Cat Self

@coolestcatiknow

Red Teams are $$$! Metrics can justify value, but picking the right metrics to drive behavior is tricky.

How do you justify the value a Red Team brings to the table?

Jamie Williams

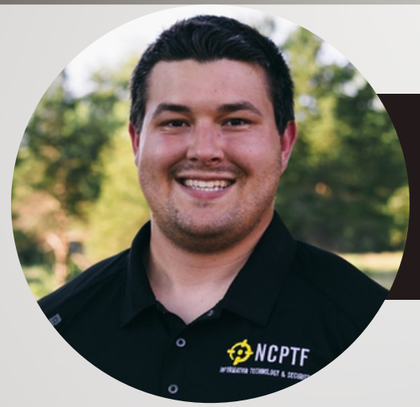
@jamieantisocial

We can measure value by working backwards from where we need to be, ensuring that every step (scoping all the way to reporting) aligns with the desired results.

Niru Ragupathy

@itsC0rg1

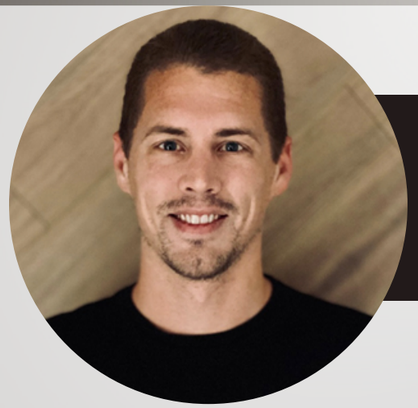
Red teams test security controls and detection capabilities, they identify security issues and wrap it in a nice story aka attack narrative. The attack chain is showcased from start to finish and helps draw attention to the business impact of computer security issues. This helps with executive visibility, driving engagement with product teams and in turn landing remediation.



TJ Null

@TJ_Null

Let’s look at it like it is a forecast. We can analyze the information to measure security improvement over time for an organization. This allows us to define a clear and measurable method by taking red team operations data and using them to show improvement regarding the security posture in an organization.



Andy Grant

@andywgrant

It is about raising awareness and visibility to areas of need. If we need to put a number to that, we can speak to the number of operations performed and the explicit risks they identified or highlighted, but we do not like to over focus on that stuff, as it can create perverse incentives.

Cat Self

@coolestcatiknow

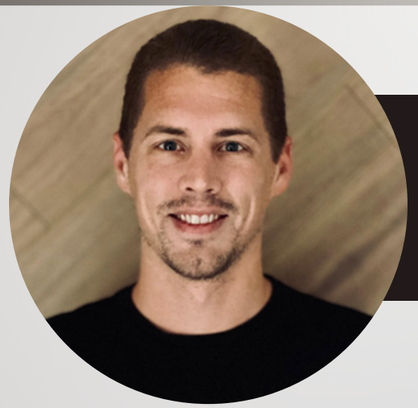
I have been on different teams and run multiple types of exercises, from known, unknown, throwdown to long term operations. But these exercises and teams had to change as the organization matured.

How do exercises or red teams change as the needs of the organization changes?

Niru Ragupathy

@itsC0rg1

We run two types of exercises - one where the attacker profile is rough and we aren't closely emulating TTPs but rather setting a rough scope to define the capability and/or general attacker methodology. For the other, we pick a specific APT group, work with our Threat intel team to research and implement the TTPs as closely as possible.



Andy Grant

@andywgrant

It is always important to remember that no true adversary is going to be static in their patterns and thus your team and operations need to be adaptable. When we want to really focus in on a very specific, minimal TTP set, we do a mini operation we call a Detection Capability Assessment, with the goal focused more on evaluating the explicit protections and response for a small scope.

Jamie Williams

@jamieantisocial

How much the red team aligns (skills, processes, etc.) with the needs of the business (and different customers) - also including the capability to adapt and be flexible as those needs evolve (ex: we brought in this thing, how soon can you assess it?).

Cat Self

@coolestcatiknow

As our Red team got snuck through the cracks, our blue team felt, "I should have caught this!". And the Red vs. Blue had taken root.

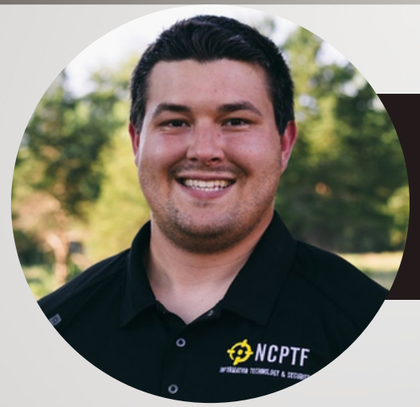
Why do you think it's Red vs. Blue? How can Red prevent this?

Panel: Who doesn't like a little spice? Emulation maturity, team culture, and TTPs.

Jamie Williams

@jamieantisocial

We like to protect ourselves and emphasize our specialities, but need to recognize that we are in this together (same goals). Cross-pollinate and learn the priorities and language of others, so that when they call you actually understand where they are coming from (and can maybe even forecast their needs).



TJ Null

@TJ_Null

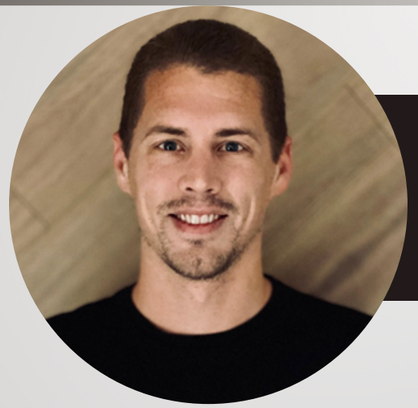
In the past, they have been separate entities but in recent years we have seen an increase with red and blue teams building a strong relationship to support each other. In the end, when we work together our teams make each other better. Red and Blue play an important role to help improve an organization's security posture from today’s sophisticated adversaries.

Niru Ragupathy

@itsC0rg1

It really shouldn't be "Red Vs. Blue" but rather "Red and Blue", at the end of the day we are all working towards the same goal, i.e, improving security. We are fortunate to have a great relationship with our Blue team. If that isn't the case in your organization, then it's up to the Red team to bridge the gap with Blue by understanding the needs of Blue. Our work products - presentations and reports - feature sections by our Detection teams to help drive this home, allowing us to celebrate each other's wins.

We also build relationships with our product teams, specifically for remediation. We have a team of TPMs who specialize in relationship building and supporting remediation of strategic issues. Having a dedicated remediation team helps us reduce context switches when working on exercises. This is a different skillset from breaking things, and hiring people with experience in remediation support is immensely valuable and underappreciated.



Andy Grant

@andywgrant

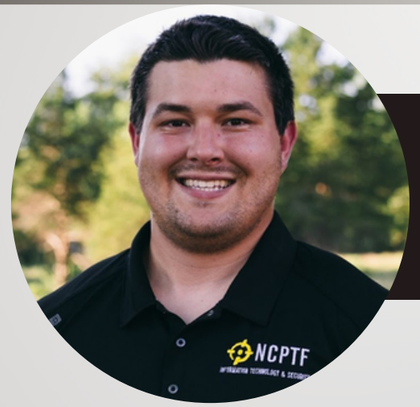
If it wasn’t red vs blue, Purple Teams wouldn’t make sense! I believe in the past teams have been weary of “sharing” details because there was too much ego tied into “winning” the operation, on both sides. How do we change this? Stop being an actual adversary! We are only meant to be emulating one. We need to all accept and act like we are all on the same team. Red is a function of defense a.k.a Blue.

Cat Self

@coolestcatiknow

That feeling of not being good enough, commonly referred to as Imposter syndrome. We all have it or have gone through it. For me, mapping out where I am, where I want to be, then working painstakingly towards it has helped. Also, recognizing that comparison is the thief of joy.

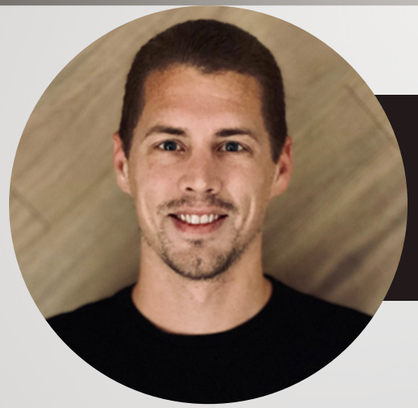
How do you work through that?



TJ Null

@TJ_Null

You have to realize there will always be other people who are going to be accomplishing more things ahead of you and that is okay. Do not set an expectation to be better than others. You should work on finding ways to embrace yourself and the progress that you have accomplished from your past.



Andy Grant

@andywgrant

Very few people go down a path without ever questioning why they are there or whether someone else should be out in front of them. It is okay (and healthy) to have self reflection and questions, but stop letting that get in the way of trying. I mean, come on, we're hackers! When have we ever let anyone tell us what is or isn't possible? Stop letting your inner voice do just that.

Niru Ragupathy

@itsC0rg1

It's easy to start to feel like you can't find the same bugs like your teammates or do the same cool things they do. It's also a lot of learning from scratch, which can be daunting. Icamtuf / Michal Zalewski, gave me great advice on this. He explained that it is important to remind ourselves that the people we look up to in a specific field / topic are usually at the top of their game. We are seeing them at their best, we don't see all the work and time they have put in to get there. So rather than comparing ourselves to others, we should compare ourselves with our past selves and see how we have grown.

Jamie Williams

@jamieantisocial

We are all learning and pushing to get things done. I make mistakes ALL THE TIME but keep working through and trying to grow. We need to respect that everyone is at a different stage of their unique journey, and they just need a healthy balance of space and support.