مرکز آپا دانشگاه سمنان

دانشگاه سمنان

# نقش مانـورهای تیـم قرمـز در ارتقـای امنیـت سـازمان

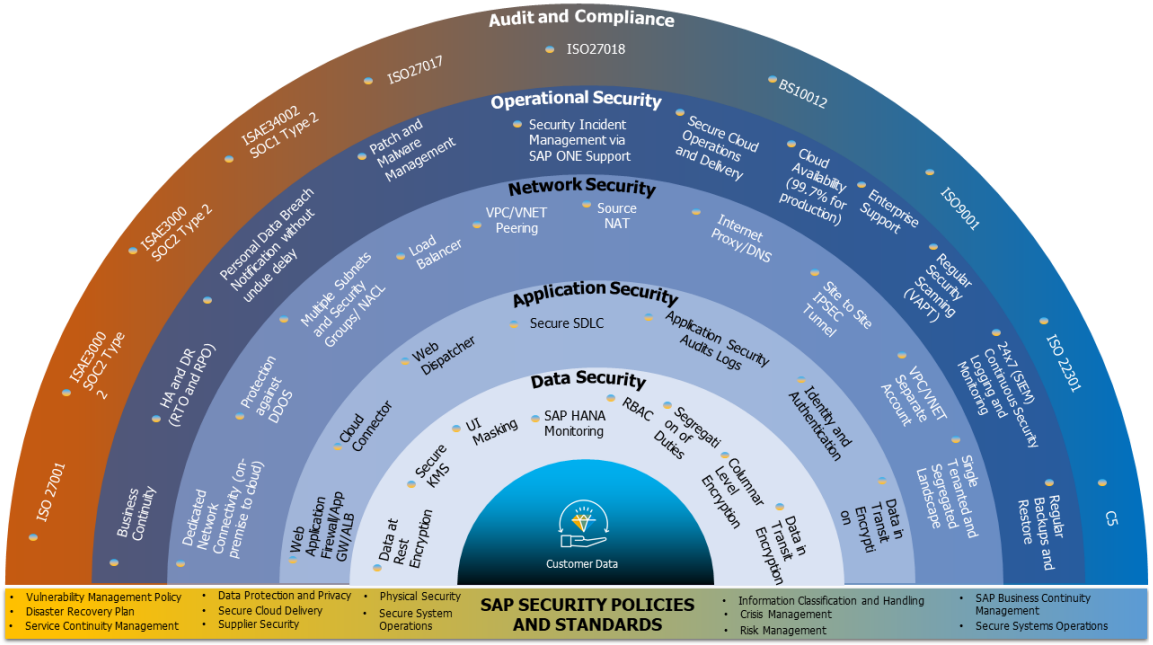

دکتر علیرضا نعیمی صدیق

cert.semnan.ac.ir
cert@semnan.ac.ir

مرکز آپا دانشگاه سمنان

# فراوانی ابزار مهاجمان دلیل محکمی بر افزایش حملات با دانش کم

# دفاع در عمق




- ✓ دفاع در عمق یک استراتژی امنیت سایبری است، که به راهبرد امنیت عمیق هم شناخته می‌شود و به رویکردی از امنیت سایبری اطلاق می‌شود که از لایه های چند گانه به‌عنوان حفاظت کل استفاده می‌کند.
- ✓ دفاع لایه‌لایه‌ای به سازمانها کمک می‌کند، آسیب‌پذیری‌های منجر به خطر را تا حد امکان کاهش و تهدیدات را کنترل نمایند.
- ✓ به بیان‌دیگر اگر مهاجمی از یک‌لایه دفاعی عبور کند، ممکن است توسط لایه دیگر مهار شود. اگر مهاجم بتواند از یکی از لایه‌های دفاعی عبور کند، بلافاصله به سد لایه دوم برخورد می‌کند.

مرکز آپا دانشگاه سمنان

# چـــرا ممکن است ســـــــازمان شـــــما مورد هدف نفوذگران قرار بگیرد؟

- اهداف رقابتی
- اهداف سیاسی و اطلاعاتی
- اهداف مالی
- انتقام یا سرگرمی

# چـــرا ممکن است ســـــازمان شـــما مـــورد هدف نفـــوذگران قـــرار بگیرد؟

- عدم شفافیت و نظارت قوی برروی پروژه ها و پیمانکاران
- ضعف در رولهای مقابله با اکسپلویت
- ارتباطات اعتماد محور با سازمانهای دیگر
- عدم آموزش کارمندان و پیمانکاران


FIREEYE FireEye Exchange SharePoint solarwinds

# امن سازی در سازمان ها

## ❑ارزیابی آسیب پذیری

اولین قدم مهم در شناسایی خطرات امنیتی

## ❑تست نفوذ

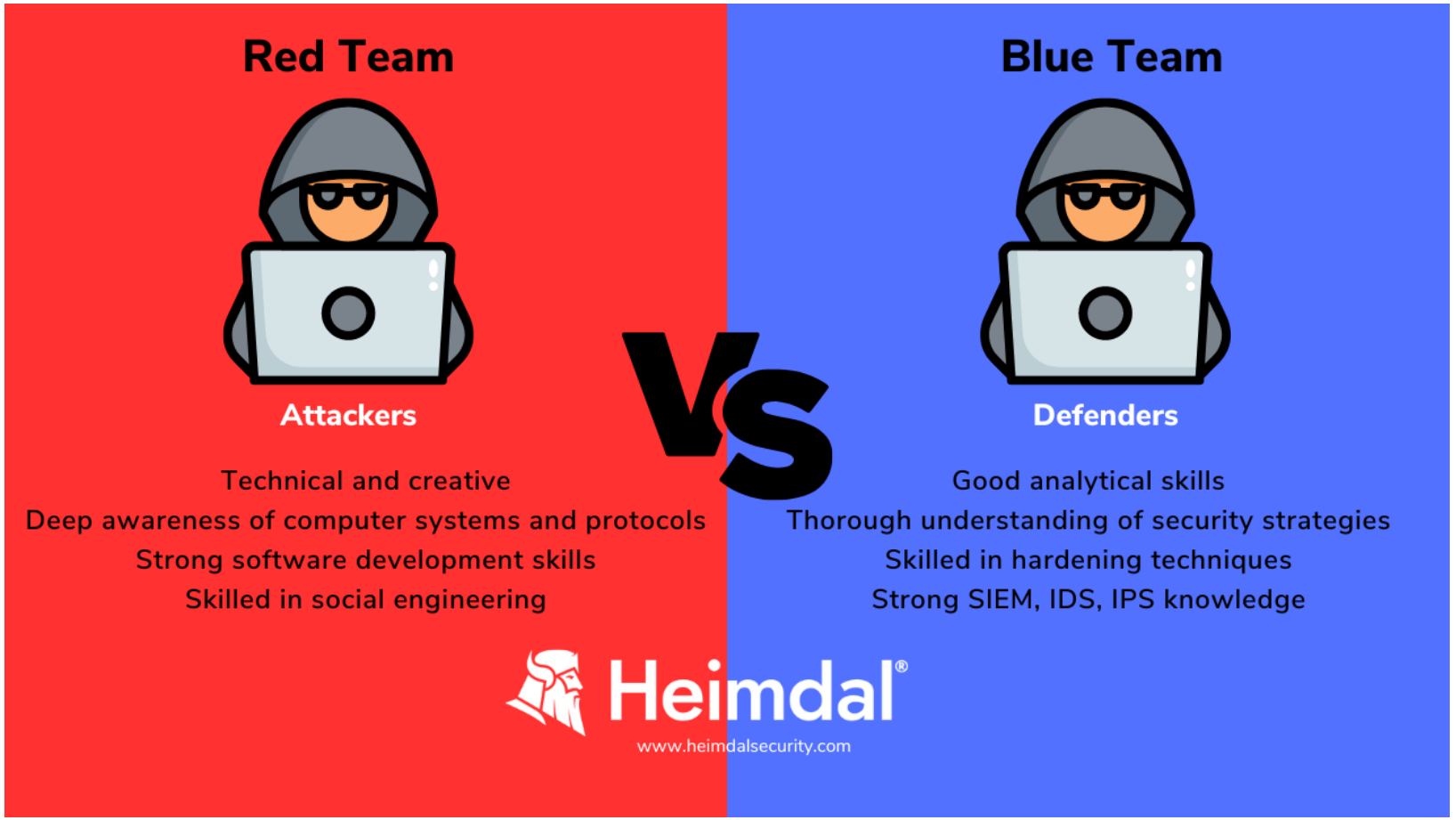
شناسایی و بهره برداری از آسیب پذیری‌ها و
تعیین اثربخشی اقدامات امنیتی یک سازمان

## ❑فعالیت های تیم قرمز

شبیه سازی جامع و واقعی از یک حمله واقعی
بررسی وضعیت امنیتی کلی یک سازمان با شناسایی و
بهره برداری از آسیب‌پذیری ها در سیستم ها، شبکه‌ها و
فرآیندها

برخلاف تست نفوذ، فعالیتهای تیم قرمز معمولا شامل افراد متعددی میشود و حتی می‌تواند سیستمهای متعددی را در برگیرد و دید جامع تری از وضعیت یک سازمان بدهد.

محافظت در مقابل
حملات سایبری




اگرچه تیم‌های قرمز و آبی در جهت مخالف هم هستند یعنی حمله و دفاع اما هدف نهایی آنها مشترک هست و آن بهبود وضعیت امنیت سازمان است .

مرکز آپا دانشگاه سمنان

# تیم قرمز

تیم قرمز (Red Team) با شبیه‌سازی عملیات هکرهای واقعی در دنیای مجازی و با استفاده از تمام تکنیک‌های نفوذ این کار را انجام می‌دهد. این امر به سازمان‌ها کمک می‌کند تا نقاط آسیب‌پذیری سیستم‌های امنیتی خود را، که می‌تواند تهدیدی برای آن‌ها باشد به درستی شناسایی کنند.

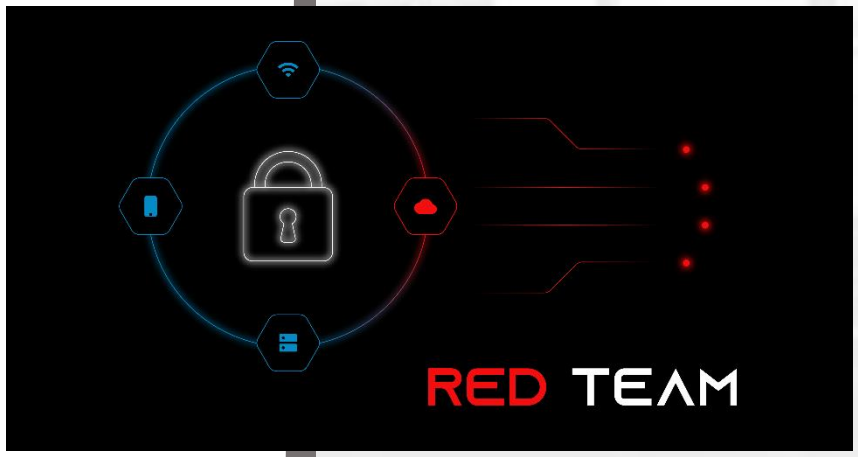

## اجزای تیم قرمز :

- ❑ سناریو
- ❑ رویکرد و نحوه اجرا
- ❑ زمان اجرا در تیم قرمز
- ❑ گزارش نهایی

مرکز آپا دانشگاه سمنان

# وظایف تیم قرمز

- سنجش میزان آمادگی تیم امنیت سازمان
- بهبود توانایی‌های دفاعی و مقاومت سازمان‌ها در برابر حملات پیچیده
- تجربه، ارزیابی و برطرف نمودن نشت‌های امنیتی در یک محیط کنترل شده
- شناسایی حیاتی‌ترین دارایی‌ها و آسیب‌پذیری‌ها و محافظت از آن‌ها
- کاهش زمان پاسخ‌گویی به وقایع و رخدادها



مرکز آپا دانشگاه سمنان

LFI

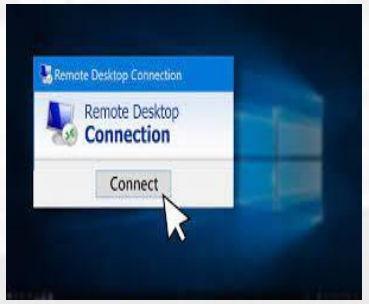
Users & password

No Zones Limit

DNS Bainded

DC ping

LDAP




LFI

User & passwords

Patch

مرکز آپا دانشگاه سمنان

LinkedIn

Phishing

Trusted Relationship

No Proxy

NO Zone Limit

NO Access Limit


مرکز آپا دانشگاه سمنان

## تفاوت تیم قرمز با تست نفوذ

چرا تیم قرمز

- شبیه سازی حملات سایبری
- دقت و سرعت تشخیص SOC
- دقت و سرعت تیم CSIRT
- سنجش سنسورها
- تست لاگ گیری

## نیازمندی های اجرای تیم قرمز

نیازمندی‌های یک تیم قرمز موفق

- آموزش کارمندان
- تست نفوذ و مقاوم سازی تجهیزات ارائه دهنده ی سرویس
- خرید تجهیزات و مکانیزمهای امنیتی
- تشکیل تیم های تدافعی (SOC,CSIRT,MSSP)
- زمان ها و دوره های مختلف
- بروز رسانی رول های جدید و trackکردن روشهای ارتقا امنیت
- هماهنگی کامل با تیم بنفش

## چالشهای اجـرای تیـم قرمـز

چالش‌های تیم قرمز

- از کار افتادن بیزنس سازمان هدف
- امکان شکست اجرای سناریو ها
- عدم تشخیص تیم آبی
- دانش ضعیف کارشناسان

مرکز آپا دانشگاه سمنان

# متدلوژی و استانداردهای تیم قرمز

- CBEST
- BANK OF MALESIA
- MITRE
- BANK OF ENGLAND

MITRE ATT&CK

CALDERA

سازمانها از کجا باید ارزیابی امنیتی و
سپس تیم قرمز را آغاز کنند

مرکز آپا دانشگاه سمنان


# سپاس از توجه تان

**تلاش ما حفظ امنیت سایبری است**

Cert.semnan.ac.ir