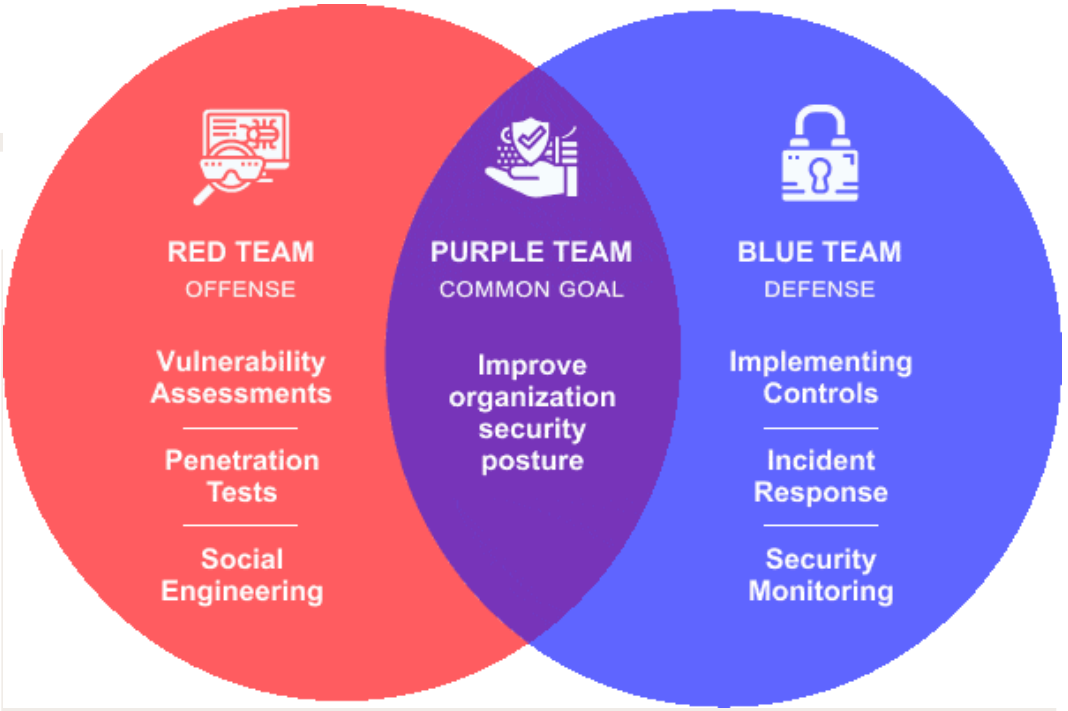
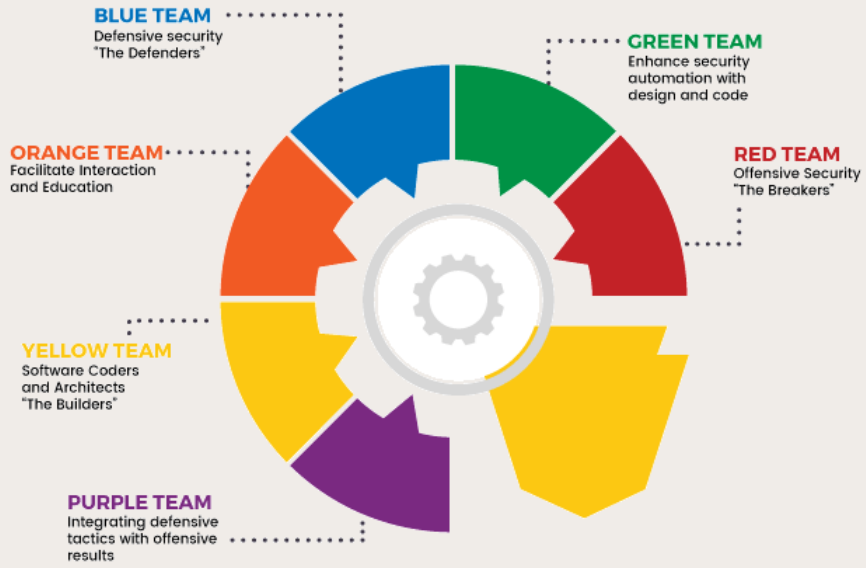


شرح شامل عن فرق الأمن السيبراني (Cybersecurity Teams)

Cyber Security Teams

Red Team vs Blue Team
Purple Team vs Green Team vs
Yellow Team vs Orange Team

الفريق البرتقالي الفريق الأصفر الفريق الأخضر الفريق البنفسجي الفريق الأزرق الفريق الأحمر

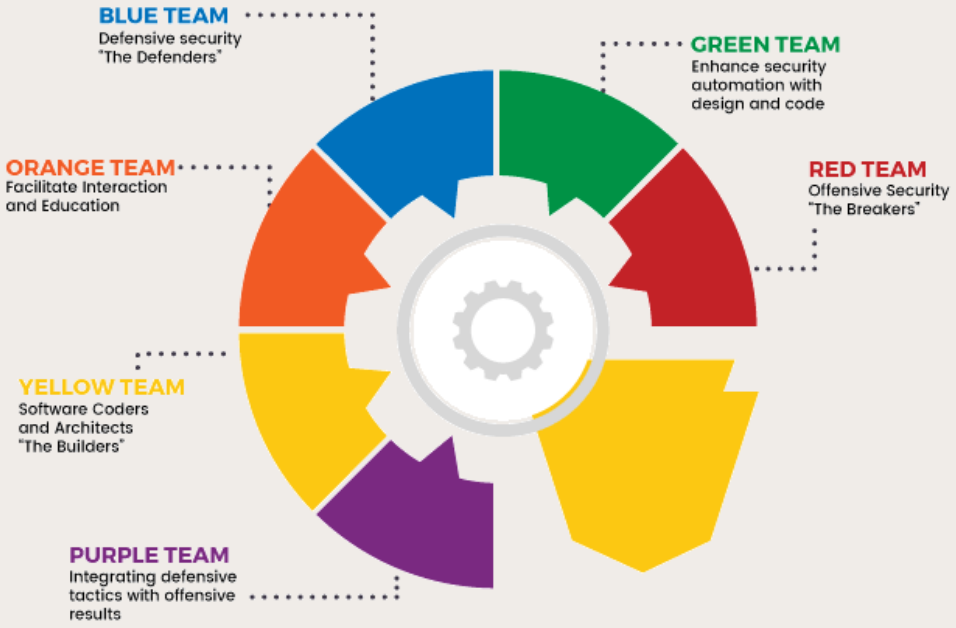


Cyber Security Teams

In this video, we'll explore the security teams like the Red Team, Blue Team, and others — and what each of them does!

في هذا الفيديو، سنتعرف على الفرق الأمنية مثل الفريق الأحمر، الفريق الأزرق، وغيرهم، ودور كل منها!

Cyber Security Teams



Cybersecurity teams are groups of professionals who work together to protect systems and networks from cyberattacks. The roles of these teams vary based on their assigned tasks, but the ultimate goal is to achieve the highest level of security.

ما هي فرق الأمن السيبراني؟

فرق الأمن السيبراني هي مجموعات من المتخصصين الذين يعملون معًا لحماية الأنظمة والشبكات من الهجمات الإلكترونية. تختلف أدوار هذه الفرق بناءً على المهام الموكلة إليها، ولكن الهدف النهائي هو تحقيق أقصى درجات الأمان للأنظمة.

Cyber Security Teams

Imagine you're running a company, and suddenly, you get a message saying your website or network has been hacked! 😱

تخيل أنك تدير شركة، وفجأة تصلك رسالة تخبرك أن موقعك الإلكتروني أو أن شبكة الشركة قد تعرضت للاختراق!

Cyber Security Teams

Who’s responsible for protecting these systems?

من المسؤول عن حماية هذه الأنظمة؟

Cyber Security Teams

In cybersecurity, there are different teams — some attack to test defenses, others defend, and some build systems and teach people how to stay safe!

في الأمن السيبراني، هناك فرق متخصصة لكل مهمة! بعضها يهاجم لاختبار الحماية، وبعضها يدافع، وفرق أخرى تطور الأنظمة او تُوعي المستخدمين ليحمون أنفسهم من هجمات وبعضهم امور الأخرى ستتعلمه بعد قليل

The Red Team are experts in offense. But don't worry, they are not criminals! They are specialists who simulate real hacker attacks to test system security.

الفريق الأحمر هم المحترفون في الهجوم. لكن لا تقلق، فهم ليسوا مجرمين!
بل هم مختصون يحاكون هجمات هكرز الحقيقيين لاختبار أمان الأنظمة.

الفريق الأحمر (Red Team)

The Attackers / Breakers

الفريق الأحمر (Red Team)

What is their role?

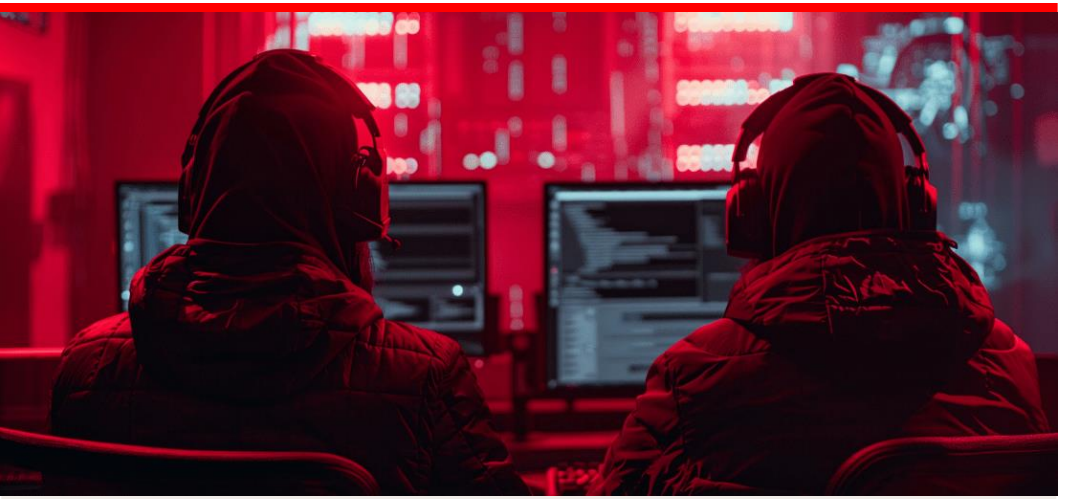
✔ Attempt to breach systems using the same techniques as hackers to discover security flaws before attackers exploit them.

✔ Evaluate the effectiveness of current security measures by testing how well they withstand attacks.

وظيفتهم:

✔ محاولة **اختراق الأنظمة** بنفس الطرق التي يستخدمها الهكرز لاكتشاف الثغرات الأمنية قبل أن يستغلها المهاجمون الحقيقيون.

✔ **تقييم مدى فعالية أنظمة الحماية الحالية** عند تعرضها للهجمات.



الفريق الأحمر (Red Team)

Imagine you have a large company and want to ensure its system is secure. The Red Team attempts to breach the system using the same methods real hackers would, identifying vulnerabilities before cybercriminals do!

تخيل أن لديك شركة كبرى، وتريد التأكد من أن نظامها آمن. يمكن للفريق الأحمر محاولة اختراق النظام بنفس الأساليب التي قد يستخدمها المخترقون الحقيقيون، لاكتشاف الثغرات قبل أن يستغلها القراصنة!

The Blue Team is the defense team

الفريق الأزرق (Blue Team)

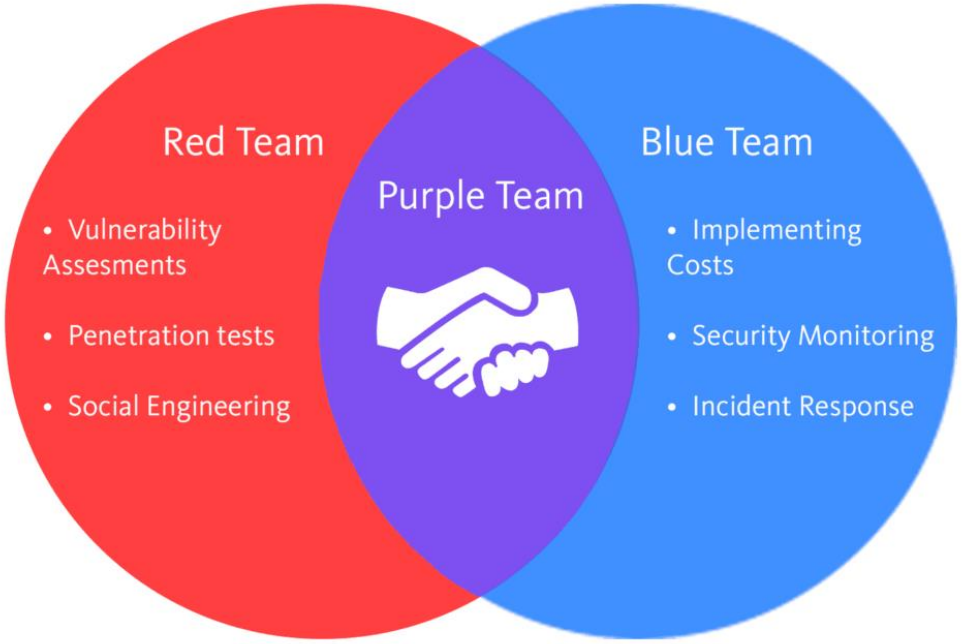
الفريق الأزرق هو فريق الدفاع.

They protect systems from attacks, monitor the network, track threats, and respond quickly. In short: they are responsible for protecting the company from any cyber attack

الفريق الأزق (Blue Team)

يحمي الأنظمة من الهجمات، يراقب الشبكة، يتتبع التهديدات، ويرد عليها بسرعة.

بالمختصر: هو المسؤول عن حماية الشركة من هجمات الكترونية.



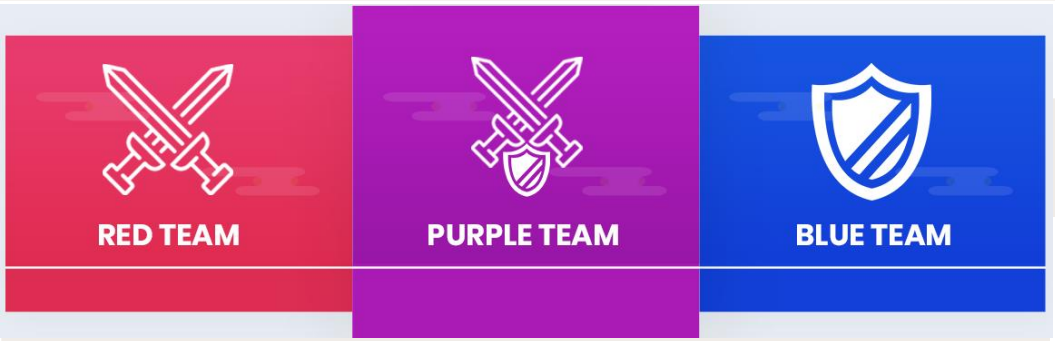
Combines the offensive tactics of the **Red Team** (attackers) with the defensive strategies of the **Blue Team** (defenders)

الفريق البنفسجي (Purple Team)

مزيجًا بين فريق الهجوم والفريق الدفاع

(فريق الأحمر والأزرق)

Red + Blue = Purple Team



Team	Role	Goal
Red Team	Attacks systems	Uncover vulnerabilities
Blue Team	Defends systems	Detect & block threats
Purple Team	**Both!**	Improve security through collaboration

Example Exercise

1. **Red Team** exploits a misconfigured server.
2. **Blue Team** fails to detect the attack.
3. **Purple Team** works together to:
   - Fix the misconfiguration.
   - Add new detection rules.
   - Train staff on similar threats.

الفريق البنفسجي (Purple Team)

يحلل نتائج اختبارات الفريق الأحمر ويقترح تحسينات للفريق الأزرق.

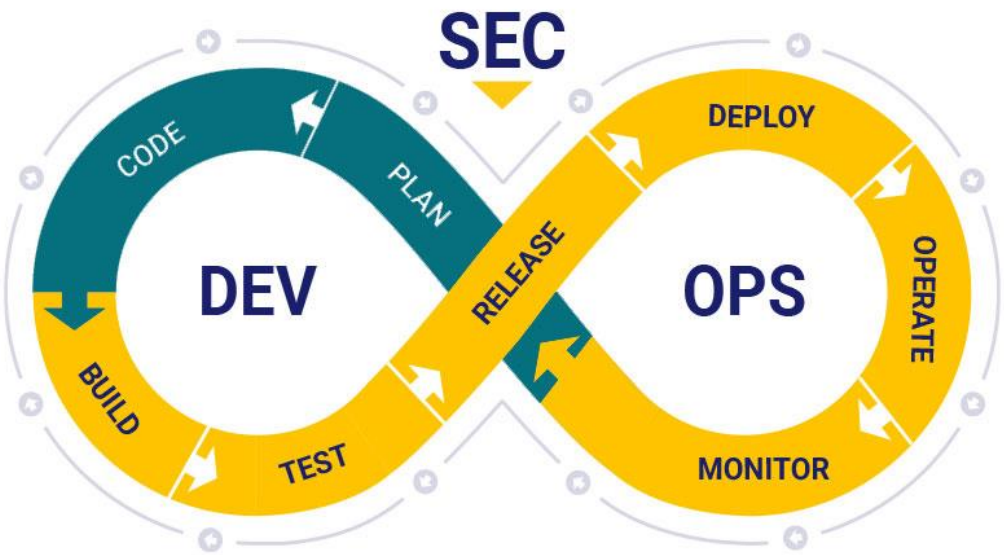
ينظم التعاون بين الهجوم والدفاع، ويطور تدريبات وخطط استجابة للحوادث.

هدفه رفع مستوى الحماية بشكل مستمر ومساعدة الشركة تكون جاهزة ضد التهديدات.

The Green Team is responsible for embedding cybersecurity into the software development process from the very beginning.

الفريق الأخضر (Green Team)

الفريق الأخضر هو الفريق الذي يعمل على دمج الأمن السيبراني داخل عملية تطوير البرمجيات منذ بدايتها.



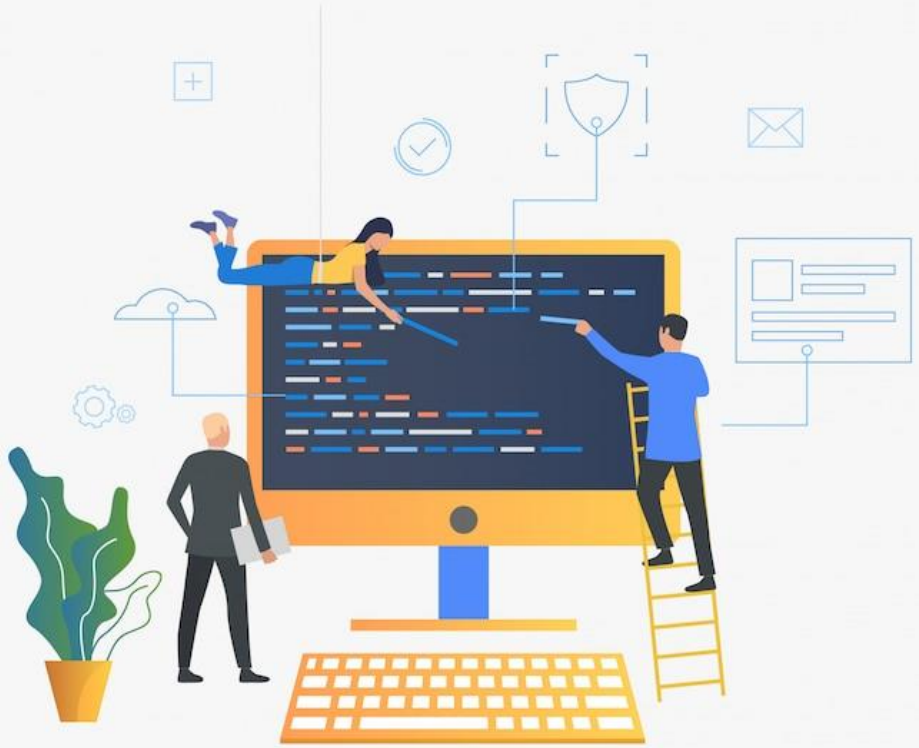
كلمة **DevSecOps** تتكوّن من ثلاثة أجزاء:

- **Dev** = Development (التطوير)
- **Sec** = Security (الأمن)
- **Ops** = Operations (التشغيل)

الفريق الأخضر (Green Team)

They focus on applying secure coding practices and integrating security tools and techniques, like DevSecOps, to make security a natural part of development.

يهتم بتطبيق مبادئ البرمجة الآمنة، ويدمج أدوات وتقنيات الحماية داخل أنظمة العمل مثل DevSecOps، ليجعل الأمن جزءًا طبيعيًا من تطوير الأنظمة.



GREEN TEAM

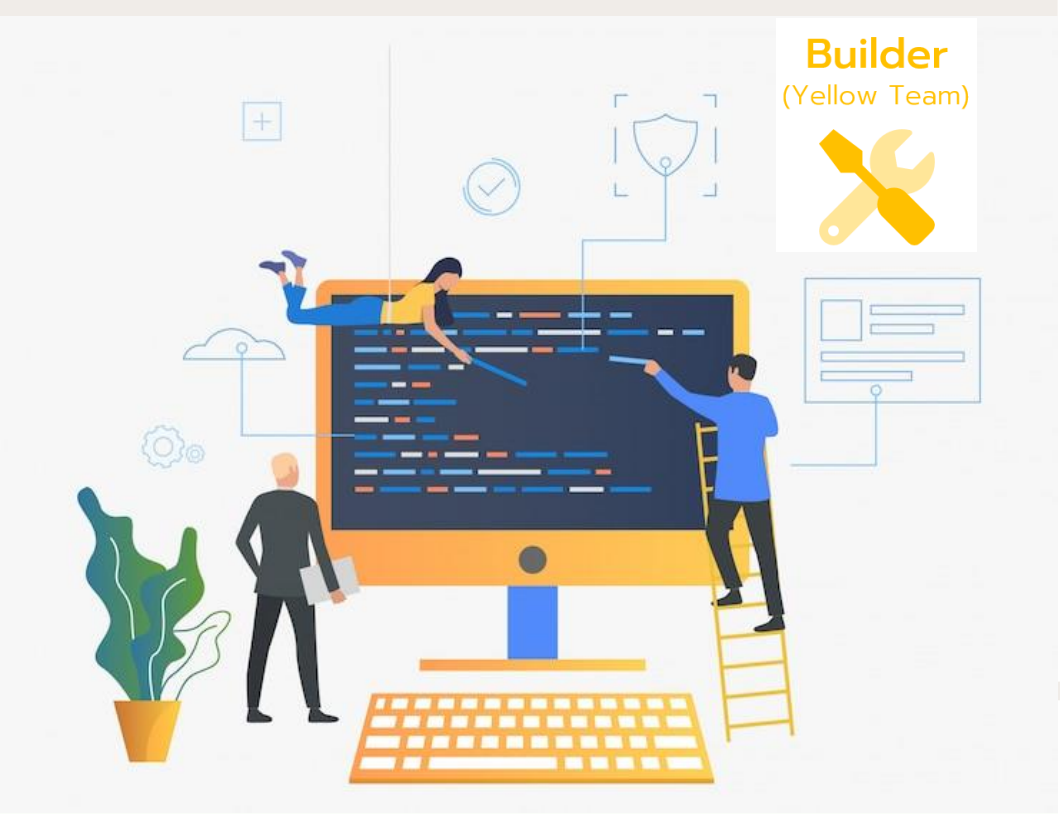
Their goal is to ensure that software is secure from the moment it is designed,

not just after it is completed.

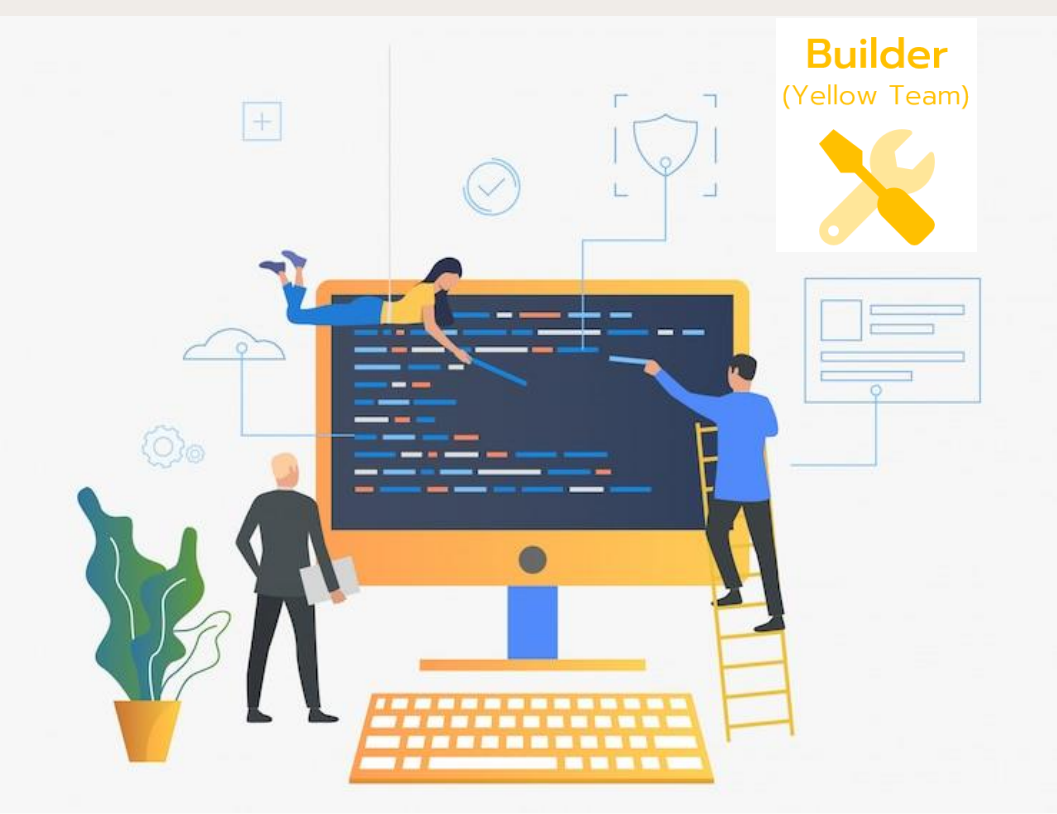
هدفه أن تكون البرمجيات آمنة منذ لحظة تصميمها،

وليس بعد الانتهاء منها.

الفريق الأخضر (Green Team)



الفريق الأصفر (Yellow Team)



YELLOW TEAM

Yellow Team: The Builders

Role and Function: Yellow Teams, also known as "Builders," are responsible for developing secure software and applications. They work closely with research and development teams to ensure security is integrated into the development process.

الفريق الأصفر (Yellow Team)

الفريق الأصفر يمكنك اعتباره فريق المبرمجين المسؤولين عن برمجة حلول للشركة. يكتبون كودًا آمنًا لضمان عدم تمكن المهاجمين من استغلال الكود أو اختراق الأنظمة.

الفريق البرتقالي (Orange Team)

The Orange Team connects the Red Team's knowledge of vulnerabilities with the Yellow Team's (builders).

الفريق البرتقالي (Orange Team)

الفريق البرتقالي هو مزيج بين الفريق الأحمر والفريق الأصفر.

الفريق البرتقالي (Orange Team)

They use the Red Team's knowledge to train the Yellow Team on how to write secure code.

يستخدم خبرة المهاجمين من Red Team

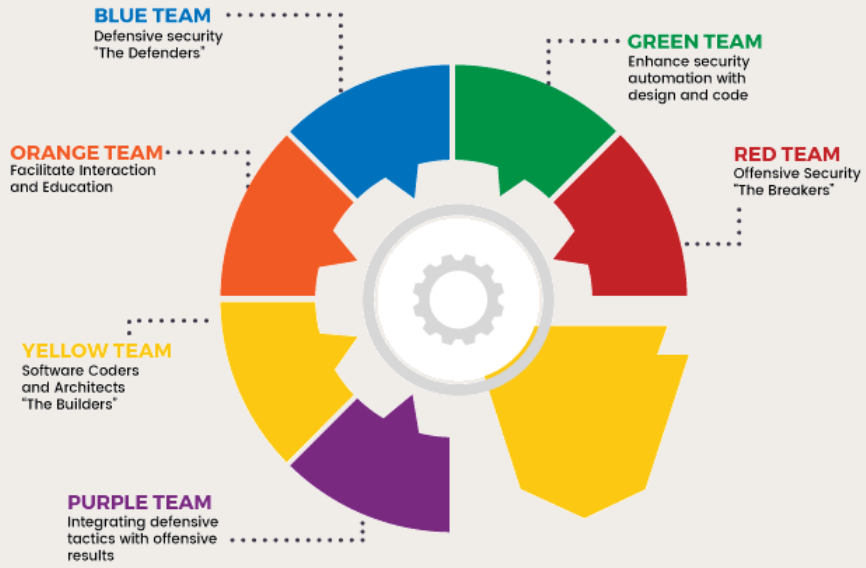
لتدريب المطورين من Yellow Team على

كتابة كود آمن.

In short: they teach developers how to build systems that are harder to hack, and help reduce vulnerabilities early.

الفريق البرتقالي (Orange Team)

بالمختصر: يعلمون المطورين كيف يكتبون كود يصعب اختراقه، ويقللون عدد الثغرات من البداية.



Cyber Security Teams