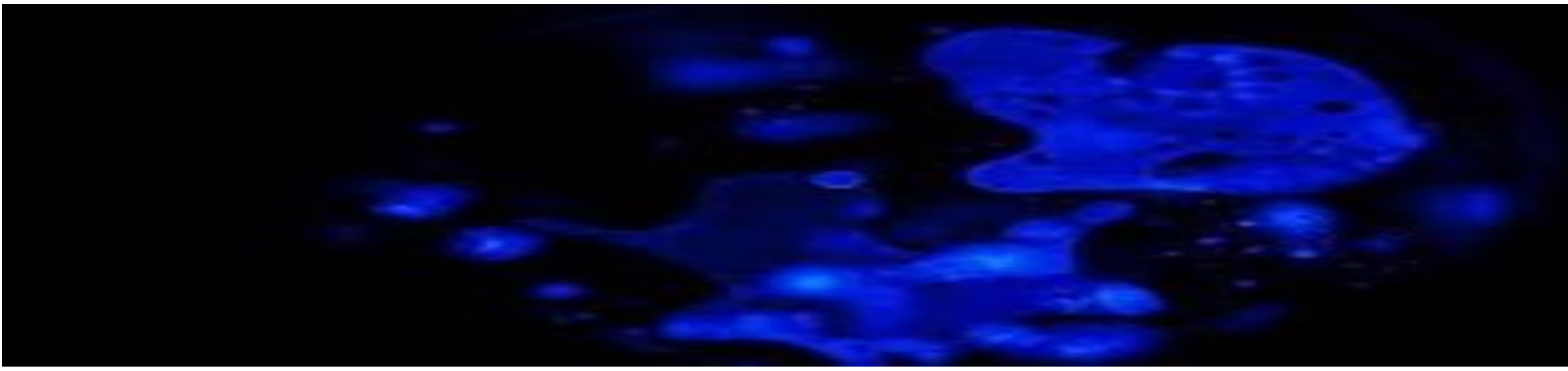


Inquirix

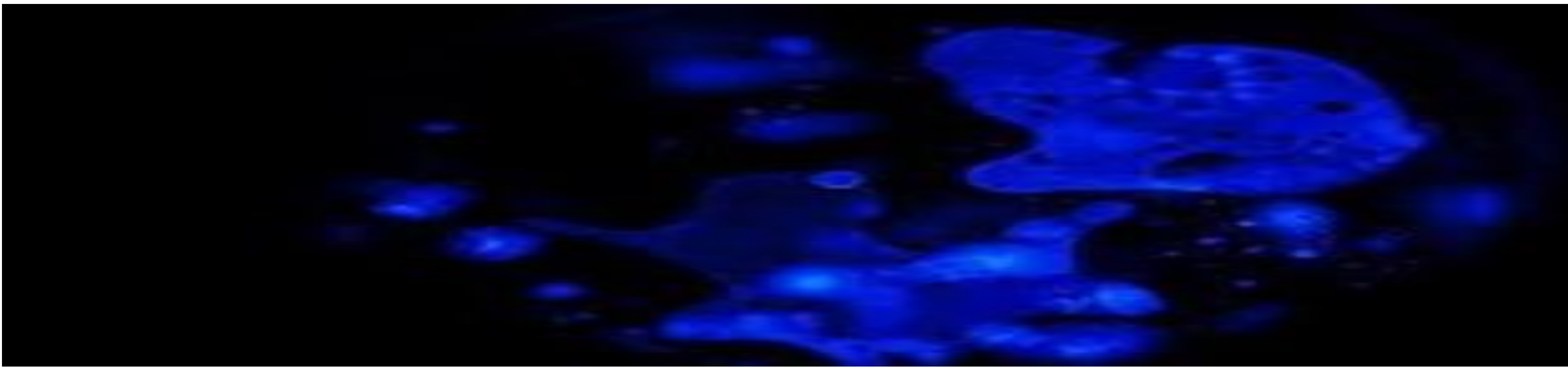
Dark Teaming – Reaching the Parts that Red Teamers Miss

AUTHOR: Abi Waddell

http://www.inquirix.org

VERSION 1.0

May 2022

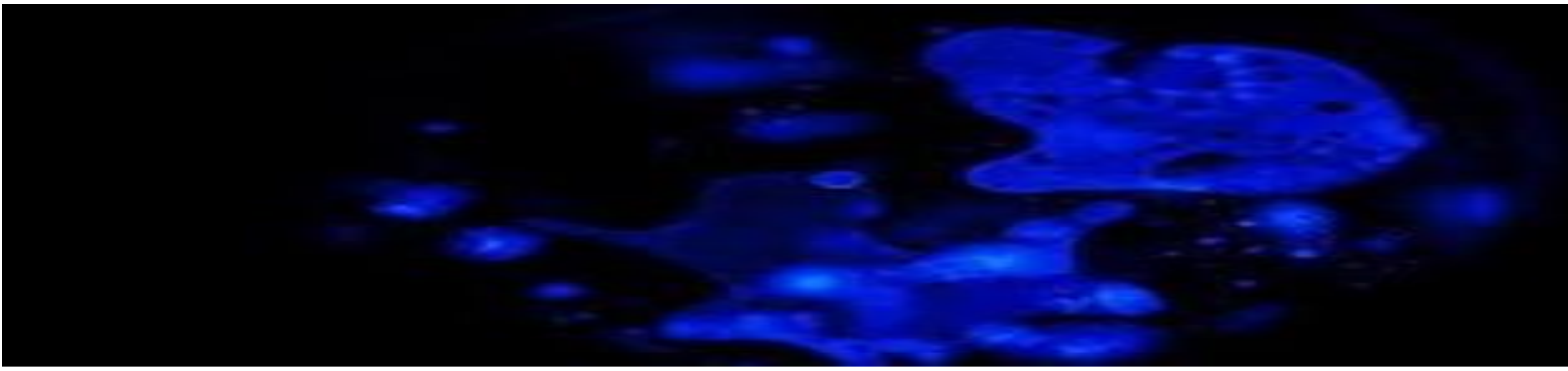


This is about dark teamers and how they can be utilised to get a more complete picture of an organisation’s threat landscape – if organisations are willing to consider it.

So, what is dark teaming? It is a term coined by Inquirix to describe an attacker who is much more focused and motivated to attain their goals, and as a result will be more likely to do this successfully. Dark team attacks run with no legal or corporate constraints and without official authority, but with benign motives such as preventing and detecting crime or researching new security vulnerabilities. Dark teaming removes all the constraints of red teaming but cannot have many of their activities `authorised’ by organisations. Their activities however do provide a much better picture of an organisation's security weaknesses.

This document describes the types of dark teamer, the advantages of dark over red teaming, dark team attack characteristics, where to find them and how to capitalise on their drivers, some famous examples in the recent past and how such benign cyber attackers should be treated more leniently than other types of cyber-criminal, with current cyber-crime laws being changed to accommodate these individuals.

What are the main characteristics and differences between red and dark teamers? Red teamers are not usually tasked with assessing the number of ways a target can be breached, the primary aim is to



get a high level of access on one or some of the internal corporate systems and to demonstrate some form of call back or exfiltration to an external server. This is especially so as they will normally be limited by the constraints of the expected testing time window. Dark teamers do not usually have an externally defined time window and can explore more of the ways a target can be breached.

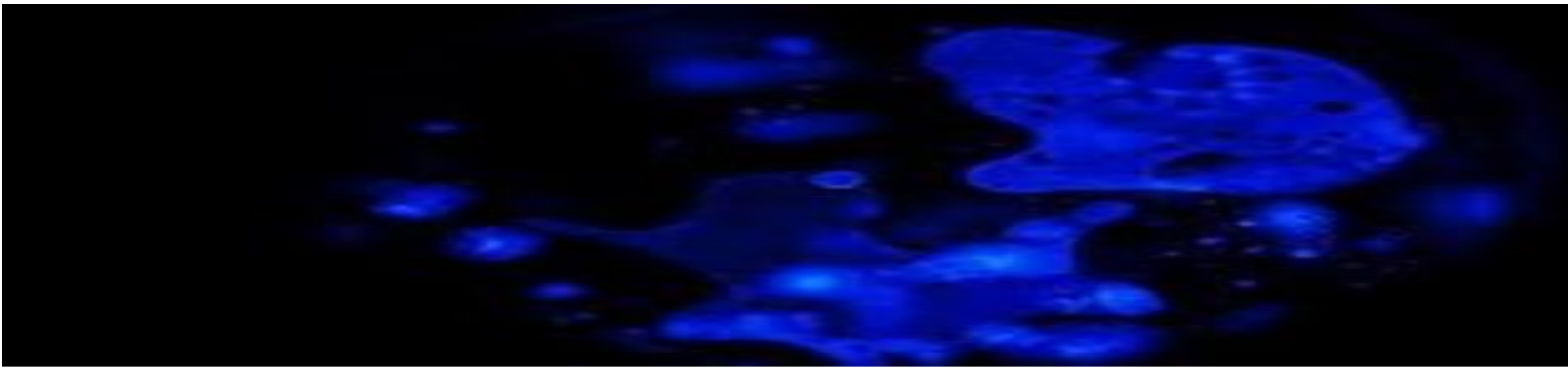
Red teamers are likely to have their IP addresses whitelisted during the test engagement which doesn't give a true reflection on what an attacker can see or do. And in most circumstances, a dark teamer has no special provision made for them.

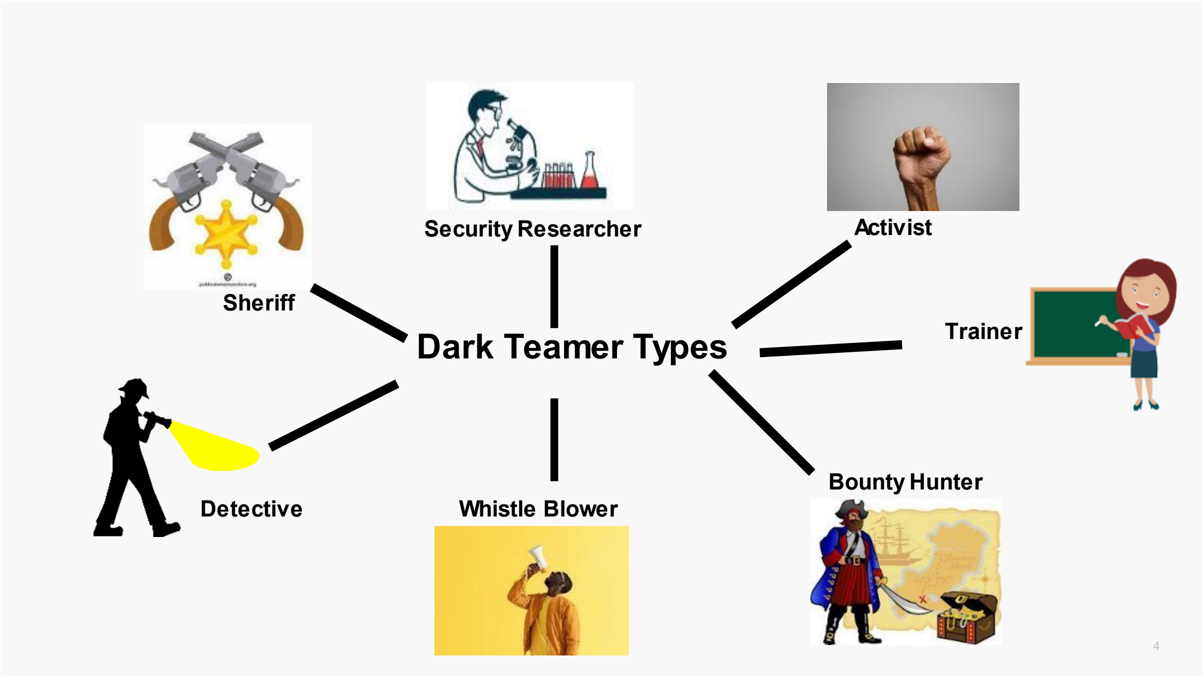
With red teamers, as mentioned, their test time window is usually short (a few days or weeks) which cuts down the time being spent on say the recon stage. They are likely to have some activities curtailed such as full malware or credential exploitation and post attack persistence. Dark teamers will be free to spend a much longer time planning and carrying out an attack, and post-attack activities.

Red teamers will usually have less time to develop zero-day exploits which may have a higher chance of success breaching the security defences, whereas dark teamers, who usually have a higher degree of motivation to breach the company, will put in more research into how this can be done.

Red teamers have to abide by their own and that of the target companies' code of practice and ethics and also the scope of the test as set out in the beginning. Dark teamers do not have these constraints.

Lastly, red teamers are treated as a corporate entity who are told to assess the target environment's security, and in return they will carry on getting their monthly pay cheque and meet their corporate sales and ongoing business targets. The individuals who make up the red team may be selected based on their particular field of expertise and knowledge. Dark teamers, however, do what they do best as this closely aligns with their drivers and their particular incentives – more on this to follow.





Dark Teamer Types

Sheriff

Security Researcher

Activist

Trainer

Detective

Whistle Blower

Bounty Hunter

4

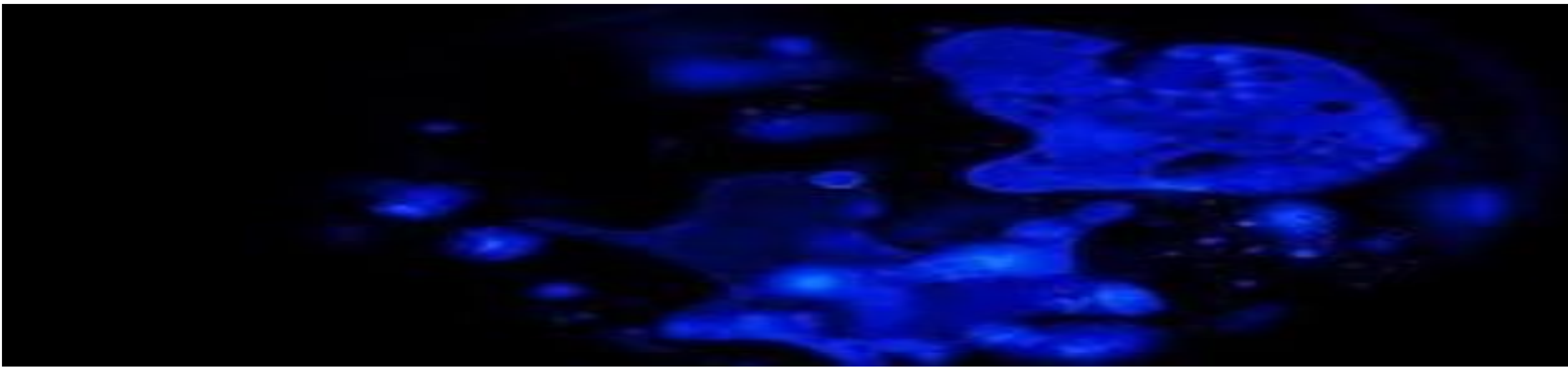
The types of dark teamer can largely be put into these 7 categories:

The **Sheriff** will want to actively police and stop crime – examples include issuing take down notices, causing a denial of service of sites offering illegal products and services, warning others about such sites or criminal suspects, offering methods and services to neutralise malware, and monitoring specific sites or users for illegal activity.

The **Security Researcher** is primarily interested in making discoveries of new vulnerabilities and security techniques to increase our understanding of technology, to indulge a general love of experimentation and discovery for its own sake and to help companies and users improve their security posture. Examples include discovering and exploiting new flaws in software, testing hypotheses around previously established assumptions, for instance encryption standards, and developing tools to mitigate known vulnerabilities. Sometimes this involves pushing the bounds of acceptable cyber usage practices, for instance, it might be that in order to discover a flaw in the two-factor authentication of an email account, the account needs to firstly be breached with the username and password.

The **Activist** or hacktivist will seek to further a particular cause (such as political, religious or ethical) by actively disrupting the services or reputation of the opposing side or using illegal cyber-attack methods to promote their cause. An example is publicising negative news about the opposing cause using illegally obtained material, website defacements and denial of service.

The **Trainer** wants to use true to life technical environments to demonstrate specific IT methods and practices. The reasons for this could be lack of time and resources to create their own environments or because there is no realistic way of creating an artificial replica of what they want to demonstrate,



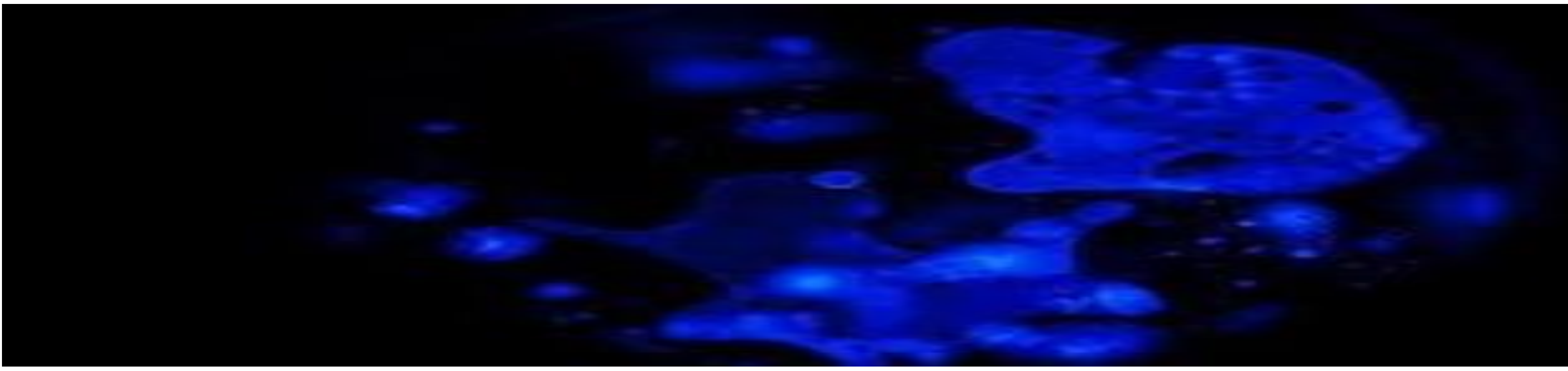
for instance if there’s a particular site that is running an unusual commercial version of an application which would be too expensive to replicate on a dummy environment but which offers the chance to demonstrate a particular security technique or flaw. Or a trainer who wants to demonstrate open-source vulnerabilities which require the use of a live Google search.

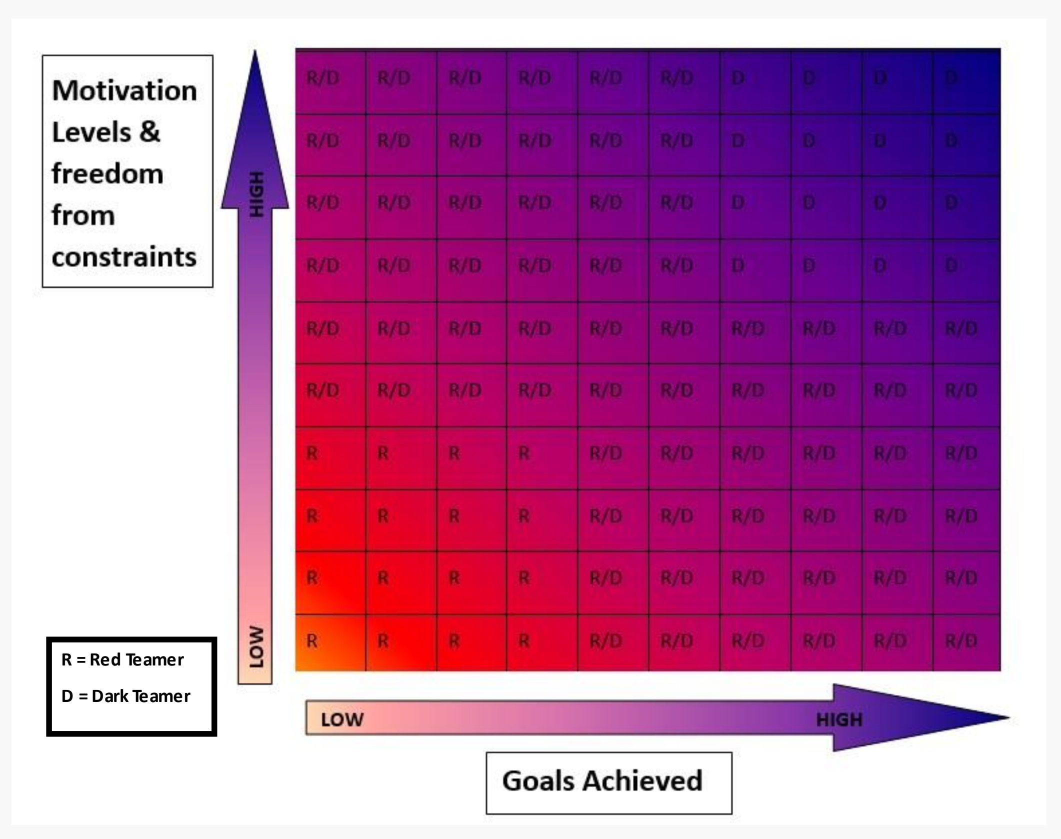
The **Bounty Hunter** seeks to gain financial reward and/or career recognition and will seek security flaws to this end. Such flaws will either be discovered in response to a specific bug bounty program request but not sticking to the official program scope and rules, or will be discovered and presented to companies who do not have a bug bounty program. Some hunters make approaches to these companies with the bug details and with demands or expectations of payment and/or recognition as a response to companies who may not respond to this help in the expected manner.

The **Whistle Blower** hacks to expose an organisation’s malpractice with the intention of helping the wider community. Whistle blowers are typically employees who do this without any active hacking but abusing their existing system privileges. A dark teamer whistle blower however performs traditional cyber-attacks (either from working for a company or by being a complete outsider) in order to blow the whistle, which is different. Examples include beaching email accounts of staff belonging to a particular organisation in order to expose staff malpractice. Or deliberately elevating system privileges in order to uncover financial irregularities.

And lastly, **The Detective** who wants to follow a trail or leads in their hunt for an elusive target – the main motivator being the enjoyment and challenge of the hunt and reaching that final goal. Examples include those who hunt for missing persons, family tree researchers, hunting threat actors and sources of cyber-attacks and following the trail of forensic leads. Obviously, many of these motives can be shared between the different types, but this just highlights the main ones characterising each type.

In all these cases the dark teamers have benign motives which often lead them into pushing the bounds of our knowledge of cyber-attacks and defence, driving social change for the good, and achieving beneficial results where other methods have failed. Ultimately, if you have two people – one who is acting the part of a threat actor and one who is actually a threat actor, the one who is just acting the part will not do as good a job. Imagine there is a real surgeon and someone pretending to be a surgeon – both who want to operate on you. The real surgeon is obviously going to make a more convincing job of it.



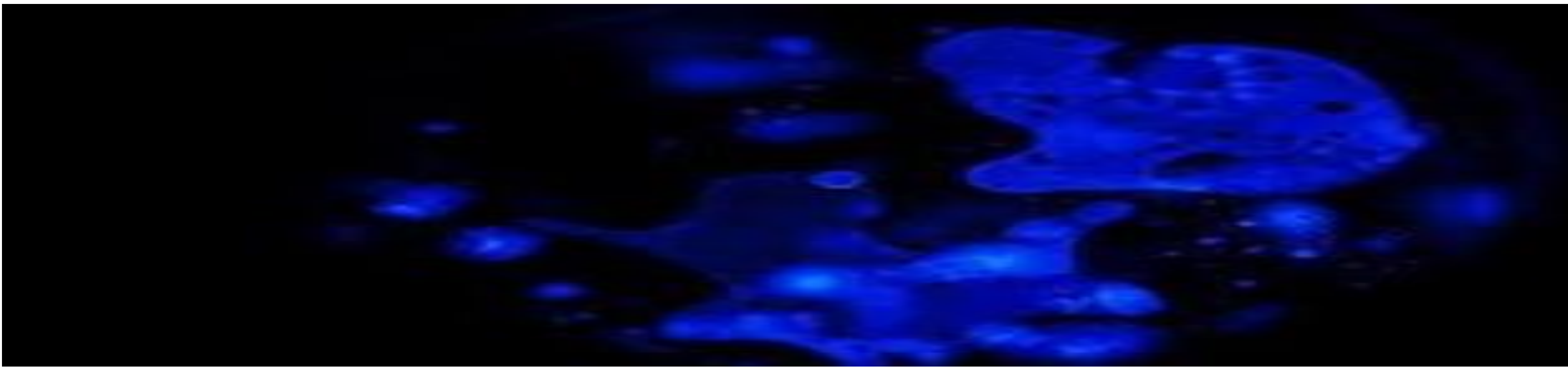


R/D	R/D	R/D	R/D	R/D	R/D	D	D	D	D
R/D	R/D	R/D	R/D	R/D	R/D	D	D	D	D
R/D	R/D	R/D	R/D	R/D	R/D	D	D	D	D
R/D	R/D	R/D	R/D	R/D	R/D	D	D	D	D
R/D	R/D	R/D	R/D	R/D	R/D	R/D	R/D	R/D	R/D
R/D	R/D	R/D	R/D	R/D	R/D	R/D	R/D	R/D	R/D
R	R	R	R	R/D	R/D	R/D	R/D	R/D	R/D
R	R	R	R	R/D	R/D	R/D	R/D	R/D	R/D
R	R	R	R	R/D	R/D	R/D	R/D	R/D	R/D
R	R	R	R	R/D	R/D	R/D	R/D	R/D	R/D

The above chart shows the basic correlation between freedom from rules and constraints and motivation, with the level of goals achieved. Red teamers, marked with `R' will be working under more rules and less motivation and will typically achieve less goals as a result. The Dark teamers, marked with a `D', will be highly motivated, and working under no constraints and will achieve more goals, and not least, get a more realistic picture of an organisation's security weaknesses. This comes back to what was said just now – a red teamer is acting the part. A dark teamer is actually the part.

Bug bounty programs mirror what companies generally desire a security tester to do and not to do. This is a typical company's requirements for bug hunters – setting out the in-scope and out of scope systems and the rules that the tester has to abide by to be eligible for a reward. Most requesting companies' bug programs are pretty similar to each other. But the more constraints there are the less likely these organisations are to understand the extent of any security weaknesses in their environment and with their assets.

So for example the following activities are prohibited: social engineering, interacting with accounts you don't own, violating anyone's privacy, putting in a backdoor, altering the rate of application requests, leveraging third party connections, looking for any third party vulnerabilities, application reverse engineering, conducting username enumeration, testing any physical security, content spoofing, running automated scanning tools, pivoting to any other systems, man in the middle

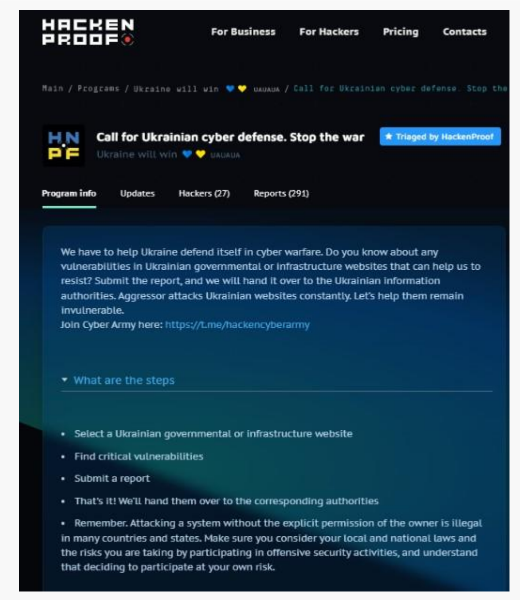


attacks, corporate firewall attacks, disclosure of non-protected information, conducting payment theft attacks and attacks requiring significant user interaction, run vulnerabilities from a jailbroken device, using SSL exploits, conducting a denial of service, exploiting DNS configuration issues, and issues that require unlikely user interaction. In other words, you must not do anything that might actually breach the network and thus emulate a threat actor.

Furthermore, many bounty programs stipulate a minimum age – sometimes 18, sometimes 14. So If you are 13 and find a serious vulnerability should this be ignored? It must be stated that it is definitely a positive thing that companies have bug bounty programs rather than none at all, and that they are seeking help to discover their security weaknesses. And they are obviously entitled to define the rules within which they believe discovered vulnerabilities merit a reward.

In this vein, the formal report titled `An approach to minimizing legal and reputational risk in Red Team hacking exercises' by Joseph DeMarco is basically like a guide on how to prevent any sort of security or legal mishap on corporate systems caused by security testers. It says things like Red Teamers should avoid viewing any financial, customer or employee data, should never exfiltrate data or use malware, and only use tools and technologies that come from reputable sources. They should never use tools that violate corporate use agreements. Testing should be done in a manner in which the user or system is not put at any additional risk; they should avoid actions that could adversely affect the Company's clients or other third parties, should avoid intercepting data flows coming to or from third party service providers, they shouldn't use any form of social engineering involving pretexting and should not be authorized to log into the Company's systems utilizing an employee's access credentials. He says that the Company should clearly state what testing devices are permitted, the acceptable methods of physical intrusion testing and will need to abide by all Company Code of Conduct policies and Memorandum of Agreement.

Clearly all these restrictions – which certainly will not be adhered to by genuine attackers – limit what testers can discover and ensure that companies don't violate their policies and insurance.



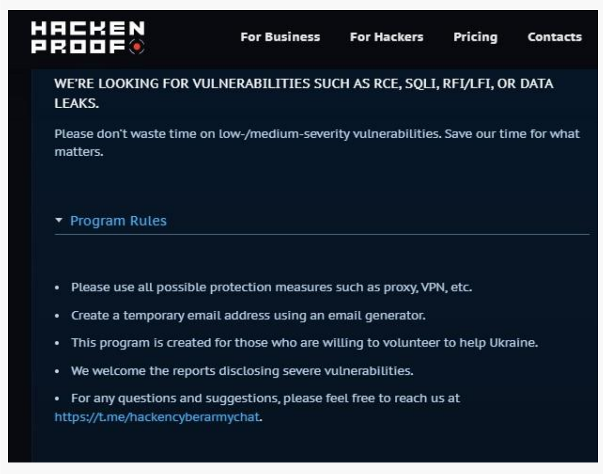
Call for Ukrainian cyber defense. Stop the war

Ukraine will win 💙💛 UAUAUA

We have to help Ukraine defend itself in cyber warfare. Do you know about any vulnerabilities in Ukrainian governmental or infrastructure websites that can help us to resist? Submit the report, and we will hand it over to the Ukrainian information authorities. Aggressor attacks Ukrainian websites constantly. Let's help them remain invulnerable.
Join Cyber Army here: https://t.me/hackencyberarmy

▾ What are the steps

- Select a Ukrainian governmental or infrastructure website
- Find critical vulnerabilities
- Submit a report
- That's it! We'll hand them over to the corresponding authorities
- Remember. Attacking a system without the explicit permission of the owner is illegal in many countries and states. Make sure you consider your local and national laws and the risks you are taking by participating in offensive security activities, and understand that deciding to participate at your own risk.

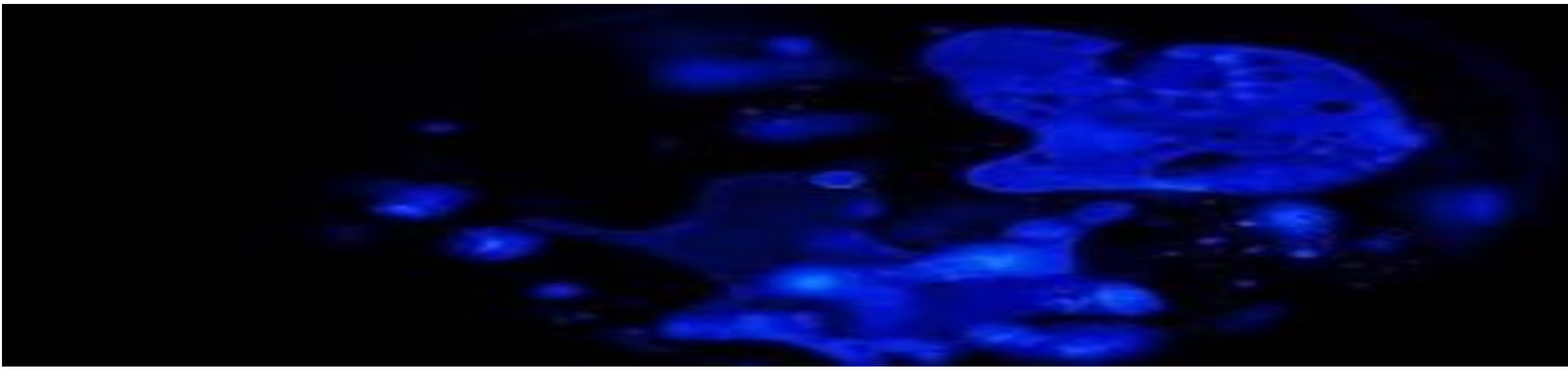


WE'RE LOOKING FOR VULNERABILITIES SUCH AS RCE, SQLI, RFI/LFI, OR DATA LEAKS.

Please don't waste time on low-/medium-severity vulnerabilities. Save our time for what matters.

▾ Program Rules

- Please use all possible protection measures such as proxy, VPN, etc.
- Create a temporary email address using an email generator.
- This program is created for those who are willing to volunteer to help Ukraine.
- We welcome the reports disclosing severe vulnerabilities.
- For any questions and suggestions, please feel free to reach us at https://t.me/hackencyberarmychat.



This above shows an example of a bug bounty program which would allow dark teamers to operate more effectively. This is a program to seek assistance with discovering security flaws on Ukrainian government and key national systems in order to help with the current war effort. There are no rewards offered and no rules about what testers can and cannot do. This appeared to have had lots of submitted vulnerability reports from testers who were probably very motivated to help with this particular cause.

The following shows some of the attack methods utilised by dark teamers – methods which red teamers would either not be permitted to use, not have time to carry out or would not consider using:

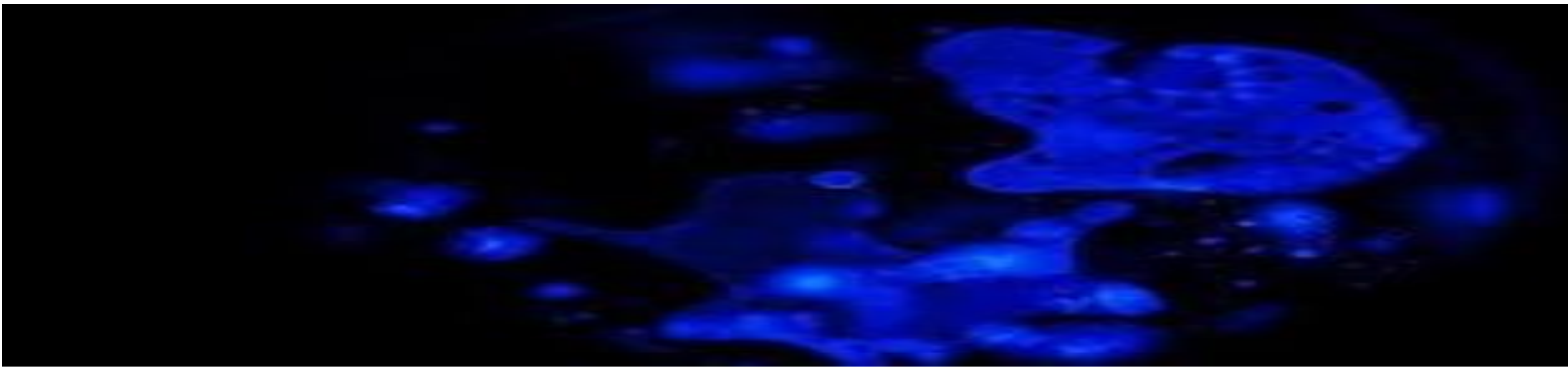
- Reputational damage through doxing, fake or genuine news propagation on social media, getting recordings of sensitive video calls, phone messages or in person conversations. What makes such attacks effective and dangerous is the ease with which they can be done, the lack of tooling or resources that the target company has to detect or prevent this and the potentially high damage to sales and reputation. With the luxury of more time, dark teamers can simply work for the target organisation or pay an existing employee there to obtain or carry out what they want done, rather than try and breach it through technical means from an external perspective.

- Targeting a company's staff via their personal accounts on non-corporate sites and also via their non-corporate devices can often be an effective way of breaching the company. Employees may use their personal email accounts to send or receive company sensitive information and, in this way, will circumvent the security controls in place on the corporate network. Social engineering attempts may target them via their social media accounts, their home Wi-Fi may be targeted, and personal apps like proof reading or file conversion sites may be hacked to obtain company data.

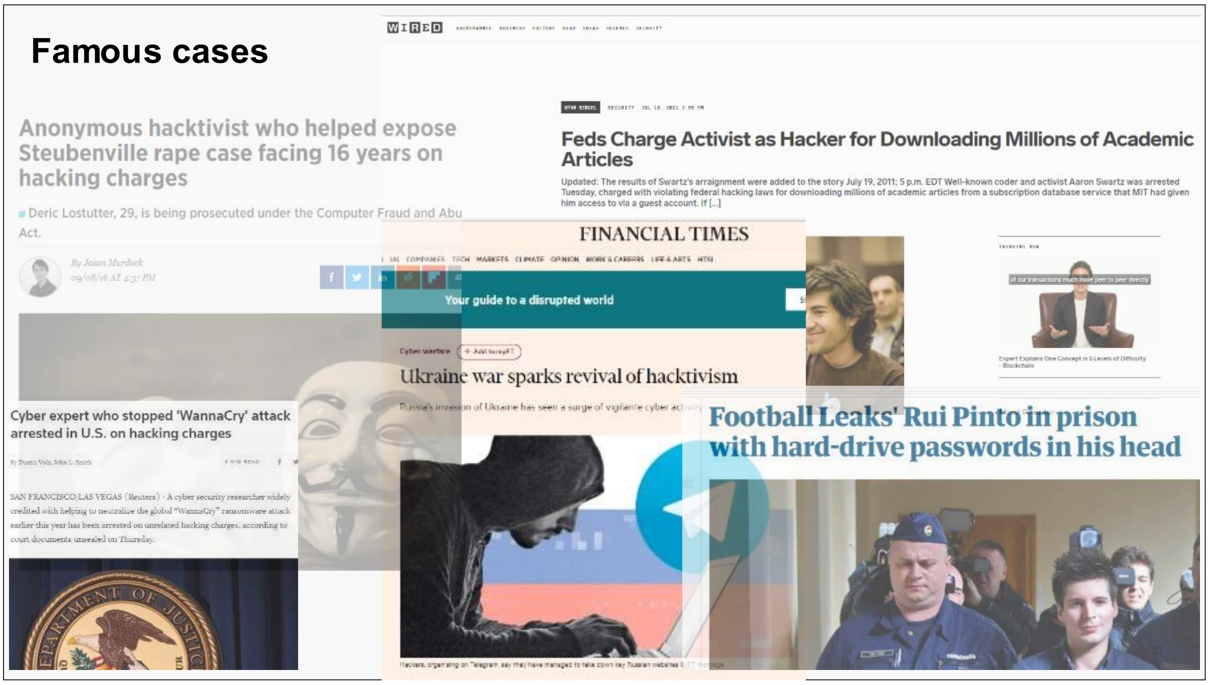
- Application and business logic flaws are not normally scrutinised by security testers and defenders as they are usually hidden from those are specifically looking for them. An application could be deemed very secure in the normal scheme of things but allow unintended attacker behaviour. Such behaviour, even if it does not lead to a critical privilege escalation or network compromise, could still lead to a resultant high degree of financial loss and reputational damage. Again, discovering these flaws is often a lengthy and manual process which red teamers may not have the time for.

- Dark teamers may conduct passive phishing by setting up fake websites to attract targets of interest. No emails or invitations are sent to the target staff, but instead adverts might be made to induce people to interact with the fake site – either to gain account credentials and personal details or to use evidence of interest in the site to further the purpose of their dark teaming activities.

- Red teamers will typically not be able to utilise hundreds of others to perform a distributed denial of service, whereas a dark teamer may, depending on the reason for the attack. An example of this could be crowdsourcing mass phone calls to the target company to disable their phone network as well as traditional system denial of service attacks.



- Lastly, dark teamers may have the time and resources to carry out the lengthier staff account brute-forcing activities.



Famous cases

WIRED

SECURITY JUL 19, 2011 2:55 PM

Feds Charge Activist as Hacker for Downloading Millions of Academic Articles

Updated: The results of Swartz's arraignment were added to the story July 19, 2011; 5 p.m. EDT Well-known coder and activist Aaron Swartz was arrested Tuesday, charged with violating federal hacking laws for downloading millions of academic articles from a subscription database service that MIT had given him access to via a guest account. If [...]

Anonymous hacktivist who helped expose Steubenville rape case facing 16 years on hacking charges

Deric Lostutter, 29, is being prosecuted under the Computer Fraud and Abu Act.

By Jason Murdock
09/08/16 AT 4:37 PM

FINANCIAL TIMES

Your guide to a disrupted world

Cyber warfare

Ukraine war sparks revival of hacktivism

Russia's invasion of Ukraine has seen a surge of vigilante cyber activity

Hackers, organising on Telegram, say they have managed to take down key Russian websites © FT montage

Cyber expert who stopped 'WannaCry' attack arrested in U.S. on hacking charges

By Dustin Volz, John L. Smith

SAN FRANCISCO/LAS VEGAS (Reuters) - A cyber security researcher widely credited with helping to neutralize the global "WannaCry" ransomware attack earlier this year has been arrested on unrelated hacking charges, according to court documents unsealed on Thursday.

Football Leaks' Rui Pinto in prison with hard-drive passwords in his head

Expert Explains One Concept in 5 Levels of Difficulty - Blockchain
of our transactions much more peer to peer directly
DEPARTMENT OF JUSTICE
10

There have been some famous cases of dark teaming in the news over the last few years to highlight this particular brand of hacking.

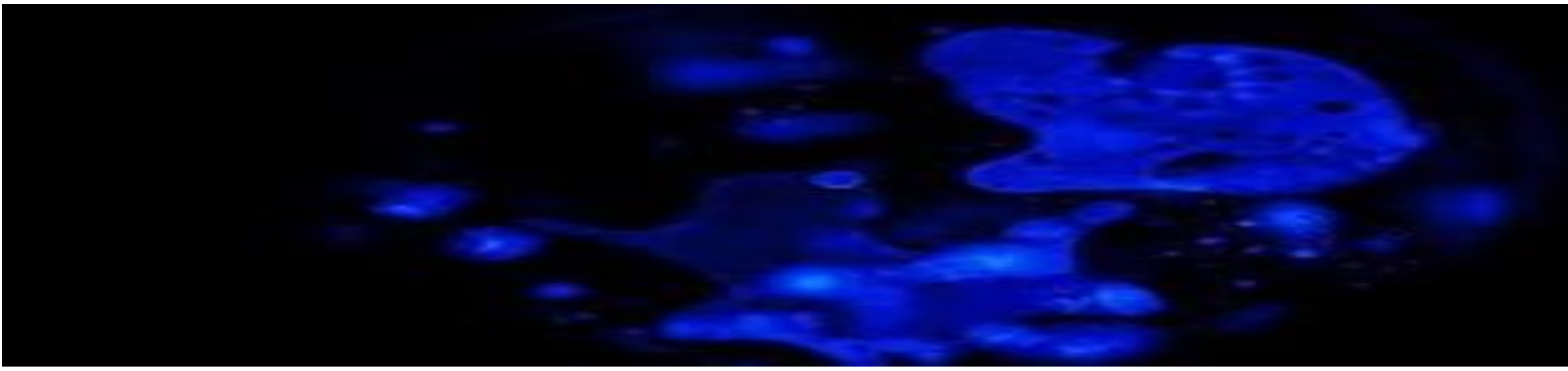
Some of the most current cases involve deliberate attacks on Russia and Ukraine by their respective opponents, most of whom will come under the `activist' category.

The case of reddit founder Aaron Swartz who illegally downloaded academic research material using a physical connection to a server at MIT, demonstrates activism around the issue of freedom of information. It is believed that the stress of being convicted of multiple counts of computer violation laws led to his suicide.

The Steubenville rape case cover up, exposed by hackers, is an example of Sheriff dark team behaviour as they hacked those helping to cover up the crime, in order to demand justice and an official apology.

The Wannacry malware was neutralised by someone who at the time was not technically dark teaming, but had made use of his skills in creating malware in a prior life, in order to do some good. It is questionable whether he would have had this knowledge and motivation had he not indulged in the dark side of cyber security for years prior to Wannacry.

The recent case of Rui Pinto who was charged with the football leaks incident is a good example of the whistle blower dark teamer who wanted to expose malpractice in the world of football.



So how does one find and recruit a dark teamer?

Starting with the sheriff, who wants to stop crime and help the community, the best way to find them is from those who have committed cyber-crimes in the past – not necessarily from `sheriff' type crimes and campaign groups.

The whistle blower also has community spirit and a desire to expose and publicise malpractice. They can be found among journalists, is internal staff, 3rd party contractors/vendors and ex-employees.

The activist's driver is to help the cause and effecting social change, being commonly found on campaign groups.

The trainer desires a realistic training environment and can be found working in IT security companies as trainers and on tech forums.

The security researcher wants to make new discoveries and be recognised for this, - often found on bug bounty sites, IT security companies, research organisations and tech forums.

The bounty hunter wants money and recognition and can be found on bug bounty sites and from current or ex-offenders mentioned in the news or other sources, IT security companies and tech forums.

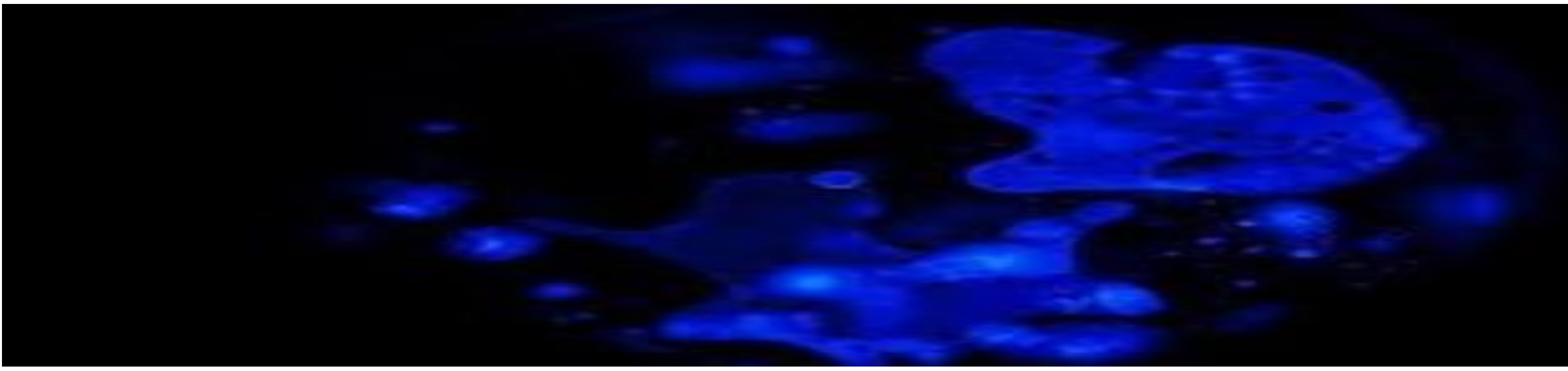
And the detective, who loves to follow a trail and capture a flag. They can be found among Journalists, in research groups, and specific social media sites.

This is not a definitive list of the qualities for each group – motivators can be shared much more than is listed here. And some people will be more than one type – for instance a detective who also wants to conduct security research.

Readers may be thinking this all sounds great but aren't there rules and policies for security testers for a reason? It would take a brave company to hire someone with a known disdain of following rules or laws. Could you trust them? What if things went wrong, and what would be the recourse for this? Would cyber insurance companies pay out? Would shareholder confidence be damaged? Well things do go wrong for legitimate red teamers who sometimes land themselves in hot water by accident.

Dark teamers do not have to be officially employed and on the payroll. They can just be communicated and collaborated with. The best advice would be to trial working with them for a short time and assess the risk versus the merits during this trial, after which the collaboration can continue.

If a dark teamer inadvertently causes network issues through their attacks for example, then the cyber insurance policy could in theory honour the conditions of the policy because in such a situation the company has suffered a breach through a deliberate attack which has not been officially authorised.



Dark teamers are not traditional criminals who want to conduct malicious actions for personal financial reward. They may have the mindset and capability of someone who does do these nefarious actions but normal legitimate security red teamers, if they are good their job, are also supposed to emulate this mindset. You are not trying to reform a criminal – just redirect their efforts into doing what they already know how to do well but for the benefit of the employing company.

The employing or collaborating company must trust and give them the benefit of the doubt but play to their motives/drivers. So rather than saying `if you work for me I will pay you £100000 a year', say `if you work with me you will help us raise our profile as being the biggest funder of anti-smoking publicity initiatives' or `you will help us to make important discoveries in the field of life saving intensive care equipment' or `you could be number 1 in our hall of fame bug hunters which is viewed by thousands every month'.

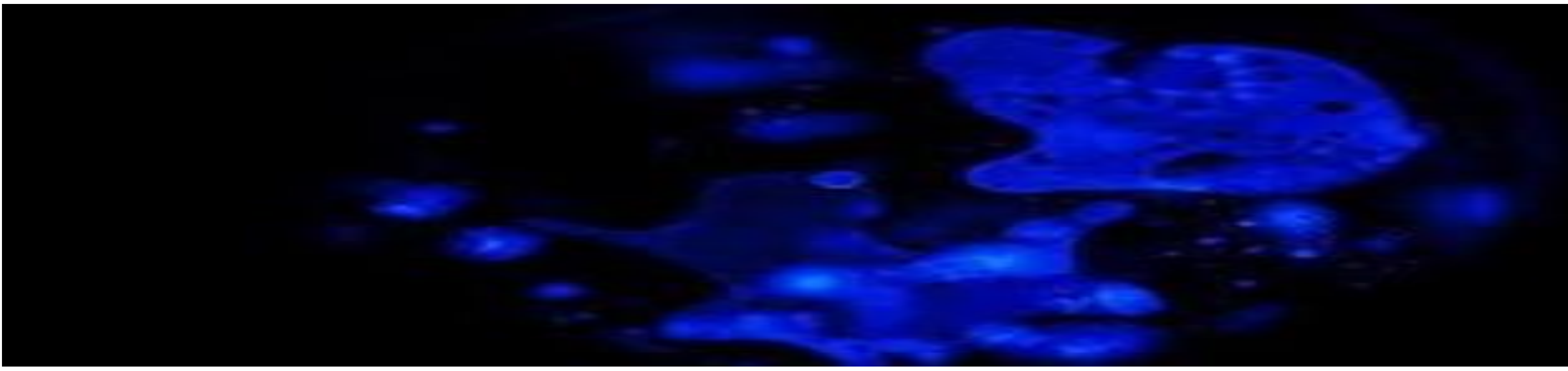
It is up to the collaborating or employing company to pitch their work proposition in the best possible way and tailored to who they approach or how they advertise.

Additionally, the company should make it possible and easy for security vulnerabilities which have only been discovered as a result of illegal actions to be anonymously and safely reported. Red teamers can and do recklessly or accidently overstep their scope and the established boundaries of their engagements. In the offline world, where there are many serving law enforcement officers with a criminal record. Dark teamers need to know that they are granted an immunity from legal repercussions if they are known, and if they are anonymous, there is a safe way to report any issues.

One could view this that it is surely better to work with an attacker and understand what they can discover, than be taken by surprise by an unknown attacker who has more malicious intentions.

It is useful to look at existing laws to see whether they could be applicable to dark teaming and possibly help in any defence case. Most countries have a good Samaritan law which offer legal protection to people who give assistance to others who are in danger or injured in order to encourage people to help others without fear of being prosecuted for unintentional injury. But people can be prosecuted for recklessness under these laws if they help someone else but cause an injury when there was no immediate peril or they fail to provide any assistance in the first place.

In many countries, `necessity` can be used as a possible justification for breaking the law – in other words, a particular conduct was necessary in order to prevent some greater harm and which would fall outside of the excuse of self defence. This allows those who have good conduct and motives to intentionally cause injury, loss or damage. The defendant must prove that the result of their actions outweighs the consequences of what they are being charged with, they have no reasonable alternative, they stopped the prohibited conduct as soon as it is not necessary and they themselves did not cause the problem or harm they were seeking to stop or avoid. The degree of harm caused needs to be weighed against the degree of harm threatened. In some countries there has to be an element of imminent danger and indeed many of these necessity laws involve an element of physical harm to people, but is separate to self defence. For instance, smashing a window to rescue someone from a burning building or ignoring traffic rules to rush a dying person to hospital in a car.



Usually, the harm that one seeks to prevent has to be serious enough to warrant the illegal activities done to prevent it, but interestingly in Switzerland in 2020 there were two cases of climate activists not convicted of trespassing on Credit Suisse branches after they claimed their actions were necessary to help tackle climate emergency issues.

Recently, the US Department of Justice amended the Computer Fraud and Abuse Act to say that researchers, ethical hackers and other well-intentioned people won't have to face federal charges if they're investigating, testing or fixing vulnerabilities in good faith and not for malicious purposes. They may still be subject to state-level charges, however. This legal amendment also has the advantage of deterring those who seek to silence whistle blowers who discover vulnerabilities, with the threat of being subject to criminal charges. For instance, in October 2021 Missouri Governor Mike Parson threatened a reporter with prosecution for pointing out a website data leak that had not even required any hacking to discover.

To sum up, organisations should tap into this dark teaming testing resource to fully understand their vulnerabilities which may not be discovered using traditional testing methods. The concept of using such people is new and obviously comes with a higher degree of risk, but this risk could be managed in the interest of making security tests much more fruitful. The protection of such testers who have benign motives should be increased through amending the current laws.

Cyber-crime still goes on, unreported by companies to the authorities or media if discovered, or just simply not discovered at all. And even when cases are investigated the attacker is rarely found. Even offline crimes such as burglary and assault are mostly under reported and unsolved. This calls for a change in how we view and utilise those who could help us highlight security vulnerabilities.