info@Horizon3.ai
www.Horizon3.ai
LinkedIn: Horizon3.ai
Twitter: @Horizon3ai

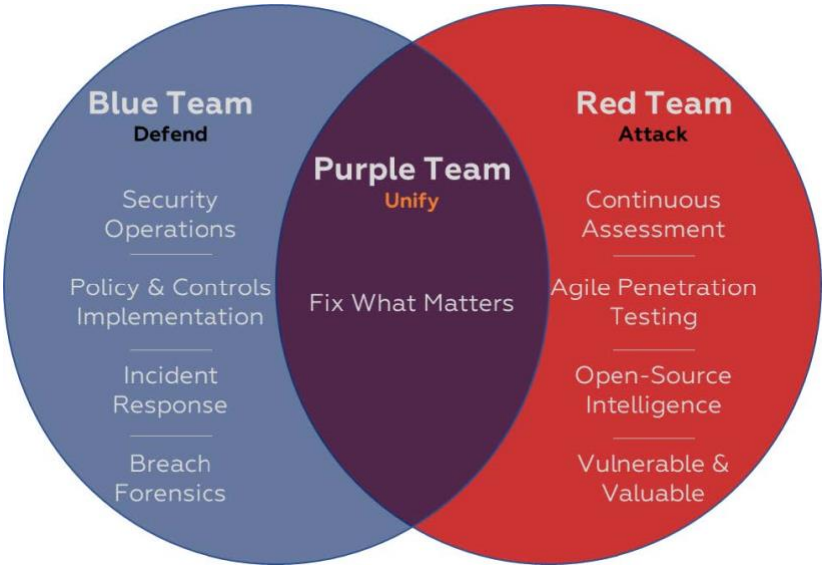
FEELING BLUE?

- Focused on endpoints
- Follow rules, use defined tools
- Blue wins by stopping Red

SEEING RED?

- Focused on attack vectors
- Break all the rules
- Red wins by pwning Blue

BLUE + RED = BETTER



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

"**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[1]

Users/Defenders have rules, **Attackers** don't - **Purple Teaming** fills the void.

Purple Teaming enables you to "turn the map around" and see your enterprise through the eyes of the attacker, enabling you to identify blind spots, ineffective tools, and identity kill chains that attackers can, and will, exploit.[2]

A Purple Team perspective can synchronize an organization on what truly matters.

[1] https://edtechmagazine.com/higher/article/2020/10/why-purple-teams-matter-higher-ed-cybersecurity-perfcon
[2] https://hbr.org/2015/03/see-your-company-through-the-eyes-of-a-hacker

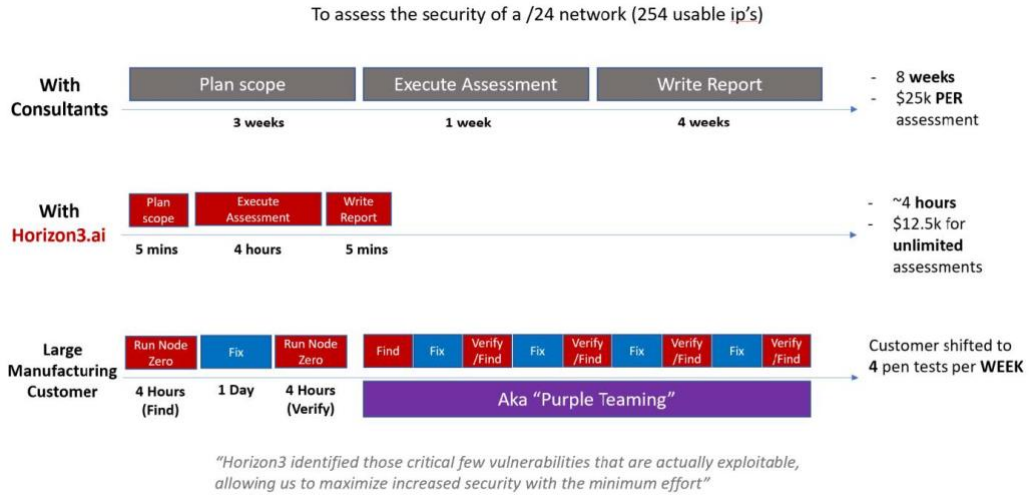
READY TO GO PURPLE?

Traditional blue/red exercises vs. purple teaming…

What Matters	Traditional Approach	BETTER Approach
Effort Required	High (Multi-Team, Coordinated)	Low (Self-Service, On Demand)
Test Frequency	Annual or Quarterly	Agile and Continuous
Total Cost	High for Single Pentest	Low for Unlimited Ops
Time to Value	Weeks to Written Report	Hours to Searchable Results
Coverage	1-2% of Environment	99+% of Environment
Expertise Needed	High to Execute	Low to Execute
Resources	External Professional Services	Internal Purple Team Partner
Ultimate Goal	**Pwn you to demonstrate value**	**Decrease risk to your company**

It is precisely these design principles that led **Horizon 3 AI** to create ***NodeZero***: a world-class, automated cyber attacker, orchestrating hundreds of attacker tools, tactics, and techniques – and adding more every day – so you can **find and fix what matters**. **NOW!**

Our own results bear this data out – executing over 600 operations in a single quarter. That's more than the largest professional services teams are conducting annually!



"Horizon3 identified those critical few vulnerabilities that are actually exploitable, allowing us to maximize increased security with the minimum effort"

Customer Profile: A global manufacturing company's IT technical champion knew they had blind spots – even though there were no compliance issues – but couldn't afford more than one Pen-test per year. Their attack surface was expanding alongside their growing IoT footprint. The value of agents and attackers was limited. Enter **Horizon 3 AI**…

In a matter of months, they've completed more than 80 operations spanning 16 datacenters and are now running four operations per week, driving their daily standup. This is a **Blue Team** using NodeZero as a **Red Team** partner to achieve **Purple Team** results at a **scale** and **speed** across their entire enterprise they could never realize through professional services or external partner testing and assessment. There are no alerts, only results…NO persistent agents, NO scripting and NO silos.