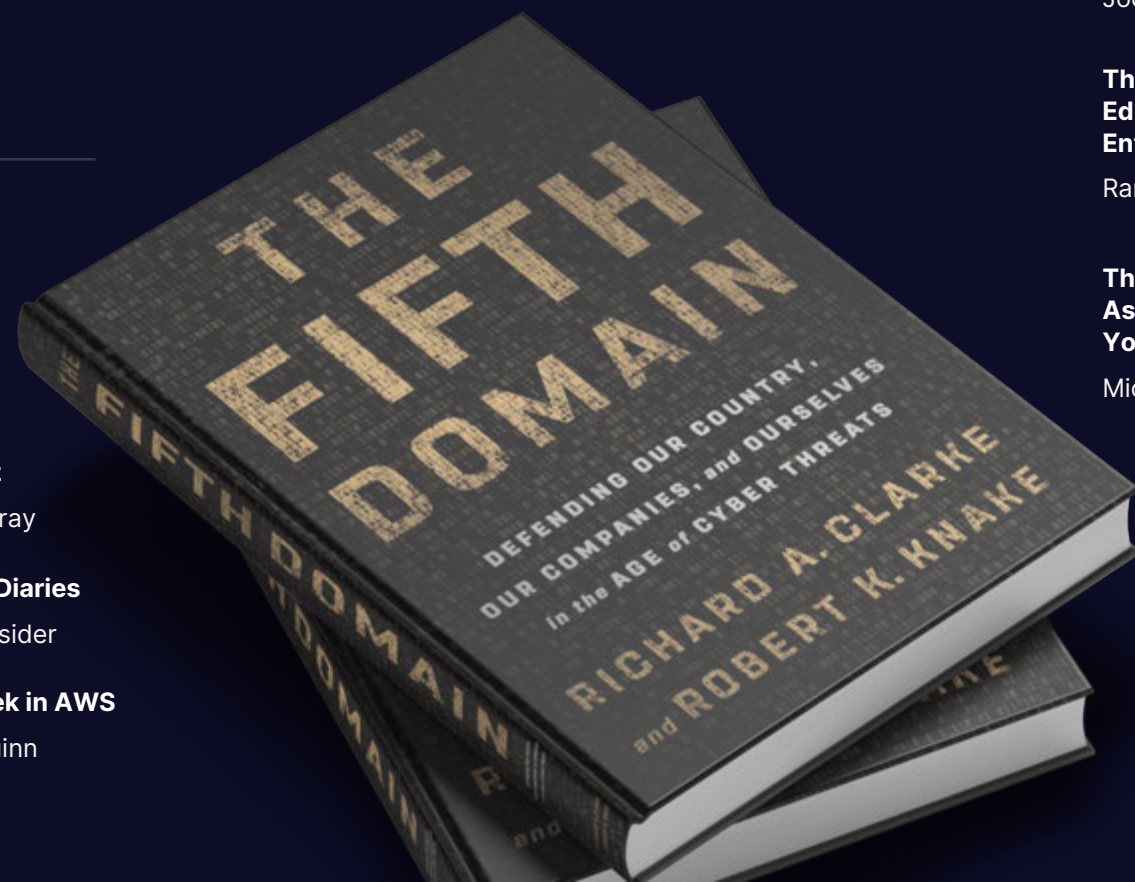
Patrick Gray

**Darknet Diaries**

Jack Rhysider

**Last Week in AWS**

Corey Quinn



**TRANSFORMATIVE**

**Creativity, Inc.**

Ed Catmull

**High Output Management**

Andrew S. Grove

**Radical Focus**

Christina Wodtke

**First, Break All the Rules**

Marcus Buckingham & Curt Coffman

**The Hard Thing About Hard Things**

Ben Horowitz

**Only the Paranoid Survive**

Andrew S. Grove

**Principles**

Ray Dalio

**Zero to One**

Peter Thiel

**Extreme Ownership: How U.S. Navy SEALs Lead & Win**

Jocko Willink

**The Monk and the Riddle: The Education of a Silicon Valley Entrepreneur**

Randy Komisar

**The Coaching Habit: Say Less, Ask More & Change the Way You Lead Forever**

Michael Bungay Stanier

**Work Rules!**

Laszlo Bock

**A Leader's Guide to Cybersecurity**

Thomas J. Parenty & Jack J. Domet

**A Message to Garcia**

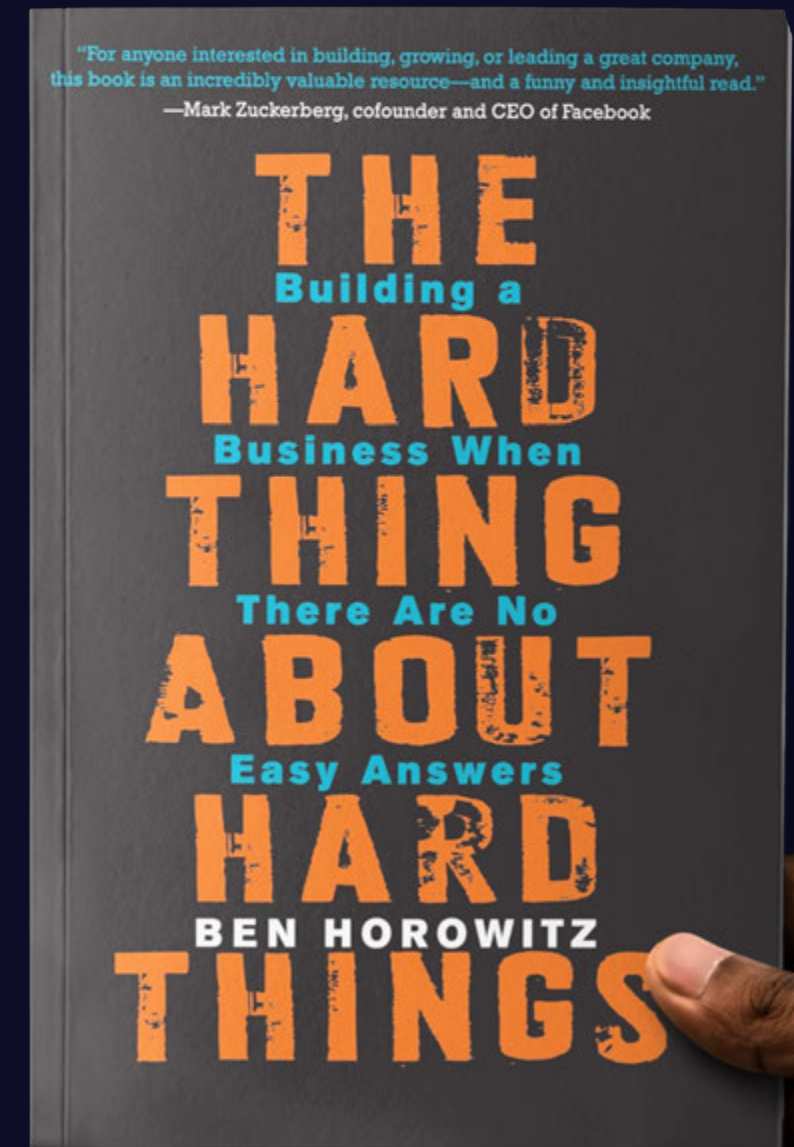
Elbert Hubbard

**The Five Dysfunctions of a Team**

Patrick Lencioni

**Thinking, Fast and Slow**

Daniel Kahneman





# Where Warlocks Stay Up Late

The Origins of Cybersecurity



## Mission

“Where Warlocks Stay Up Late” (WWSUL) is an interview series dedicated to documenting the history of cybersecurity. Inspired by the seminal book “Where Wizards Stay Up Late: The Origins of the Internet,” this interview series aims to capture the stories, insights, and legacies of the pioneering figures who shaped the field of cybersecurity, from its inception to the present day.

## Purpose & Vision

Our mission is to create a definitive oral history of cybersecurity by delving deep into the experiences and contributions of the visionaries who were instrumental in its development. This series will provide a platform for these trailblazers to share their personal stories, challenges, triumphs, and the indelible impact they have made on the digital world.



## Interview Format

The WWSUL interview series will follow a general structure that helps to extract deep insights and personal stories from the interviewees. Regardless of how well I know the guest, the guest should assume I know nothing and be as descriptive as possible because the guest’s life and story is important for documenting the history of the Internet, cybersecurity, and national security.



Stay  
Connected

[wherewarlocksstayuplate.com](http://wherewarlocksstayuplate.com)





**praetorian**