سپارا
SPARA

تیم قرمز

Red Team

درباره اسپارا

ما در اسپارا امنیت را بازتعریف کرده‌ایم. راهکارهای ما با شناخت عمیق تهدیدهای امروز و فردا طراحی شده‌اند تا شما یک قدم جلوتر از خطر باشید. اسپارا فقط ارائه‌دهنده خدمات نیست، شریک استراتژیک شما در مسیر رشد ایمن و پایدار است. ما به همراه جمعی از بهترین متخصصان کشور محصولات نوین، خدمات متنوع و راهکارهای جامع امنیت سایبری را به سازمان‌ها ارائه می‌دهیم.

محصولات و خدمات ما:

PAM (Satrap) EDR IAP Isolator Platform MFA VPN

Blue Team Red Team Pentest Purple Team GRC

Application Control

معرفـــی تیم قرمز اسپـــارا

اســتفاده از هر ابزار یــا تکنولوژی جدید در کنــار مزایایی که دارد، می‌تواند راه ورودی جدیدی برای نفوذ و دسترســی به لایه‌های مختلــف ســازمان ایجاد کنــد. مهاجمــان ســایبری و هکرها با استفاده از به‌روزترین روش‌های نفوذ ابتدا نقاط آسیب‌پذیر شما را شناســایی می‌کنند و سپس با اســتفاده از این نقاط به داخل ســازمان نفوذ کرده و خسارات جبران‌ناپذیری به بار می‌آورند. به همین دلیل شناســایی و محــدود کردن این راه‌هــای ورودی به دانش، تجربه و تخصص بالایی نیاز دارد.

تیم قرمز (Red Team) اسپارا با بیش از هشت سال تجربه و دانــش تخصصــی کــه در زمینــه امنیــت ســایبری دارد و بــا پیاده‌ســازی حمله‌های شبیه‌سازی‌شــده، به ســازمان‌ها کمک می‌کند تا آمادگی خودشان را در برابر حملات پیشرفته ارزیابی و با شناســایی نقاط نفوذ و برطرف کردن آن‌ها، به سطح بالایی از امنیت برسند.

درصد موفقیت عواملی که باعث نفوذپـــذیری سازمـــان‌ها مـــی‌شود:

٪۹۵

بروت فــورس

٪۹۵

ذخیــره اطلاعــات محرمانه بــدون رمزنــگاری در ایمیل‌ها و شبکه‌های اجتماعی

٪۹۰

پیکربندی نامناسب تجهیزات امنیتی و سرویس‌ها

٪۹۰

مهندسی اجتماعی

٪۸۰

استفاده از رمزهای عبور ساده

٪۷۵

داشتن الگو برای رمزهای عبور (مانند company name@123)

٪۷۰

عدم به‌روزرسانی سامانه‌ها

RED TEAM

ویژگی‌های تیم قرمز اسپارا

- امکان شبیه‌سازی پیشرفته‌ترین حملات و تهدیدها (APT) متناسب با زیرساخت و ویژگی‌های هر سازمان
- توسعه حملات گوناگون بر اساس پایگاه داده جامعی از تهدیدها (Threat Intelligence)
- به‌کارگیری به‌روزترین ابزارها و امکان توسعه ابزارهای اختصاصی در صورت لزوم
- ارائه گزارش کاملی از روش‌های دسترسی به هدف حمله

شیوه عملکرد تیم قرمز

۱ پس از تعیین هدف حمله از سمت سازمان، تیم قرمز اطلاعاتی درباره سازمان ازجمله زیرساخت و افراد آن جمع‌آوری می‌کند.

۲ تلاش برای ایجاد دسترسی از طریق نفوذ به شبکه، اجرای آزمون نفوذ یا استفاده از دسترسی افراد از طریق مهندسی اجتماعی آغاز می‌شود.

۳ سپس تیم قرمز تلاش می‌کند تا با استفاده از روش‌های مختلف دسترسی خودش را گسترش دهد و به سمت هدف تعیین‌شده حرکت کند.

۴ در پایان و پس از رسیدن به هدف، گزارش کاملی از روند توسه حمله و روش‌های موفق و ناموفق به‌کار گرفته‌شده به سازمان ارائه می‌دهد.

مطالعه این گزارش در کنار حضور تیم آبی در خود سازمان باعث می‌شود تا امکان شناسایی مهاجمانی که در شبکه حضور دارند افزایش پیدا کند و هم‌چنین سیاست‌های امنیتی سازمان بازبینی شود و در صورت نیاز مورد اصلاح قرار بگیرد.

فازهای اجرایی پروژه تیم قرمز

۱ شناسایی

۲ تحلیل آسیب‌پذیری

۳ دسترسی اولیه

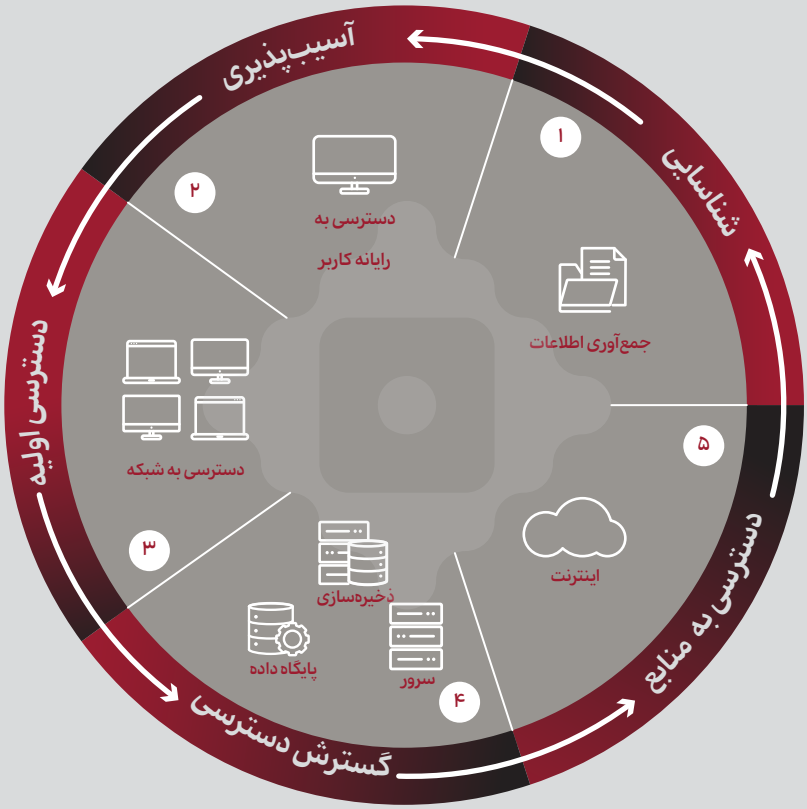
۴ گسترش دسترسی

۵ دسترسی به منابع

۶ استخراج اطلاعات

۷ گزارش‌دهی

بررسی یکی از سناریوهای حمله تیم قرمز



مزایای تیم قرمز اسپارا

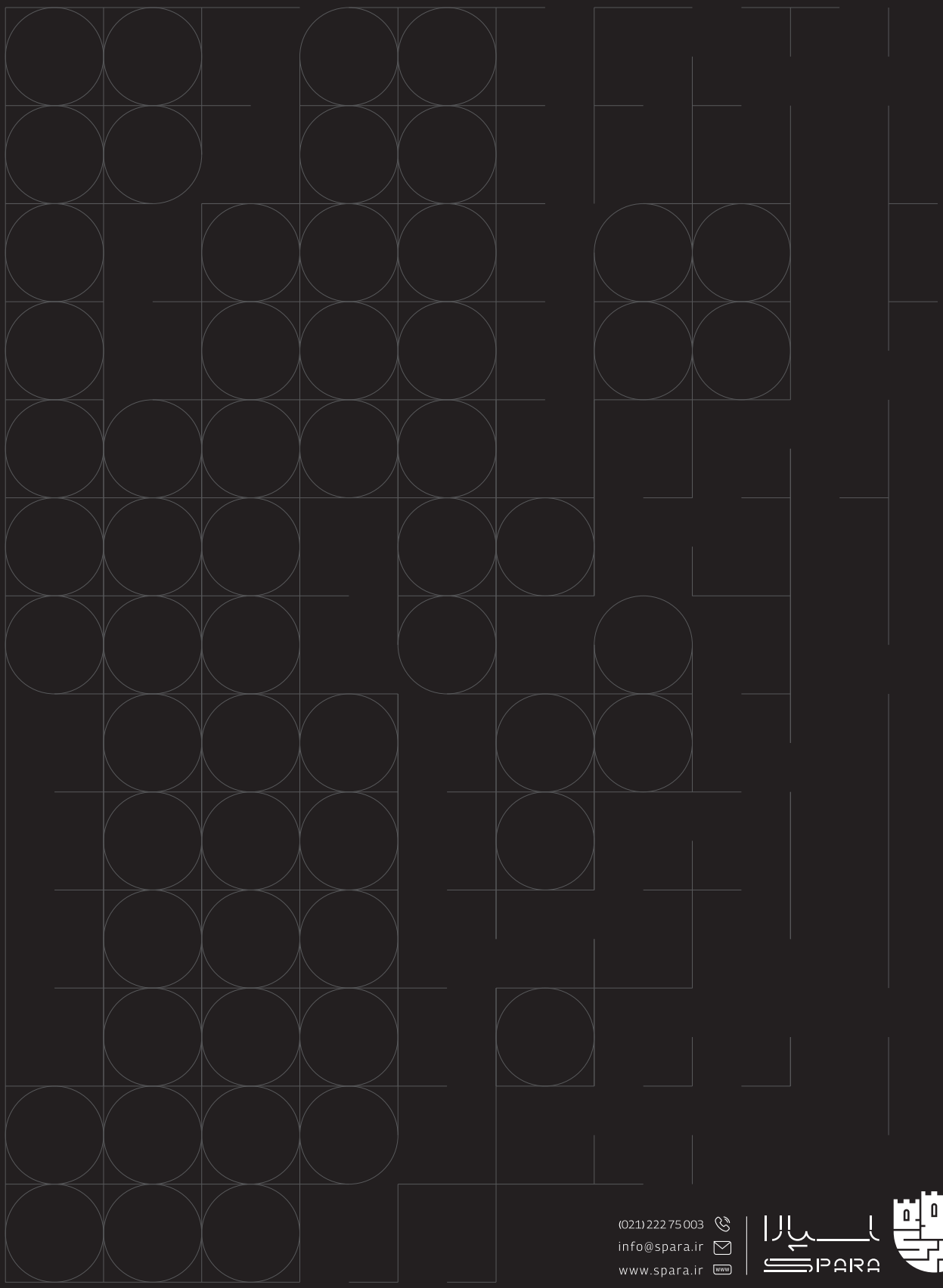
- شناسایی نقاط ضعف در طراحی و توسعه معماری امنیتی
- ارزیابی عملکرد ساختار و زیرساخت امنیتی سازمان
- درک بهتر تاثیرات رخدادهای امنیتی روی کسب‌وکار سازمان
- ارزیابی میزان آمادگی متخصصین امنیتی سازمان در برابر تهدیدات سایبری APT
- شناسایی آسیب‌پذیری‌های موجود در سامانه‌ها و سیستم‌عامل‌ها
- ایجاد یک فرصت آموزش عملی برای تیم SOC و CERT سازمان (یک دوره آموزشی نیز در انتهای عملیات تیم قرمز برای کارشناسان و مدیران سازمان برگزار خواهد شد)
- آشنایی با پتانسیل تخریبی تیم‌های APT و بهره‌برداری از این دانش در تصمیمات آینده سازمان

تفاوت خدمات تیم قرمز و آزمون نفوذ

تیم قرمز	آزمون نفوذ
برای سنجش اثربخشی راهکارهای دفاعی شما، یک یا چند سناریو حمله واقعی را روی سازمان شبیه‌سازی می کند.	تمرکز خود را روی پیدا کردن آسیب‌پذیری‌های فنی قرار می‌دهد که به‌شکل پیش‌فرض در زیرساخت فناوری اطلاعات شما وجود دارد.
مانند هکرهای واقعی، بدون هیچ اطلاعات و دانشی درباره سازمان، حملات شبیه‌سازی‌شده‌اش را انجام می‌دهد.	نیاز به یک سری اطلاعات مانند آدرس‌های IP یا اطلاعات احراز هویت به‌منظور دسترسی به یک سامانه دارد.
فرایندهای امنیتی سازمان را به شکل جامع بررسی می‌کند.	در یک محیط ایزوله و به شکل کنترل‌شده انجام می‌شود.
در نهایت باید گفت که این دو خدمت مکمل هم هستند و وجود آن‌ها برای حفظ امنیت یک سازمان در برابر تهدیدات سایبری پیچیده، بسیار حیاتی است.	

RED TEAM

مشتریان اسپارا



(021) 222 75 003
info@spara.ir
www.spara.ir

اسپارا
SPARA