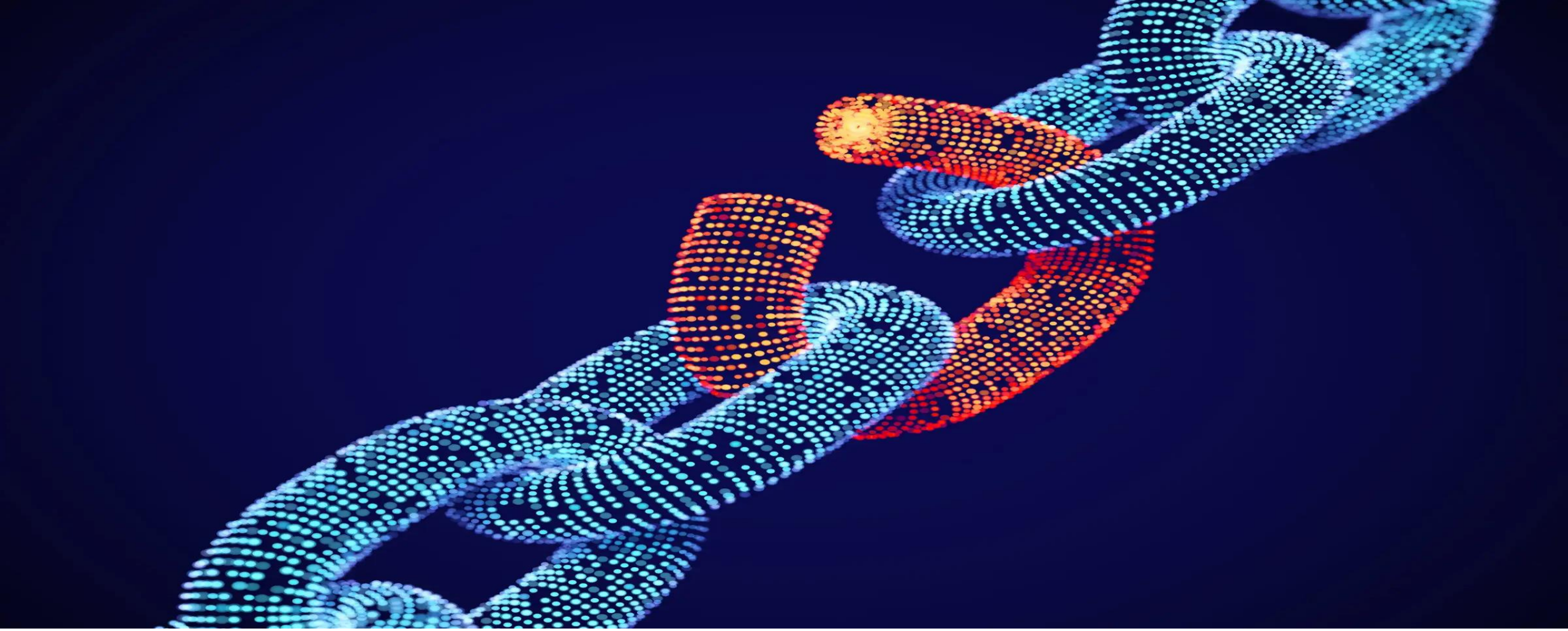
شرکت امن پرداز شن هوشمند فرداد


شرکت امن پرداز شن هوشمند فرداد

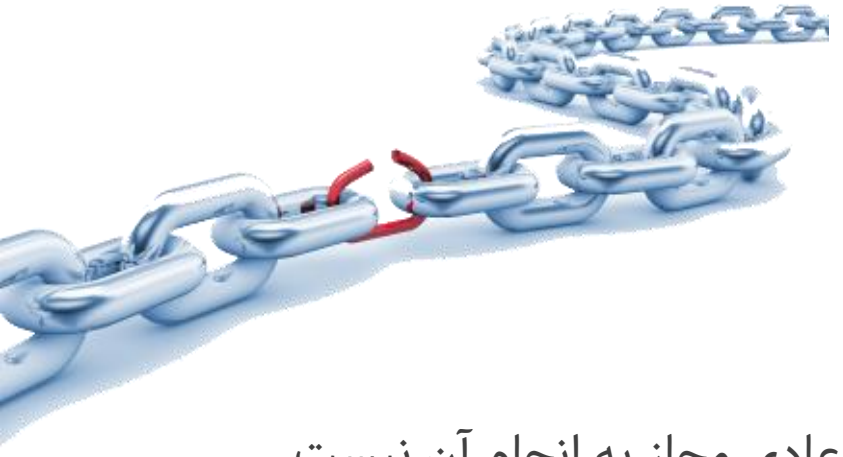

شرکت امن پرداز شن هوشمند فرداد



آسیب‌پذیری

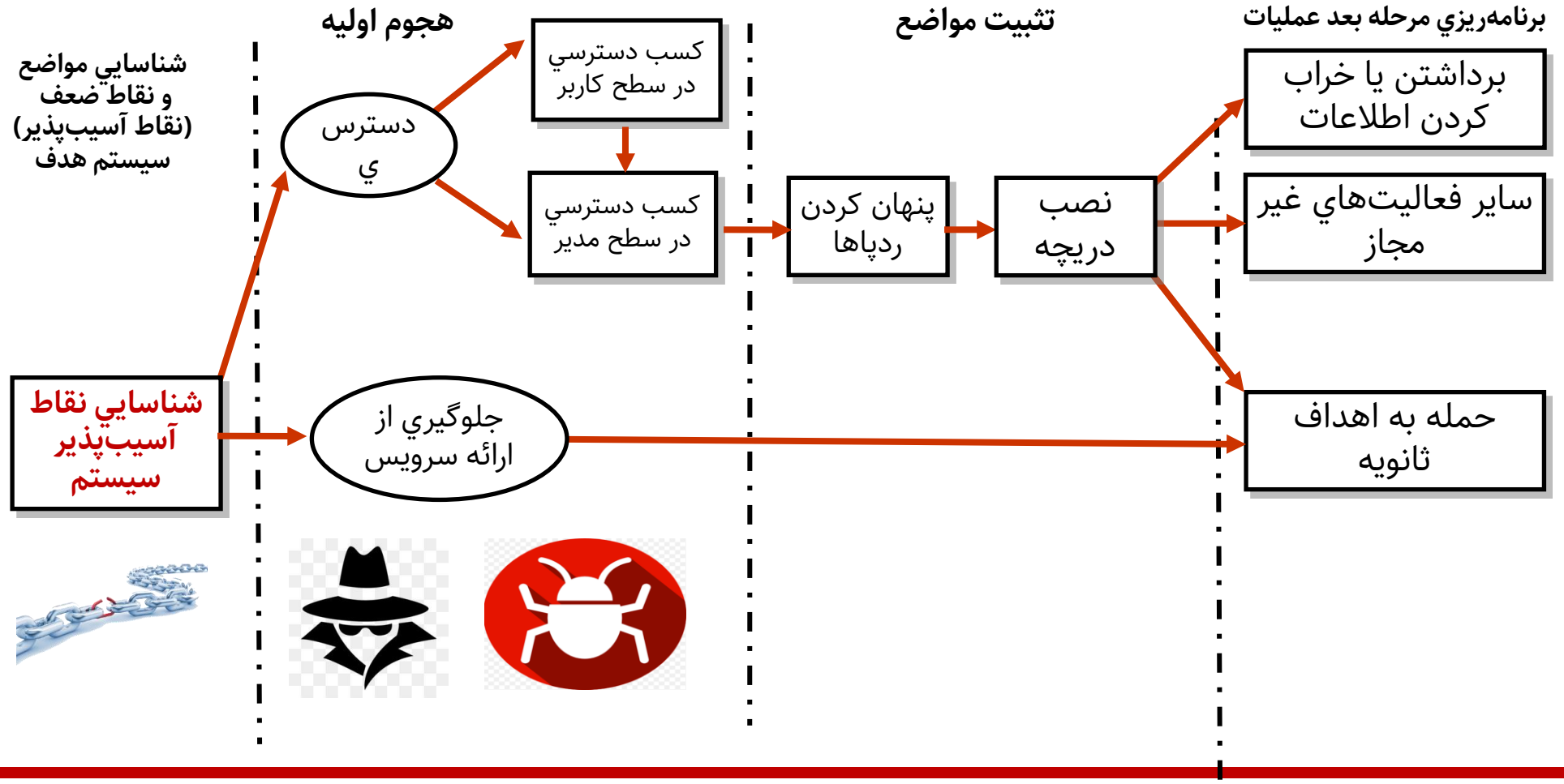
آسیب‌پذیری (Vulnerability)

هرگونه ضعف در یکی از مولفه‌های شبکه (**سخت‌افزار**، **نرم‌افزار**، **پیکربندی** یا **امنیت فیزیکی**) که می‌تواند **مستقیماً** برای دسترسی یافتن به سیستم یا شبکه‌ای مورد سوءاستفاده قرار گیرد.



ضعفی از سیستم که به نفوذگر اجازه می‌دهد تا کاری را انجام دهد که در حالت عادی مجاز به انجام آن نیست.

(روند کلي انجام یک حمله در محیط شبکه‌های رایانه‌ای)



انواع مهاجمان

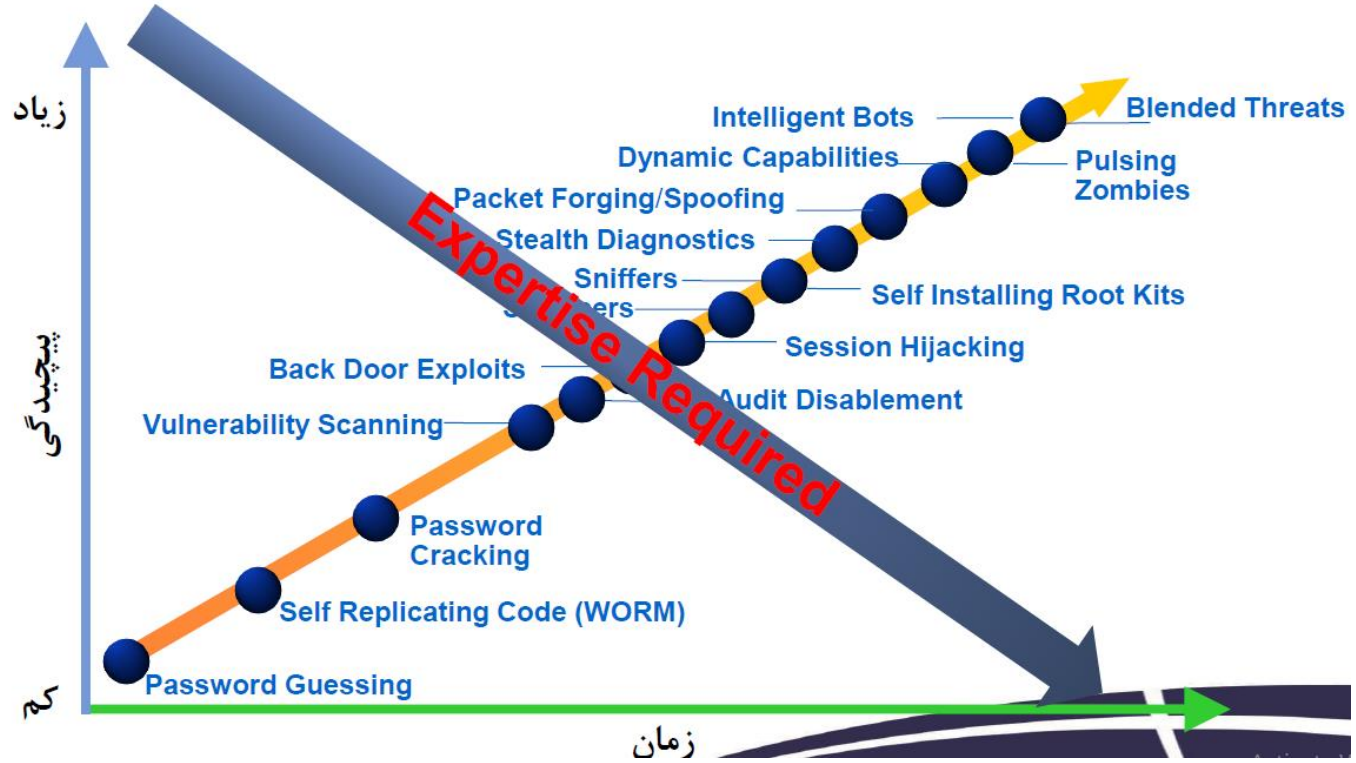
مهاجمان بازیگوش

مهاجمان مصمم

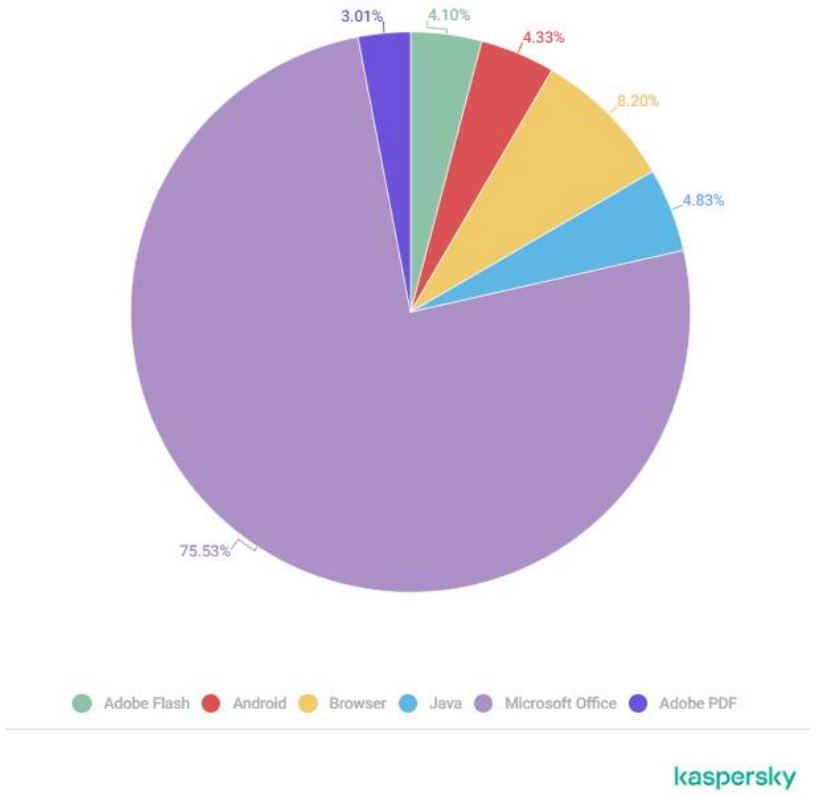
سیر تکاملی حملات

پیچیدگی بیشتر ابزارهای نفوذ

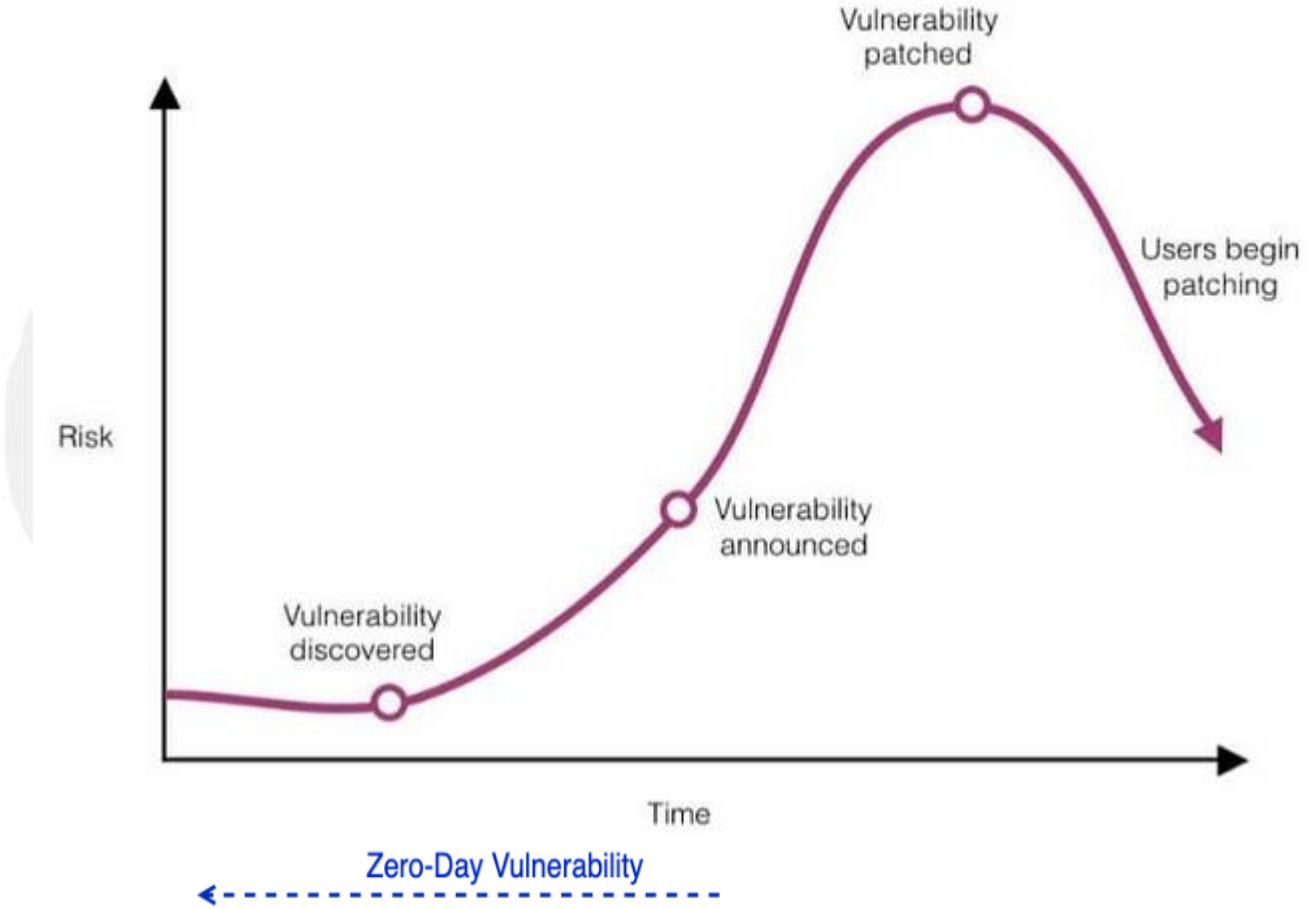
ساده‌تر شدن استفاده از آنها



محبوب‌ترین برنامه‌ها برای اهداف خرابکارانه



چرخه حیات آسیب‌پذیری



چند نمونه آسیب‌پذیری مطرح

- CVE 2022-26937
- CVE 2022-22012
- CVE 2022-29130

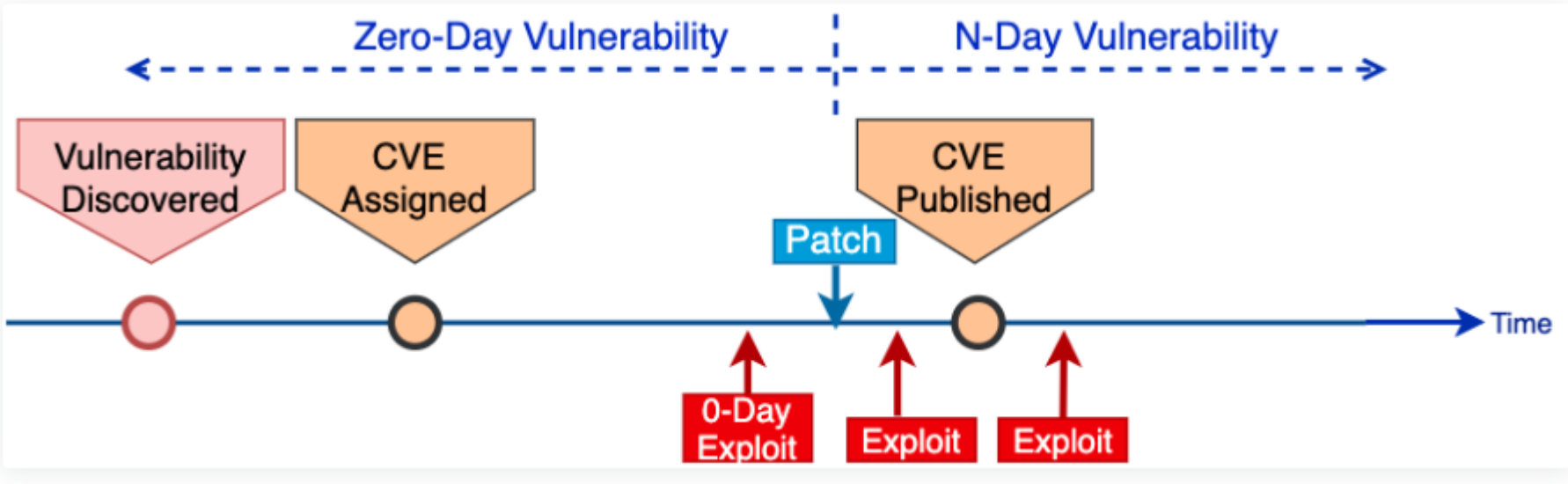
شهرداری تهران

- استفاده از آسیب‌پذیری AD در انتشار

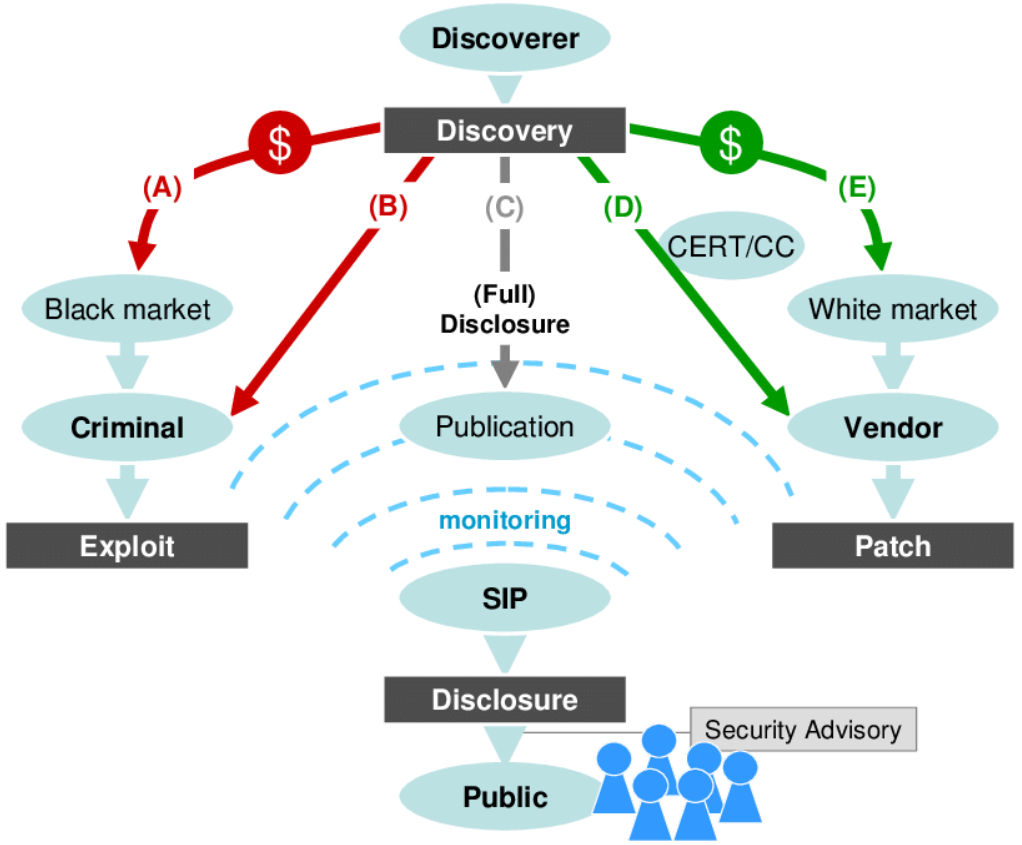
فولاد مبارکه

کشف/ وصله /بهره برداری آسیب‌پذیری

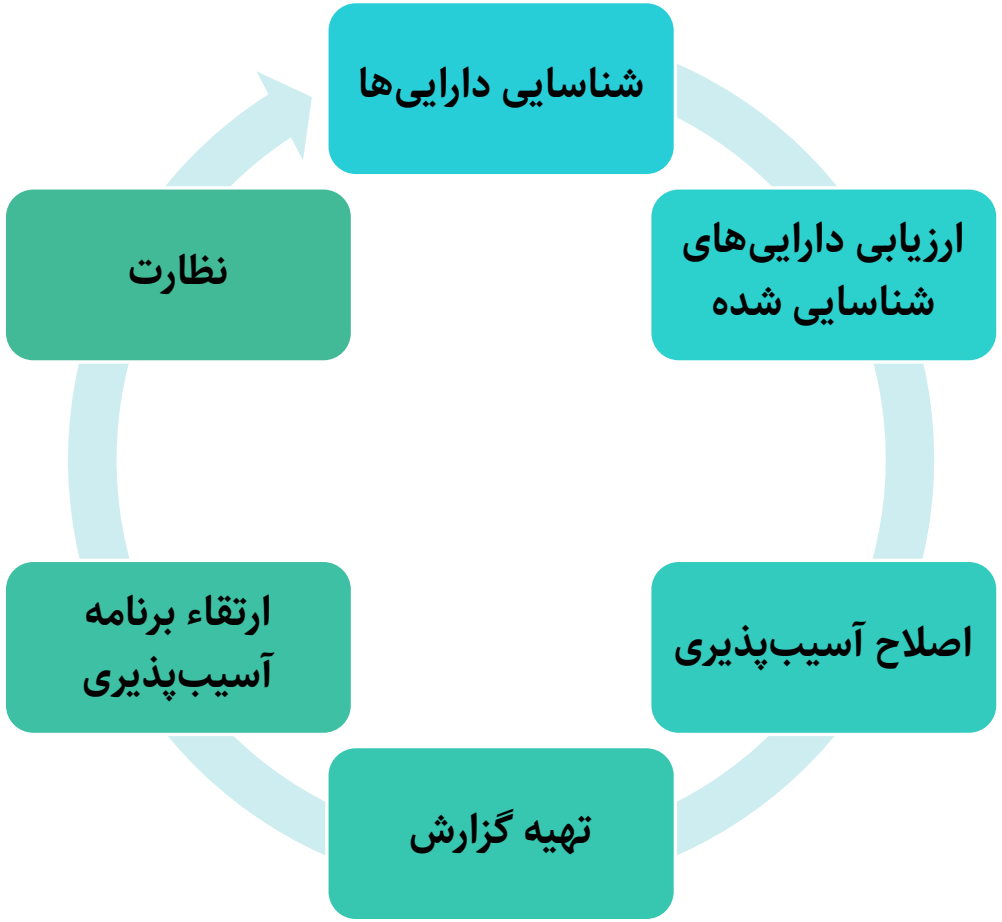
- 14% are zero-day (published before the vendors release the patch), 23% are published within a week after the patch release and 50% are published within a month after the patch release. On average, an exploit is published 37 days after the patch is released. Patch as soon as possible – the risk of a vulnerability being exploited increases quickly after vendors release the patches.

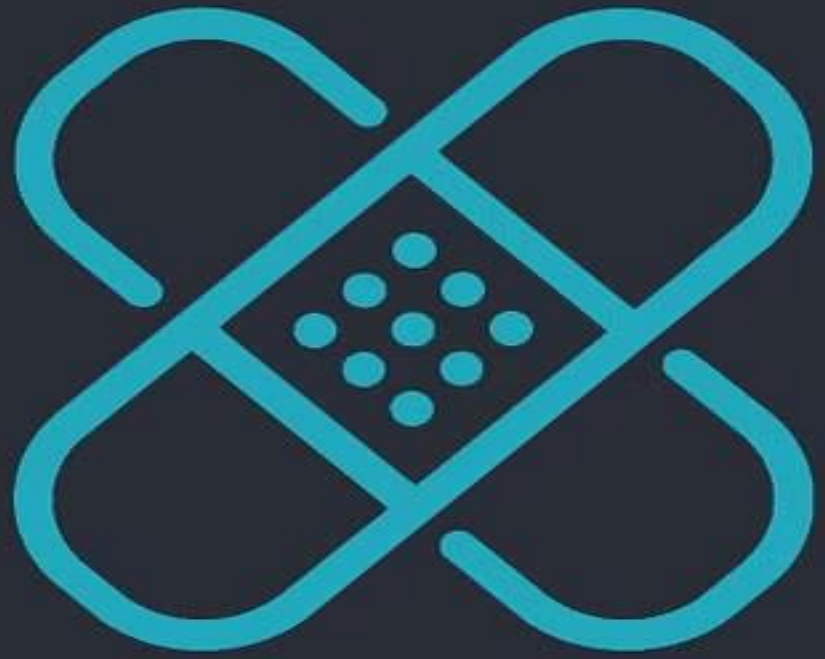


چرخه حیات آسیب‌پذیری و اکوسیستم امنیت سایبری



مراحل مهم در مدیریت آسیب پذیری





مدیریت وصله

گزارش مایکروسافت در مورد مدیریت وصله

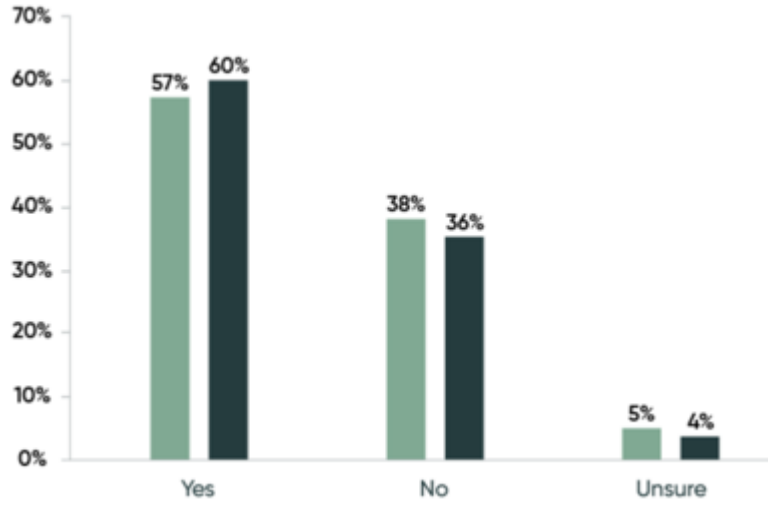
More than half of known network vulnerabilities found in 2021 were found to be lacking a patch. Plus, 68 percent of organizations impacted by ransomware did not have an effective vulnerability and patch management process, and many had a high dependence on manual processes versus automated patching capabilities. With today's threat landscape, it was only a matter of time before this zero-day vulnerability was exploited.

Microsoft

نگاهی به مطالعات در زمینه مدیریت وصله

60% of data breaches are attributed to poor patch management

The average time to apply, test and fully deploy patches is 97 days. The findings reveal the difficulties in keeping endpoints effectively patched.



servicenow

Ponemon INSTITUTE

زنجیره‌ی سرویس های امنیتی

PROACTIVE

- **Patch Mng**
- Config Mng
- Auditing
- Pentest
- Hardening
- Red Teams

PROTECT

- UTM
- WAF
- Next Gen Firewall
- Firewall

DETECT, RESPOND

- SIEM
- SOAR
- Antiviruses
- EDR
- Threat Hunting
- Incidence Response

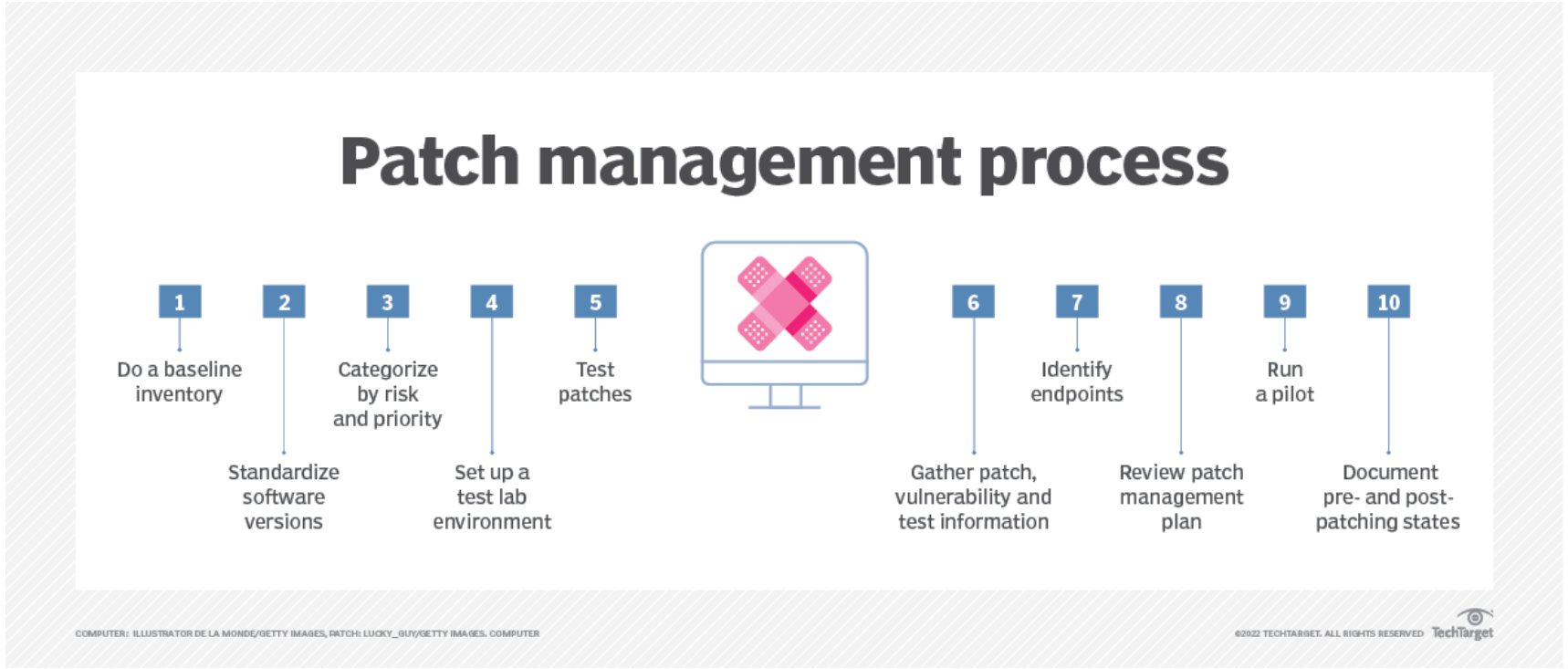
RECOVER

- Forensics
- Backups

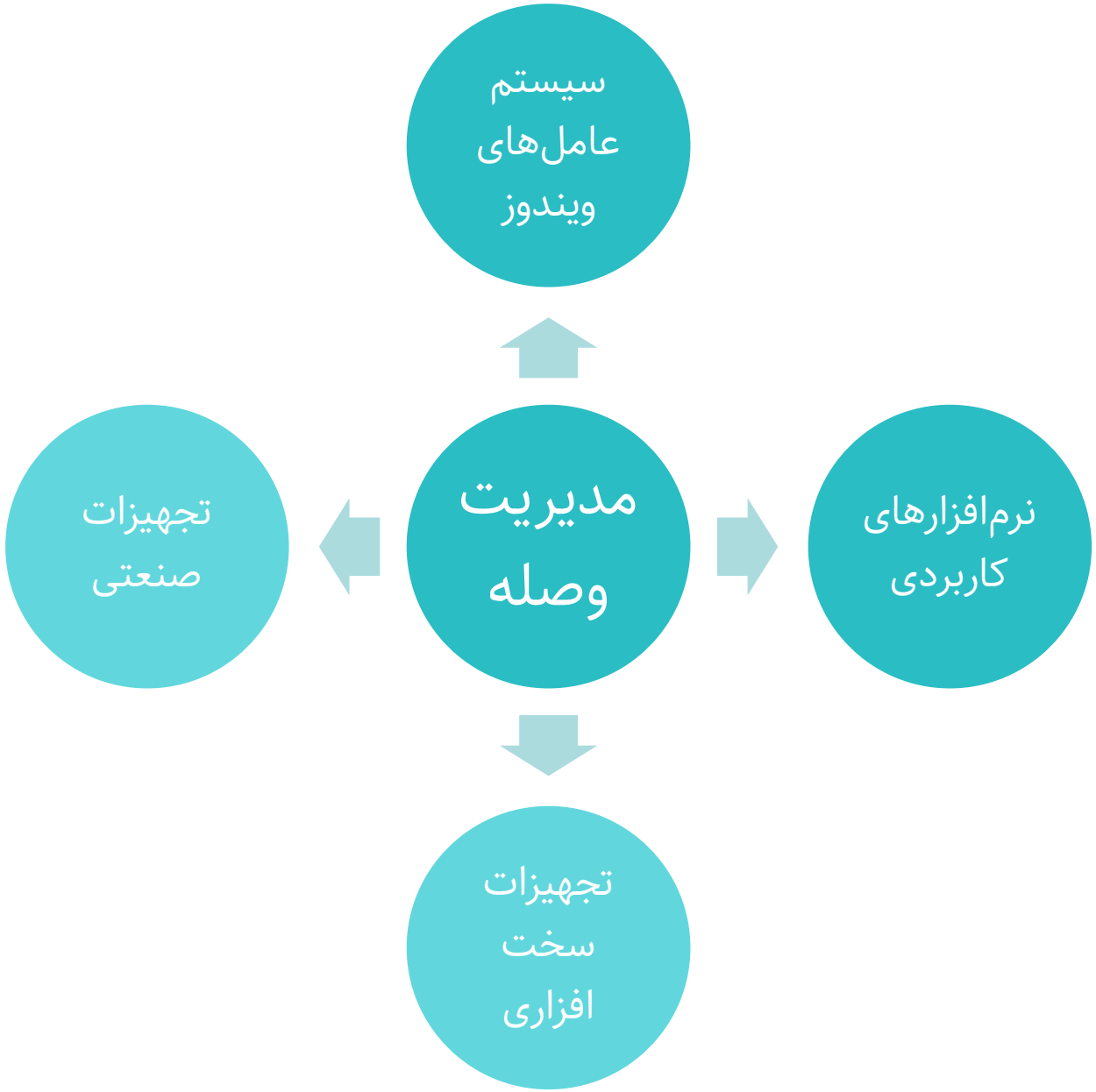
سوالات مهم

- چه تعدادی از سیستم‌ها به‌روز نیستند؟
- مدت زمان نصب وصله پس از انتشار؟
- چه تعدادی از سیستم‌ها و در چه زمانی به‌روز شده‌اند؟
- از کجا وصله‌های مطمئن دریافت کنم؟
- زمانبدی اجرا و اعمال سیاست برای به‌روز کردن سیستم‌ها را چگونه انجام دهم؟
- در صورت قطع و یا بروز اختلال در ارتباط اینترنت چگونه سامانه‌ها را به روز کنم؟
- چگونه اطمینان پیدا کنم 100 درصد سامانه‌ها به روز شده اند؟
- .....

فرآیند مدیریت وصله



حیطه کاربری مدیریت وصله



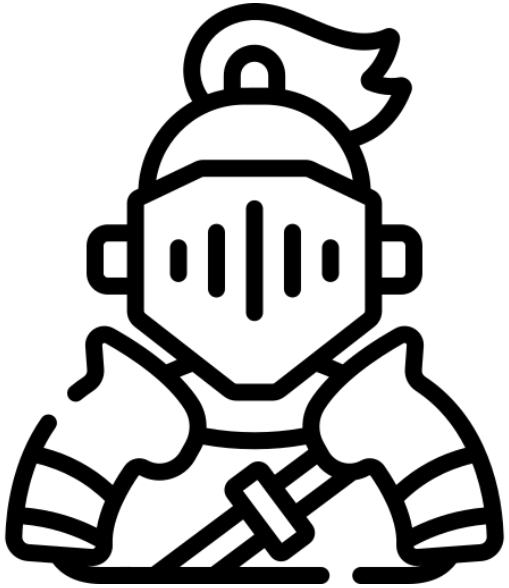
شرکت امن پردازش هوشمند فرداد
AMN PARDAZESH HOUSHMAND FARDAD Co.

سامانه مدیریت وصله

نصب و بروزرسانی خودکار سیستم‌عامل و انواع نرم‌افزارهای کاربردی به صورت متمرکز

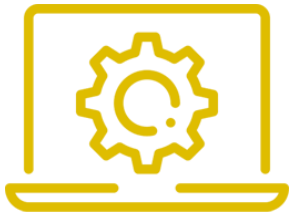
چرا سامانه مدیریت وصله فربد

- گزارش‌های غلط برخی سامانه‌ها
- خدمات محصول
- مزایای محصول بومی
  - ✓ اعتماد به وصله‌های ارسالی و شخصی‌سازی



ویژگی‌های اصلی

پویش خودکار و
تشخیص نیازها

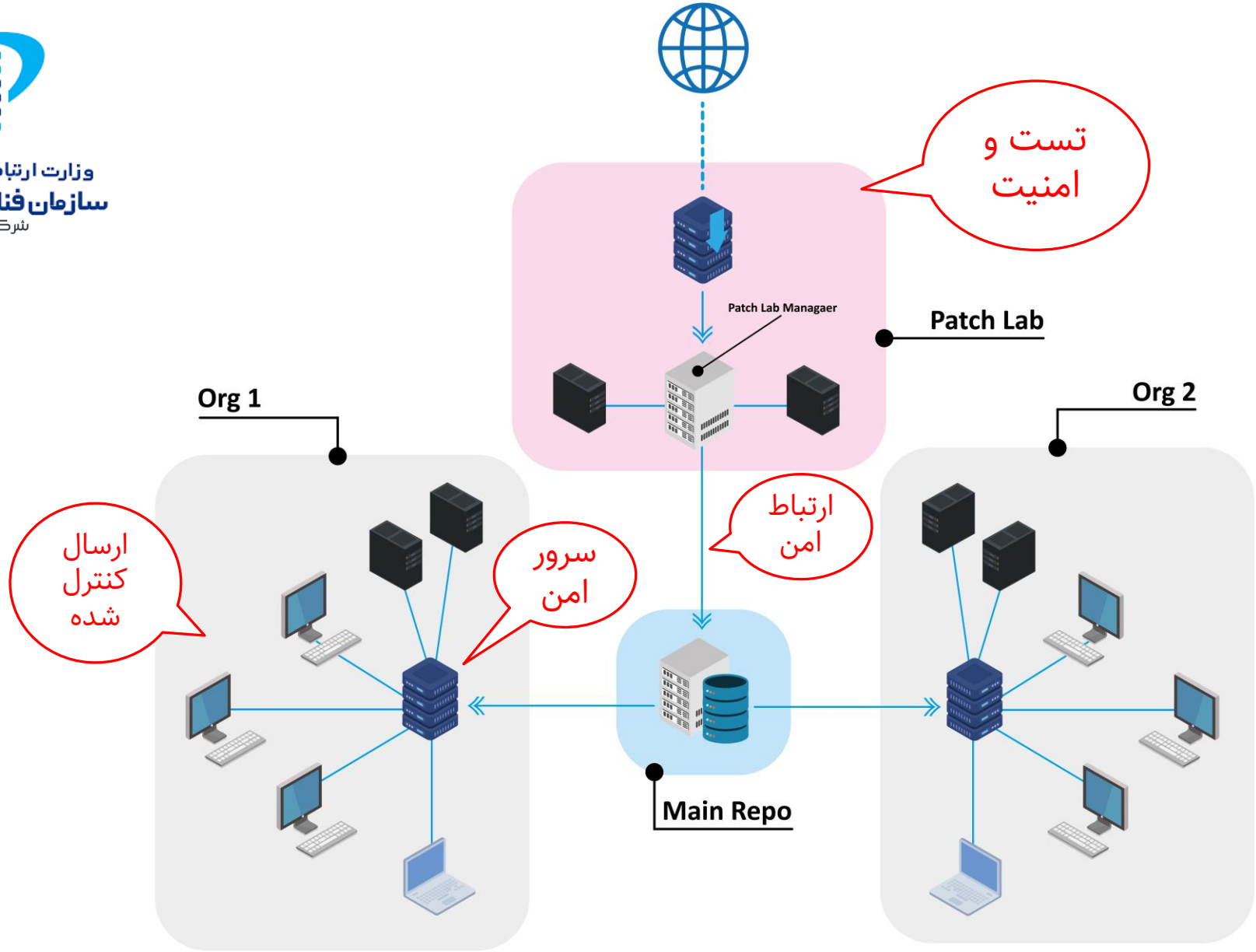


سیاست‌گذاری در نصب
وصله و بیان استثناها

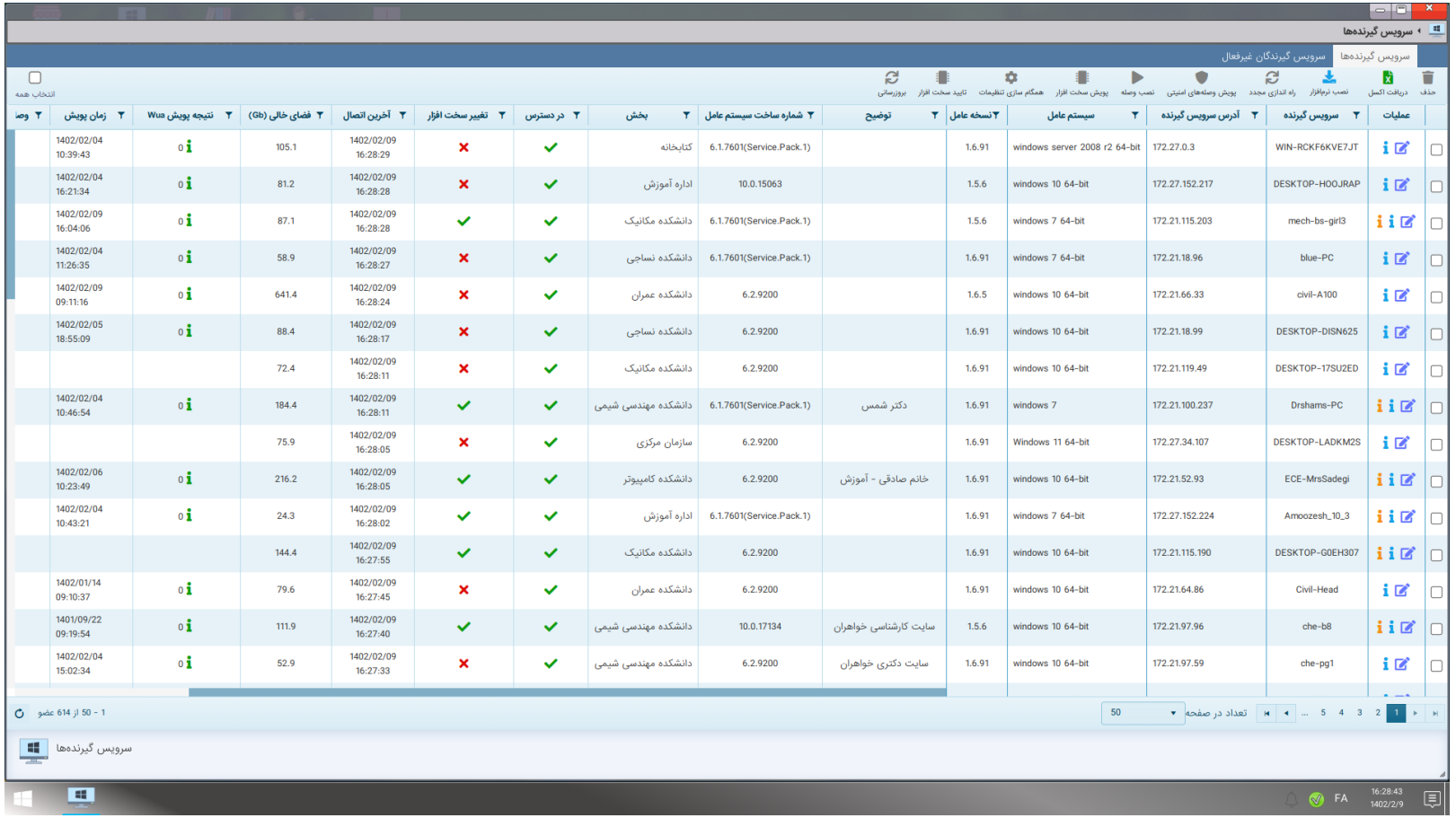
تست قبل از نصب

گزارش گیری

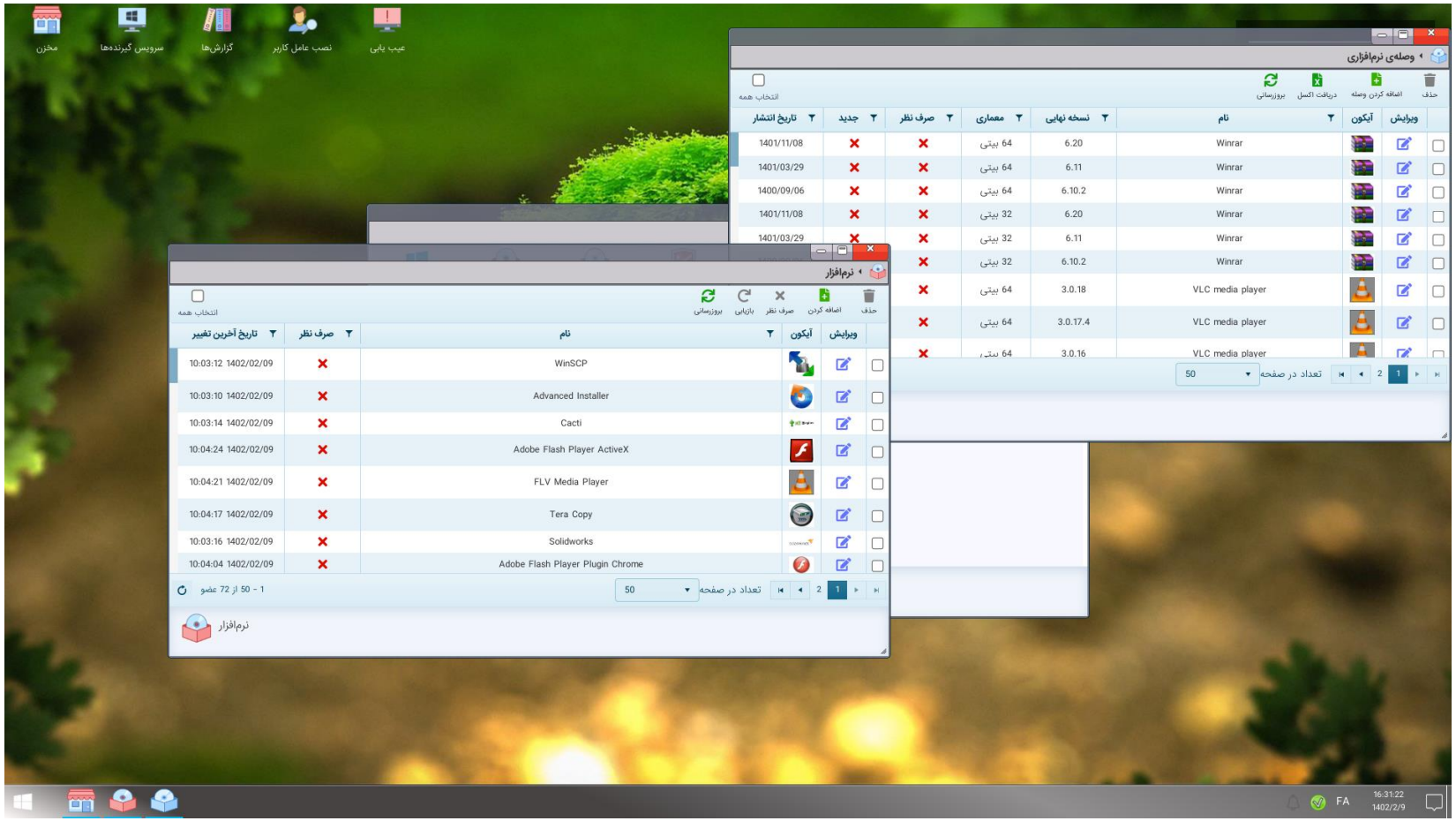
وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
شرکت امن پردازش هوشمند فرداد



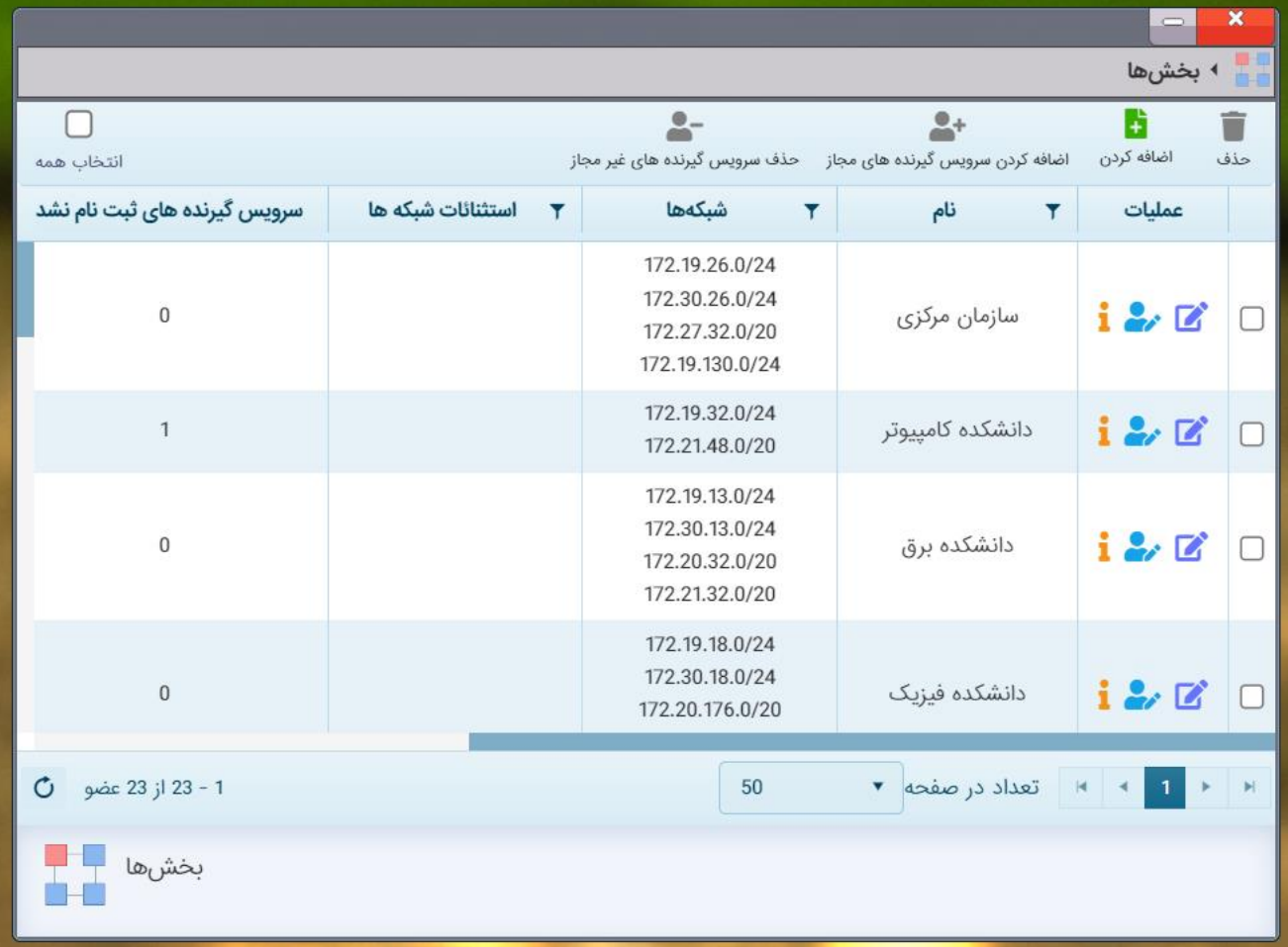
اجرای بلادرنگ دستورات پویش و نصب از راه دور

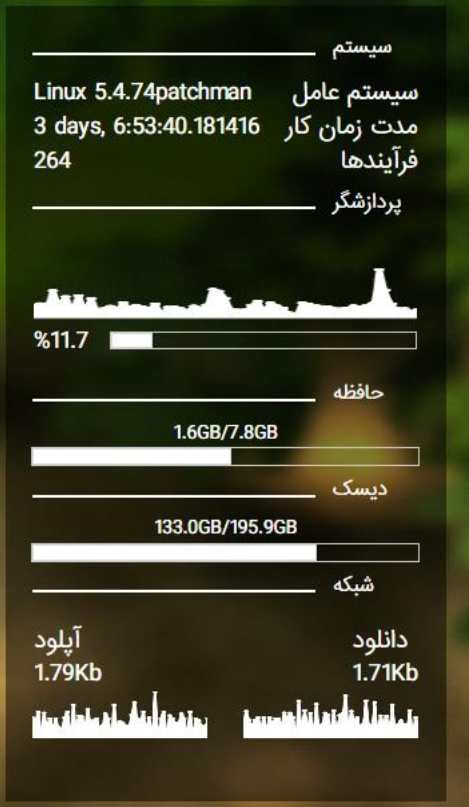


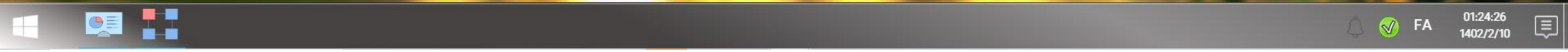
به روزرسانی انواع سیستم‌عامل‌ها و نرم‌افزارها



بخش‌بندی و مدیریت کاربران







گزارش نرم‌افزارها و سخت‌افزارهای سازمان

شرکت امن پردازش هوشمند فرداد

ویژگی‌های سازمانی

سازمان‌های کوچک

- اتصال به اکتیو دایرکتوری

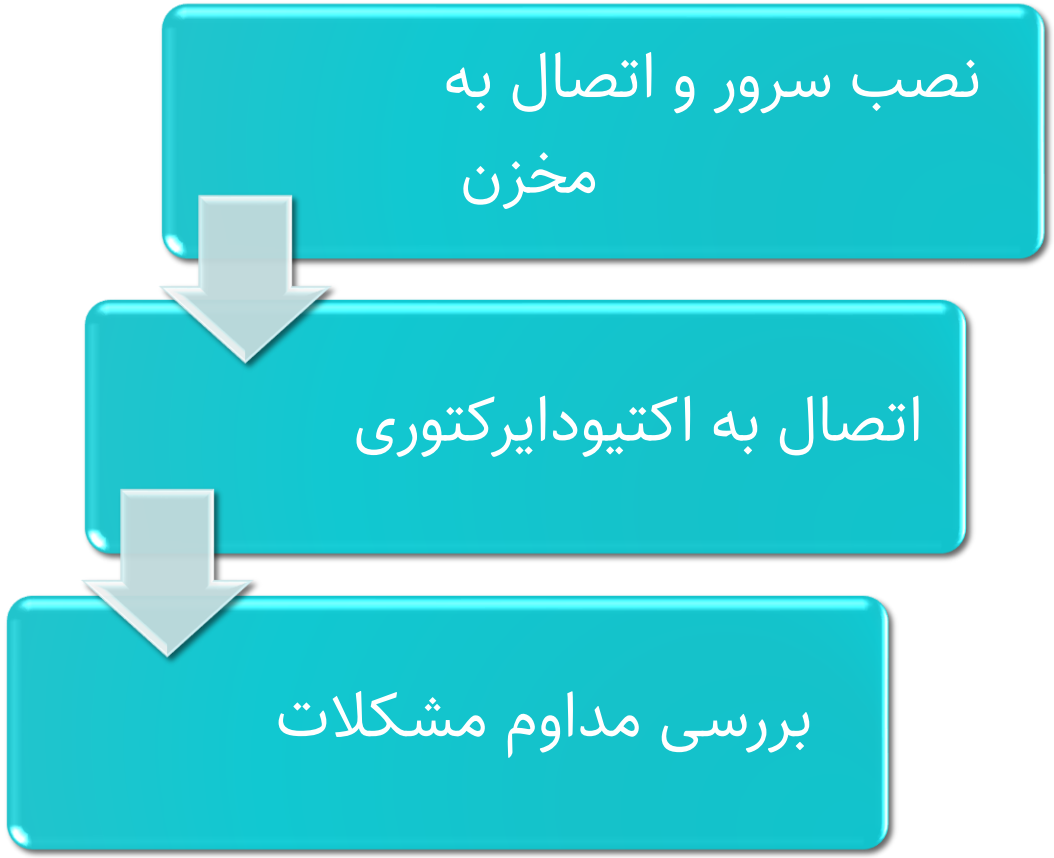
سازمان‌های متوسط

- تعریف بخش‌ها و زیرشبکه
- مدیریت کاربران

سازمان‌های بزرگ

- ساختار سلسه مراتبی
- مخازن جایگزین

استقرار


نصب سرور و اتصال به مخزن
اتصال به اکتیودایرکتوری
بررسی مداوم مشکلات

سوالات متداول

- نرم‌افزارهای کرک
- تجهیزات شبکه مانند ESXI، ماشین‌های آن
- مشکلاتی که با به روزرسانی پیش می‌آید؟
- ایجاد استثنا در به‌روزرسانی ممکن است؟
- به روزرسانی سرورها
- لینوکس

پیش نمایش

شرکت امن پرداز شن هوشمند فرداد

با تشکر از توجه شما

؟