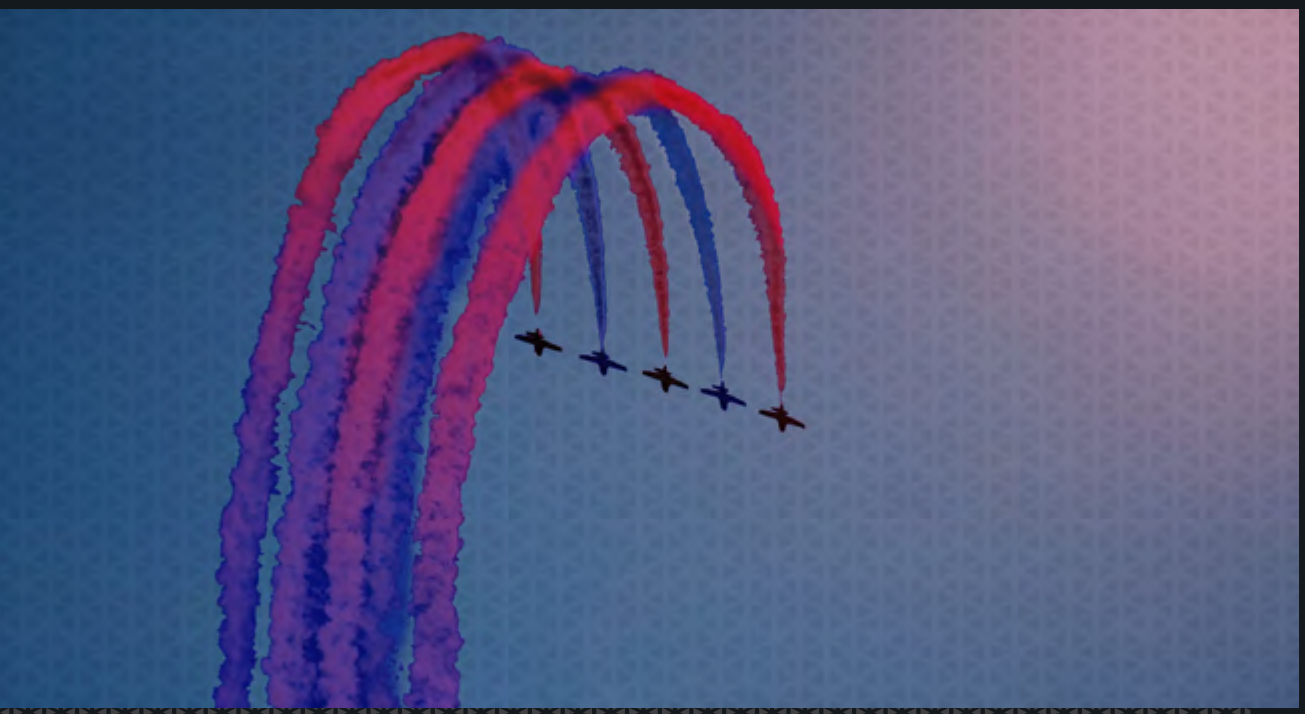
HORIZON3.ai

~~TRUST~~ BUT VERIFY

WHITEPAPER

High Performance Purple Teams



Power of Purple

 @Horizon3ai info@horizon3.ai www.horizon3.ai

"An informed public is a resilient public."[i]

Silos don't yield. Whether you're referring to organizational silos or siloed applications, each operates independently and avoids sharing information. Most are born out of an immediate need, then in order to survive perpetuate an enduring need for their niche product. Their goals can always be circumstantially tied to a higher organizational intent, but rarely directly support a higher purpose.

9/11 painted a vivid picture on just how siloed our law enforcement and investigative institutions were across local, county, state, and federal lines. As a country, we like to believe we have learned and grown, in those respective siloes… yet with uniquely worded authorities used to maintain primacy and exclude intrusion, silos endure. Authorities intended to create order and limit spending sprawl continue to restrict insights and limit outcomes for our nation.

More recently, our 2016 General Elections vividly illustrated just how siloed our public institution responsibilities were with respect to democratic election security. What was initially viewed as a National Committee's poor cybersecurity practices and Big Tech's social media influence extrapolated and resolved to reveal a malicious nation-state campaign. Once again, collaboration became a key tenet and Cross-Functional Teams emerged as an extremely popular placative option in Washington, DC. However, a few leaders understood the larger organizational purpose. New authorities were delegated, and a few leaned into the 2018 Midterms with more than policy, but also action. No longer was foreign meddling one organization's indicators and another's warnings — **it was a threat to us all.**

A whole-of-government partnership was needed, and the Russia Small Group was formed. Departments, Agencies, Commands and Allies broke down a few precious cyber silos and came together to achieve and accomplish more than any could if left to their own vices and authorities.

Unified offense and defense, Red and Blue, interagency and joint teams that previously knew of one another were now enabling and informing one another, creating not only a sustainable loop but a momentum-gathering dynamo that dissuaded would-be detractors and encouraged allies to link elbows and join our fight.

There were growing pains, mostly with traditional agendas and egos, but when a leader puts their lieutenants in a headlock and makes clear the goals and the stakes — the first seedlings of action and trust take hold, and when combined with highly skilled and competent people, gain new insights and start to realize new possibilities.

And you can't imagine going back...

Feeling Blue

... And some can't envision how to move forward.

Silos are far from unique to government. From board rooms to server rooms, sacred cows emerge and endure. Practices and tools that got you here are relied upon to get you there. In our own cybersecurity communities, we have favorite tools and practices and rely on them wholeheartedly. They provide us metrics we reuse to justify their — and our own — existence. While fears of disruption from cyber-attacks continue to rise, C-Suites cross their fingers and hope for the best. CISOs justify a growing spend, equate risk offsets with ROI, while faith in teams and technology continues to drop.

> When asked how organizations evaluate cybersecurity technology efficacy, **none of the 100+ interviewees referred to a common definition of efficacy.**

Private companies are recognizing that as their footprint turns more and more digital, resiliency of a growing digital attack surface is a greater challenge than ever. In light of the recent pervasive supply chain attack, escalating ransomware attacks, and legitimate credential attacks on the rise, it feels like attackers are succeeding while detection and protection tools are failing.

Where companies and governments see threats, nation states and transnational criminals alike see opportunity. This isn't a tech problem; this is a threat to us all.

Bottom Line: the same old defense strategies are not working, while attacker tactics are. Professionals and practitioners alike are starting to echo "If you can't beat them, join them."

Cybercrime is expected to cost the world $10.5 trillion by 2025, making it the third largest economy after the U.S. and China.

Seeing Red

One of the most frustrating aspects of a hack is that it feels like an attacker knew more about your network than you did.

We spend millions in malware signature detection and sandbox execution, endpoint detection, threat indicators, vulnerability assessments and scans, proxies and firewalls… and still they got in. Same goes for a Red Team operation or a penetration test.

Simply put, a hacker avoids your strengths and exploits your weaknesses. An attacker probes your environment to see where your defenses are focused, and where they aren't. Blue is usually focused on endpoints, so Red focuses on attack vectors. Red maneuvers, while Blue watches. And there is a LOT to watch.

Addressing this threat, and in an attempt to more fully assess their security posture, companies are calling on the services and perspective of Red Teams and pentesters more:

- A 2020 survey found 92% (up 20% from 2019) of companies are performing red team exercises and 96% are performing purple team exercises, citing the importance of information sharing.
- While up to 42% of organizations may claim in-house penetration testing teams, less than 8% of organizations operate their own Red Teams, choosing to use external firms.

The evidence is clear: companies want to "turn the map around" and see what an attacker sees. If ignorance is bliss, insights are invaluable... until you are faced with paying a professional services bill.

Right now, a lot of professionals are thinking the same thing: I have a problem causing me pain. I need a solution that alleviates my pain. What is the cheapest, quickest and easiest way to do that?

Cybersecurity solutions are rarely painless. Cheap, quick, and easy are in the eye of the CFO, COO, and CISO beholders. Are Red Teams at the top of your list? Red Teams and Penetration Testers are rarely cheap, quick, or easy, hired as consultants, professional services, or stood up in-house.

CHEAP

Offensive-skilled talent is wide and varied, and often associated with hefty salaries. Externally hired professional services and consultants increase costs. Certifications are expensive, and staying relevant requires dedication and skillset proof. Coverage is usually specific to a target or vulnerability, so coverage is minimum, thus driving cost to premium.

QUICK

Audits and exercises require coordination and scheduling — often weeks ahead to dedicate a team, decide on target and exercise criteria, perform probing and reconnaissance, execute operations, and have additional time for producing a comprehensive final report. Rarely frequent, their findings tend to hemorrhage value quickly.

EASY

Working around risk pitches, board skepticism, annual budgets, business operations, development schedules, release timing, and personnel work schedules to ensure zero interruption to customers... which is why it is often a planned and scheduled “exercise” where security, information technology, and infrastructure teams are the ones interrupted.

And perhaps most painfully of all: Red wants to demonstrate value. They were hired to hack and exploit, and how do they accomplish their goal while showing purchasers their money was well spent? By pwning you. Blue wins by stopping Red and proving their value to their leadership, while Red wins by beating Blue, or worse, by embarrassing them.

We now have two separate teams with varying perspectives and differing goals.

A better solution is needed. Better yet... a full-on pivot.

Purple Pivot

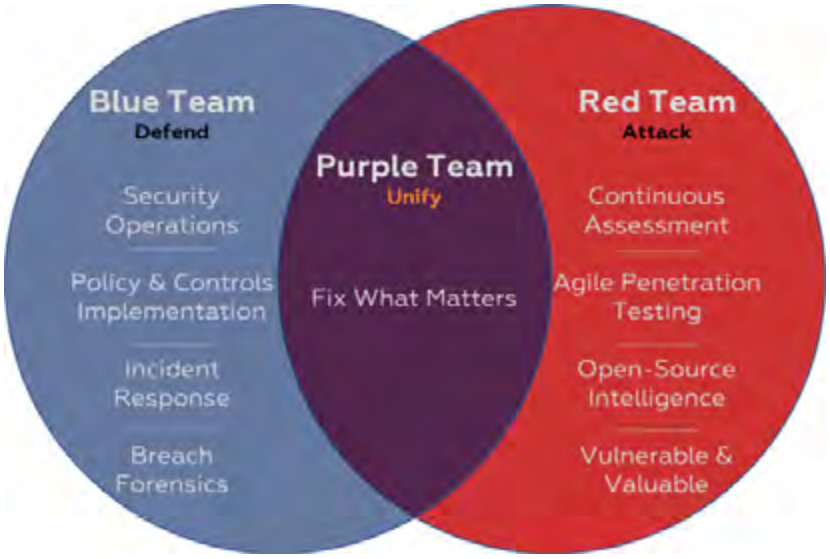
Much like our whole-of-government, organizational leadership is realizing a whole-of-company approach is needed, so leaders are pulling people from across directorates, rethinking their risk environment, and forming teams of rivals.

Seeking to capitalize on diverse perspectives and create stronger, more resilient teams, we're seeing a pivot to Purple Teams across industry. Typically, with a combination of Blue Teams (Defense) and Red Teams (Offense), there is more and more of a commitment within companies to breakdown traditional silos and exercise their defensive cybersecurity capabilities against offensive perspectives.

Competition between teams may give you insights into which team is more capable at achieving their tasks… but creating a common goal and definition of success is critical here to identifying your company's blind spots and gaps in your cybersecurity posture.

Across industry and even in education, "Purple teaming changes the way defenders approach their jobs. It helps them to think more like the adversary. That learning is a game changer because that is what enables them to incorporate new ideas and new tactics." — EDUCAUSE Cybersecurity Program Director, Brian Kelly

The truth of the matter is that Purple Teams exploit the dichotomy that users/defenders have rules,



while attackers don't. Rules intend to mitigate risk, but if an attacker can get around that rule with little risk, then we need to alter our perspective on not only the risk, but the perceived value of the rule. This is why attackers often know more about your environment than you do, and why it's so important to bring this perspective onto your team. A Purple Team perspective can clarify and unify value here and synchronize an organization on what truly matters.

One Note(s)

Purple

Exercise

More often than not, when looking to make a Purple Pivot, most organizations (and professional services selling to them) refer to this as incorporating Purple Team Exercises. We see most organizations focusing entirely too much attention on the two words:

1. **PURPLE:** explaining the roles of Red and Blue was not the focus of this paper, but understanding that traditional segmentation and how it detracts from your intended success is. Combining Red and Blue to make Purple is valuable — always more so than Red versus Blue — but not always as inclusive as it could be. People, processes, and technologies from your development operations and information technology teams will have not only valuable, but also critical insights into how the business operations infrastructure and applications link together. Any organizational entity in the arena will have input and vote into recommended security changes learned. You're better off baking them in, versus bolting them on later.

2. **EXERCISE:** building security operations muscle memory is valuable but can also create a cyclic view on such tests. Traditionally, those cycles are lengthy, static, and value atrophies quickly. Preparation and dedication up to and during scheduled events can perpetuate the illusion of Red and Blue (i.e. still separate). If Red and Blue only come together for such tests, they might as well be summer camp pen pals. Olympic swimming relay teams don't come together every four years… continuous operations with continuous coordination leads to high performance and preparation.

Bottom Line: Team brings home the win. Accelerating that team to perform at a high level is possible.

Into the Breach

> If everyone is thinking alike, then somebody isn't thinking.
>
> — Gen George S. Patton

Once more, we have identified our problem and a potential solution, which is still traditionally wrought with Red pain, enough to detract those who not only desire, but need this kind of solution most. What we need are answers that take a Purple Team from nice-to-have to must-have. Now.

It is these precise design criteria that led Horizon 3 AI to create NodeZero: a world-class cyber attacker, completely autonomous and AI-driven, orchestrating 100s of attacker tools, tactics, and techniques so you can find and fix what matters.

Our own results bear this data out, executing over 600 operations (ops) in a single quarter, more than the largest professional services and consultants with exquisite multi-person teams are conducting annually.

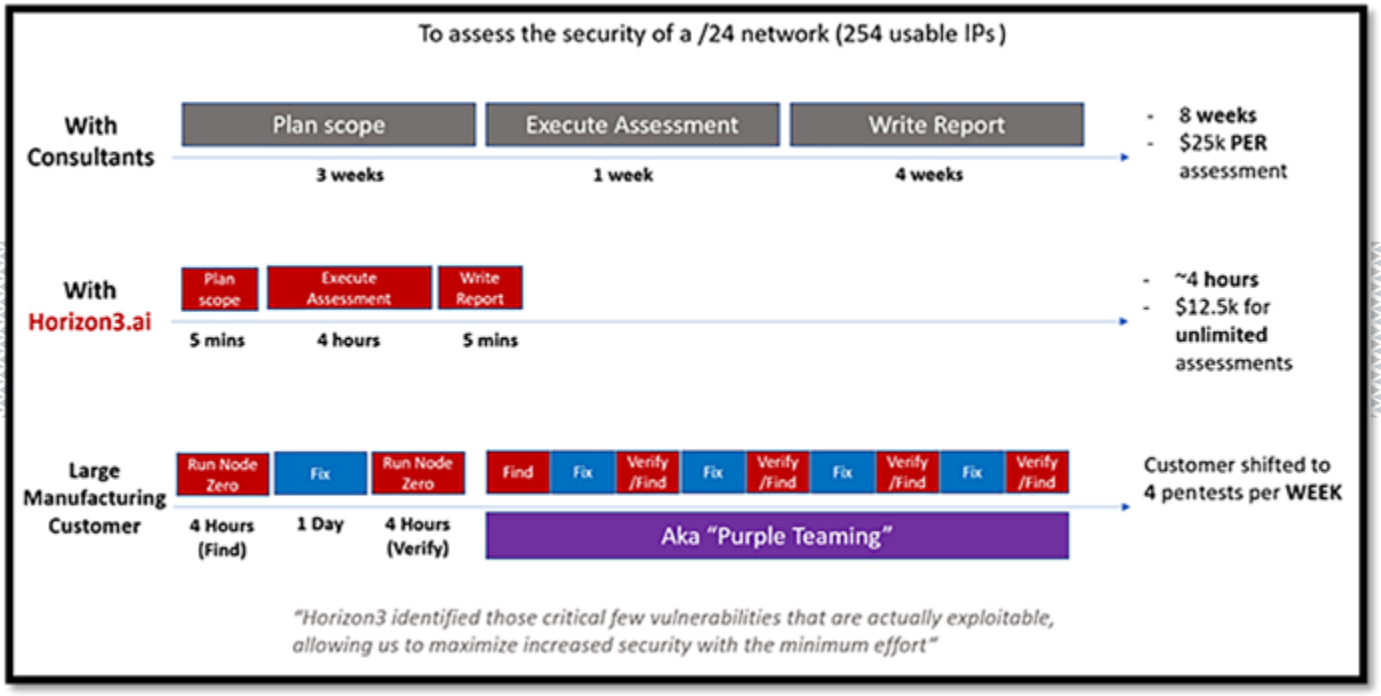
What Matters	Traditional	Needed
Effort	High Coordination	Low Self-Service
Frequency	Annually or Quarterly	Agile & Continuous
Cost	High for Single Op	Low for Unlimited Ops
Speed	Weeks	Hours
Coverage	1-2%	99+%
Expertise	High	Low
Team	External ProServ	Inside Purple Team Partner
Goal	Pwn you to demo value	Decrease risk to company

COMPANY #1 – a global consulting company's Red Team experimented and starting using NodeZero to accelerate their own delivered Time-To-Value. As a traditional 2-3 person Red Team, they'd scope and assess 1-3 /24s and take 6-16 weeks from contract signing to complete.

NodeZero enabled them to run 15 operations in 24 days, assessing 22K+ hosts and finding 3800+ attack vectors. This was 99%+ coverage enabling 4 people to operate like an 80-person Red Team, ultimately saving 600+ man-hours per /24 operation and 1000 man-hours per /16. That's a 50x coverage in 50x less time. That's the potential of autonomous and AI-driven Purple Teaming. **Painless.**

COMPANY #2 – a global manufacturing company's IT technical champion knew they had blind spots, even with no compliance requirements, but couldn't afford more than one penetration test per year. Their attack surface was expanding spanning temperature kiosks and growing IoT footprint. Both agents and an attacker's value were limited.

One year later, they've completed >200 operations spanning 37 datacenters and were running four operations per week, driving their daily standup. This is an example of a Blue Team using NodeZero as a Red Team partner to achieve Purple Team results across their entire enterprise at a scale and speed they could never achieve through professional services or external partner testing and assessments. There are no alerts, only results. **And no silos.**



And you can't imagine going back.

Recommendations

The Power of Purple is enticing, but it's the unified team that wins.

Every CEO and CISO, peer, and practitioner needs to ask and answer:

> Are we unifying and driving our people and our partners towards a painless and powerful cybersecurity posture?

Then verify the answer.
Horizon 3 AI can help.

...because dividing and conquering your own is what an adversary does.

HORIZON3.ai

~~TRUST BUT~~ VERIFY

I. https://www.dhs.gov/news/2019/11/05/joint-statement-doj-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020-elections

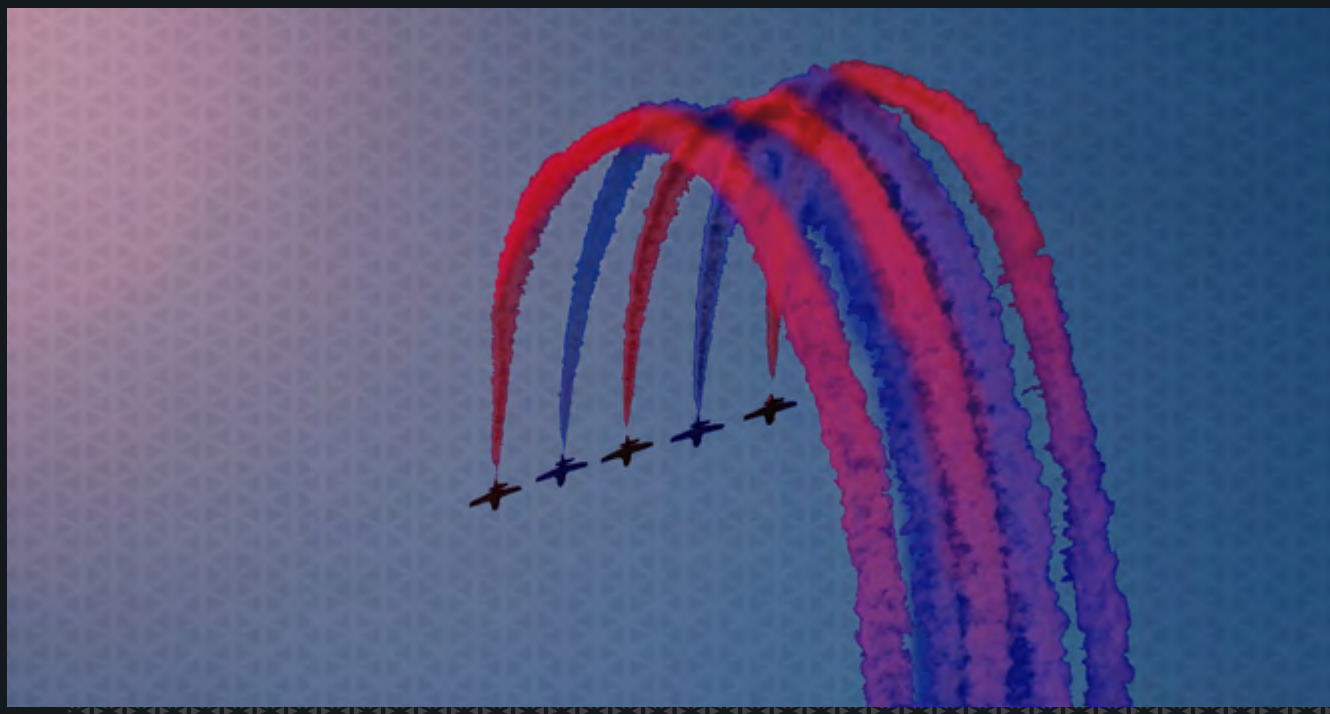
II. https://www.jcs.mil/Media/News/News-Display/Article/1759176/cyber-command-expects-lessons-from-2018-midterms-to-apply-in-2020/

III. https://www.debatesecurity.com/downloads/Cybersecurity-Technology-Efficacy-Research-Report-V1.0.pdf

IV. https://securityboulevard.com/2020/09/the-pandemic-of-credential-based-cyberattacks/

V. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

VI. https://www.exabeam.com/security-operations-center/2020-red-and-blue-team-survey/#:~:text=Our%202020%20survey%20found%2092,and%2027%25%20once%20a%20year



VII. Core Security, "2020 Penetration Testing Report"; a HelpSystems Company; www.coresecurity.com

VIII. https://hbr.org/2015/03/see-your-company-through-the-eyes-of-a-hacker

IX. https://edtechmagazine.com/higher/article/2020/10/why-purple-teams-matter-higher-ed-cybersecurity-perfcon

https://www.certitudesecurity.com/blog/analysis-and-assessments/what-are-red-teams-and-why-conduct-exercises/

https://www.contextis.com/en/blog/top-findings-from-red-team-engagements