سپارا
SPARA

تیم بنفش
Purple Team

PURPLE 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

آمار و ارقامی از تیم بنفش

کمتر از ۱۲ دقیقه

میانگین زمان شناسایی تهدید

کمتر از ۴۵ دقیقه

میانگین زمان مهار تهدید

کمتر از ۱۰ دقیقه

تشخیص اولین مرحله Lateral Movement

۵ دقیقه

کمترین زمان شناسایی یک حمله واقعی

معرفی خدمت تیم بنفش

سازمان‌ها امروز با مجموعه‌ای از تهدیدهای پیچیده و چند لایه روبه‌رو هستند که اغلب فراتر از توان ابزارهای امنیتی سنتی عمل می‌کنند. برخی از مهم‌ترین چالش‌ها شامل موارد زیر است:

- عدم شناسایی حملات خاموش مانند بدافزارهای بدون فایل، **APT** ها.
- کمبود ارتباط بین تیم‌های تهاجمی و تدافعی که باعث می‌شود درس‌آموخته های حملات واقعی به سیاست‌های دفاعی تبدیل نشوند.
- پیچیدگی زیرساخت‌ها (شبکه، سرویس‌ها، Active Directory) و پیکربندی‌های ناامن که مهاجم از آن‌ها به‌عنوان نقطه ورود استفاده می‌کنند.
- نبود دید یکپارچه نسبت به رفتار مهاجمان و ناتوانی در تطبیق آن با چهارچوب‌هایی مانند **MITRE ATT&CK**.
- فقدان فرایند فارنزیک حرفه‌ای که بتواند علت حادثه، مسیر نفوذ و آسیب را با دقت علمی بازبینی کند.

تیم بنفش اسپارا با هدف ارتقای امنیت سایبری سازمان از طریق ترکیبی از رویکردهای تهاجمی و تدافعی فعالیت می‌کند. این تیم با همکاری نزدیک با تیم‌های قرمز و آبی، تلاش دارد تا با شبیه‌سازی حملات واقعی، شناسایی و رفع آسیب‌پذیری‌ها و بهبود مکانیزم‌های دفاعی، سطح امنیت شبکه و سرویس‌های سازمان را به حداکثر برساند.

رویکرد تیم بنفش اسپارا

Attack-Driven Defense

دفاع مبتنی بر نتایج حملات واقعی

Hypothesis-Based Hunting

شکار تهدید بر اساس فرضیه‌های عملیاتی و رفتار مهاجمان

Continuous Validation

اعتبارسنجی مداوم کنترل‌های امنیتی

Forensic-Integration Hardening

هر حادثه یا نشانه، ورودی‌های مستقیم فرایند امن‌سازی هستند

خدمات ارائه‌شده در تیم بنفش اسپارا

1

شکار تهدیدات (Threat Hunting)

تکنیک‌ها و تاکتیک‌های مورد استفاده:

رویکرد مبتنی بر فرضیه:

- مدل‌سازی فرضیه‌های حمله بر مبنای اطلاعات تهدید
- فرضیه‌سازی بر اساس MITRE TTPs برای شناسایی تکنیک‌های مهاجم در محیط سازمان

تحلیل داده‌های رفتاری و منابع لاگ:

- تحلیل عمیق لاگ‌های SIEM، EDR، Windows Event Logs، Sysmon
- تحلیل ترافیک شبکه برای شناسایی C2، Beaconing، DGA patterns، Communication
- شناسایی Process Injection، anomalous parent-child processes و Thread hijacking

PURPLE TEAM

جستجوی فعال نشانه‌های مهاجم

- شناسایی اجرای بدون فایل
- بررسی Persistence Methods:
  - Registry Run Keys
  - Scheduled Tasks
  - WMI Subscription
  - DLL Search Order Hijacking
- تشخیص تکنیک‌های Defense Evasion مانند:
  - Obfuscation
  - Deception
  - Log Clearing
  - Timestomping

تحلیل مسیر حمله

- تطبیق یافته‌ها با MITRE Enterprise ATT&CK
- شناسایی Lateral Mouvement بر اساس SMB، RDP، WinRM، PsExec

اقدامات واکنش و اصلاح

- قرنطینه سیستم آلوده
- تنظیم قوانین IOA/IOC در SIEM و EDR
- اعمال کنترل‌های سخت‌سازی مبتنی بر نتایج Hunting

2

امن‌سازی شبکه (Network Hardening)

تکنیک‌ها و تاکتیک‌های مورد استفاده:

فاز شناخت و اکتشاف

- اسکن پورت و سرویس با Nmap، Masscan
- تشخیص misconfigurationهای فایروال و روتینگ
- Mapping کامل Topology و Asset Inventory

تحلیل سطح حمله

- شناسایی exposed services، پروتکل‌های ناامن
- کشف Shadow IT و دارایی‌های که خارج از CMDB هستند
- سواستفاده از Misconfiguration ACLها یا VLANها

تست نفوذ شبکه

- بهره‌برداری از آسیب‌پذیری‌های شناخته‌شده با Nessus/Nexpose
- تست Lateral Movement بر اساس ARP Poisoning، Pass-the-Hash و Kerberoasting
- تست مقاومت IDS/IPS در برابر evasion techniques مانند fragmentation و encoding

مانیتورینگ و تحلیل ترافیک

- تحلیل پروتکل با Zeek
- شخیص حملات Port scanning، anomalous flow و brut-force
- استفاده از Suricata برای Rule-based detection و NIDS correlation

تقویت امنیت شبکه

- طراحی و اصلاح Segmentation و Micro-Segmentation
- تقویت Access Control و Zero Trust Network Access
- اصلاح Rule-set فایروال‌ها، IPS، WAF

3

امن‌سازی سرویس‌ها به‌خصوص Active Directory

تکنیک‌ها و تاکتیک‌های مورد استفاده:

تحلیل ساختار AD و کشف مسیرهای حمله

- استخراج گراف AD با BloodHound و تحلیل Neo4j
- شناسایی حساب‌های با Privilege بالا و Misconfiguration Delegation
- شناسایی Shadow Admins

شبیه‌سازی حملات

- Kerberoasting، AS-REP Roasting
- Pass-the-Ticket، Pass-the-Hash
- Exploiting unconstrained delegation
- DC Sync/ DC Shadow

تحلیل پروتکل‌ها و سرویس‌ها

- بررسی امنیت NTLM، LDAP، SMB Signing، Kerberos
- بررسی دسترسی‌های GPOها و Misconfigured policies

امن‌سازی و اقدامات اصلاحی

- حذف پروتکل‌های ناامن، فعال‌سازی SMB Signing
- پیاده‌سازی Tiering Model برای حساب‌ها
- محدودسازی Local Adminها
- اعمال اصول Least Privilege، JIT/JEA

4

فارنزیک دیجیتال

تکنیک‌ها و تاکتیک‌های مورد استفاده:جمع‌آوری شواهد

- Imaging دیسک با ابزارهای FTK/EnCase
- Memory Forensics با Volatility و Rekall
- استخراج ترافیک شبکه و PCAPها

تحلیل فارنزیکی سیستم

- بررسی Execution Artifacts:
  Prefetch-
  ShimCach-
  SRUM-
- تحلیل فایل‌های مشکوک، DLL، Malicious Scripts
  Injection
- تحلیل Persistence artifacts

تحلیل فارنزیکی شبکه

- شناسایی ارتباطات C2
- تحلیل Beaconing patternها
- شناسایی Exfiltration (DNS tunneling, HTTPS exfil, SMB exfil)

بازسازی زنجیره حمله

- تطبیق با MITRE ATT&CK و Cyber Kill Chain
- شناسایی نقطه ورود
- تحلیل آسیب‌پذیری exploited و داده‌های سرقت‌شده

خروجی و اقدامات اصلاحی

- ارائه گزارش Incident Timeline
- انجام Remediation Plan
- ارائه Ruleهای امنیتی برای SIEM/EDR

مزیت‌های تیم بنفش اسپارا

یکپارچه‌سازی رویکردهای تهاجمی و تدافعی

استفاده از ابزارهای پیشرفته عملیاتی EDR/Forensics) /BloodHound/ (Zeek

تسلط کامل به چهارچوب MITRE ATT&CK

طراحی سناریوهای اختصاصی حمله برای مشتری

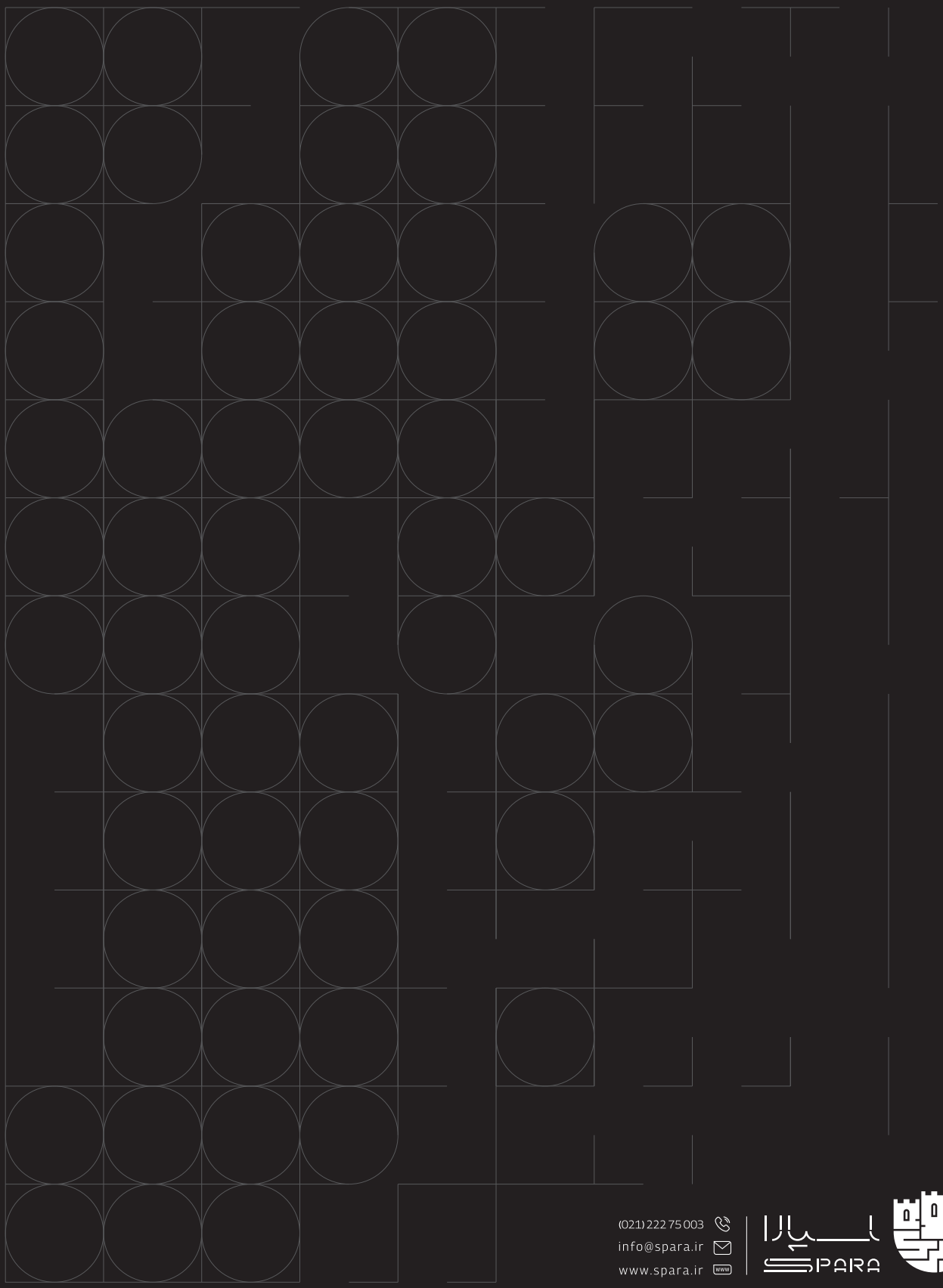
بهبود مداوم تاب‌آوری سازمان

مستندسازی حرفه‌ای

شناسایی تهدیدات فراتر از توان ابزارهای امنیتی

رویکرد بومی‌سازی شده

مشتریان اسپارا



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

اسپارا
SPARA