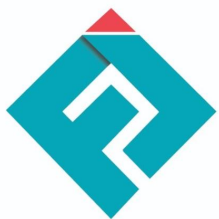
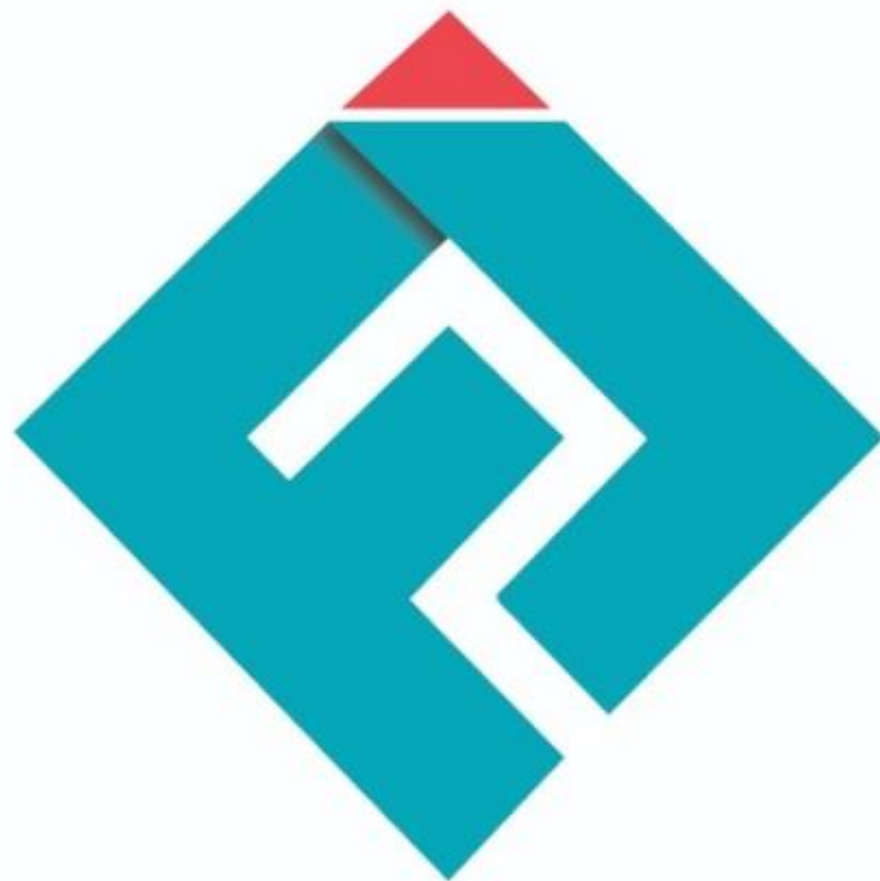


شرکت آمان پردازش هوشمند فرداد

کتابخانه دیجیتال



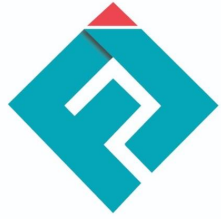
شرکت امن پردازش هوشمند فرداد



شرکت امن پردازش هوشمند فرداد

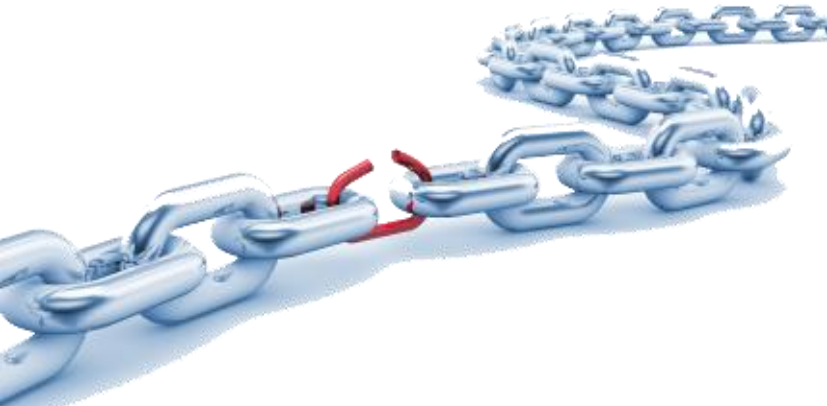


آسیب پذیری

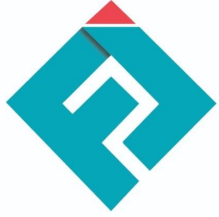


آسیب پذیری (Vulnerability)

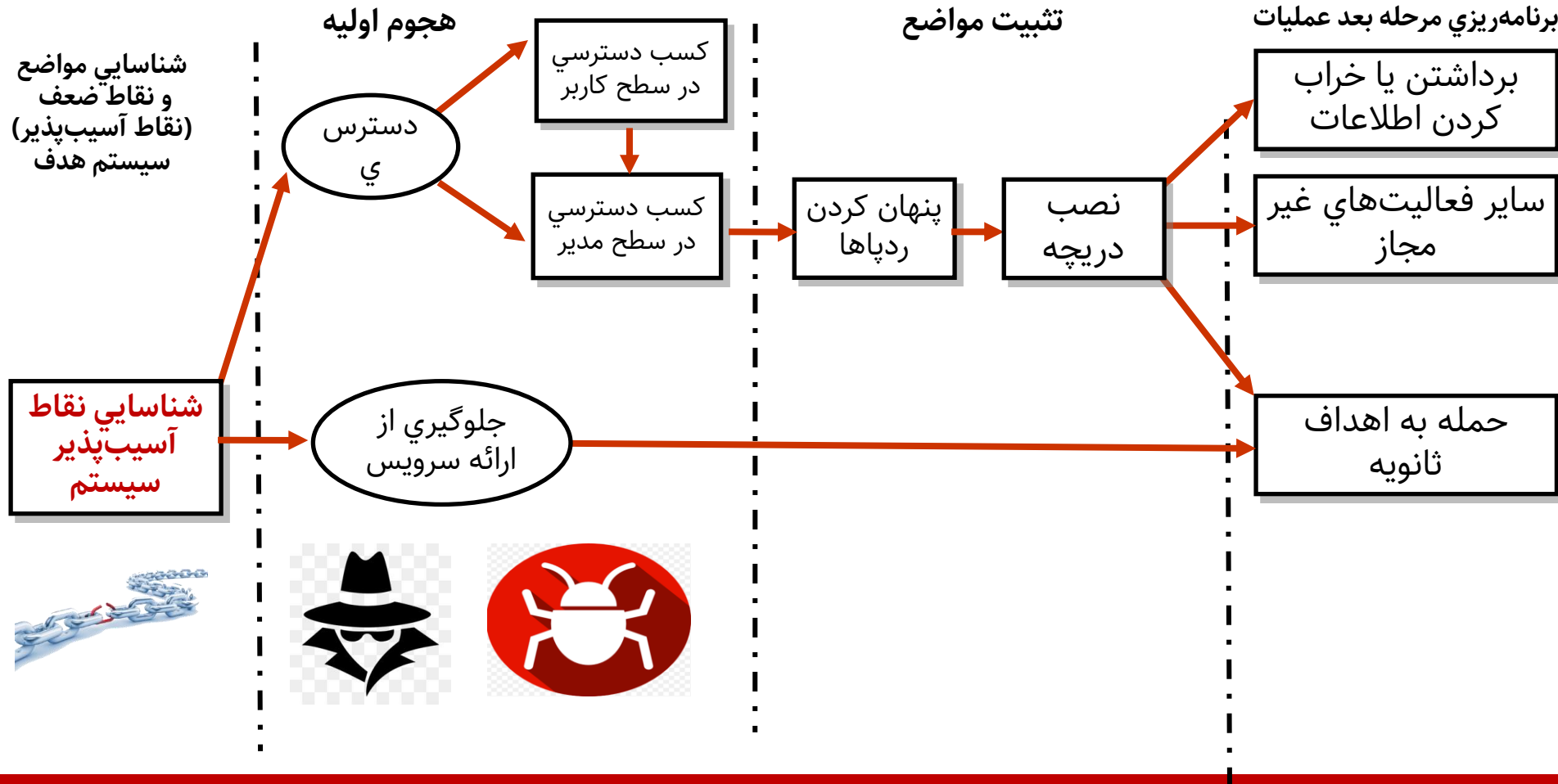
هرگونه ضعف در یکی از مولفه های شبکه (**سخت افزار**، **نرم افزار**، **پیکربندی** یا **امنیت فیزیکی**) که می تواند **مستقیماً** برای دسترسی یافتن به سیستم یا شبکه ای مورد سوءاستفاده قرار گیرد.

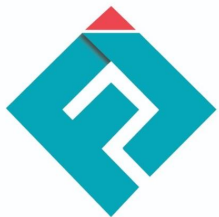


ضعفی از سیستم که به نفوذگر اجازه می دهد تا کاری را انجام دهد که در حالت عادی مجاز به انجام آن نیست.



روند کلی انجام یک حمله در محیط شبکه‌های رایانه‌ای

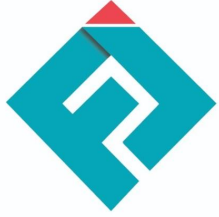




انواع مهاجمان

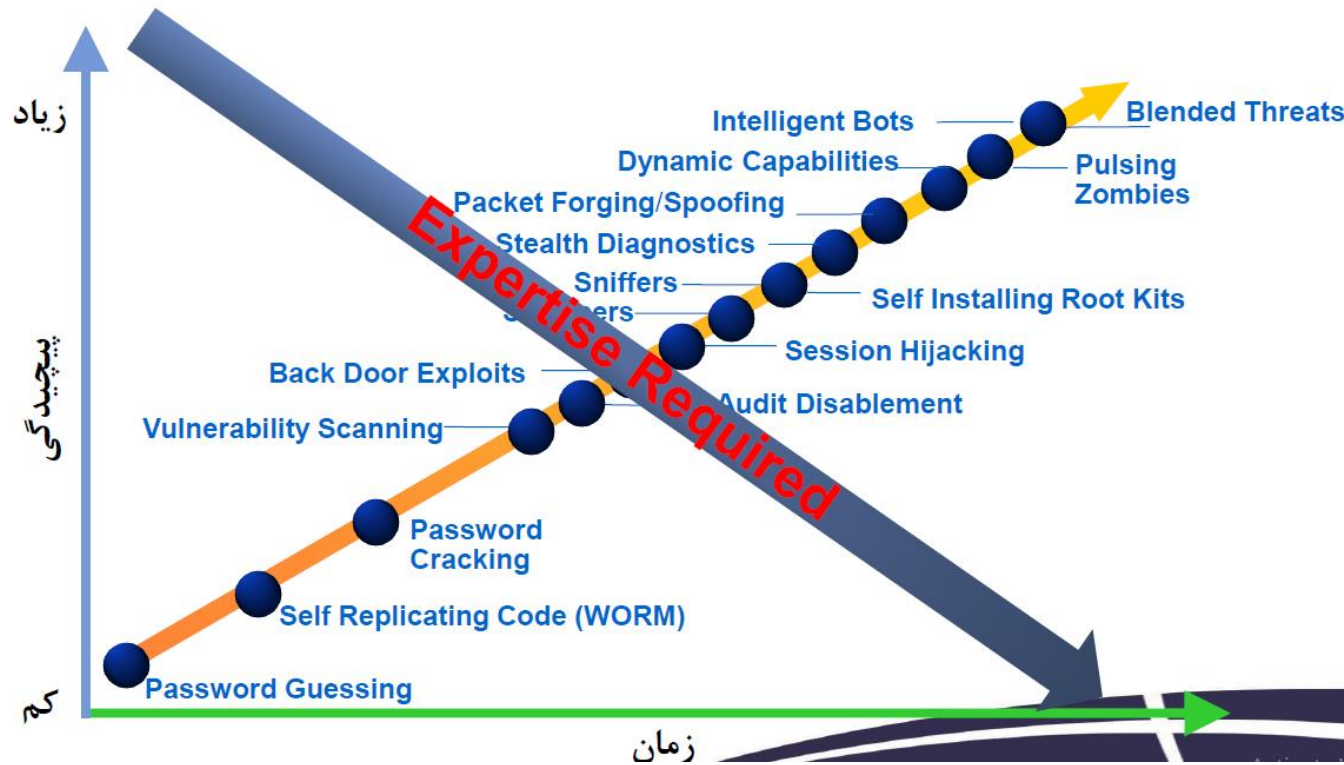
مهاجمان بازیگوش

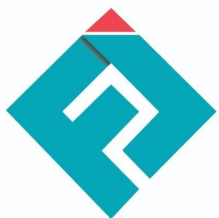
مهاجمان مصمم



سیر تکاملی حملات

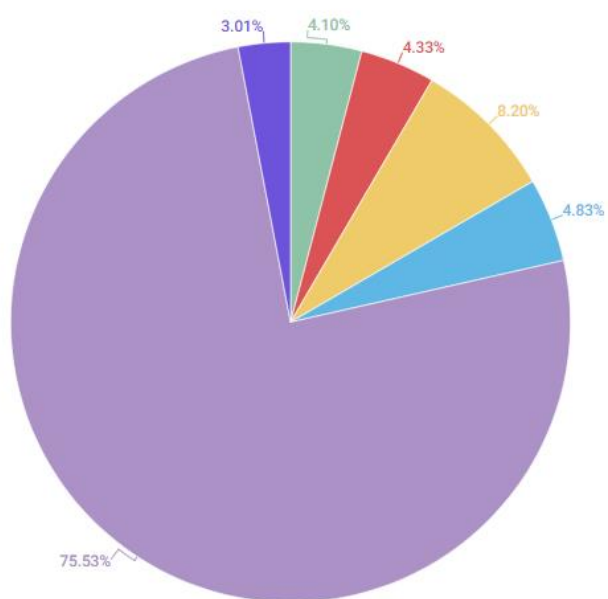
پیچیدگی بیشتر ابزارهای نفوذ
ساده تر شدن استفاده از آنها





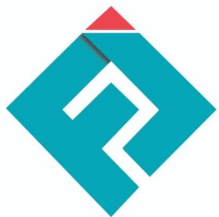
شرکت امن پردازش هوشمند فرداد

محبوبترین برنامه‌ها برای اهداف خرابکارانه



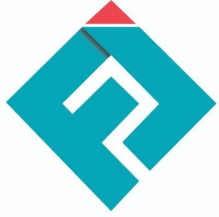
Adobe Flash Android Browser Java Microsoft Office Adobe PDF

kaspersky



چرخه حیات آسیب پذیری





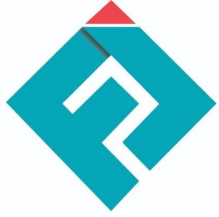
چند نمونه آسیب پذیری مطرح

شهرداری تهران

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

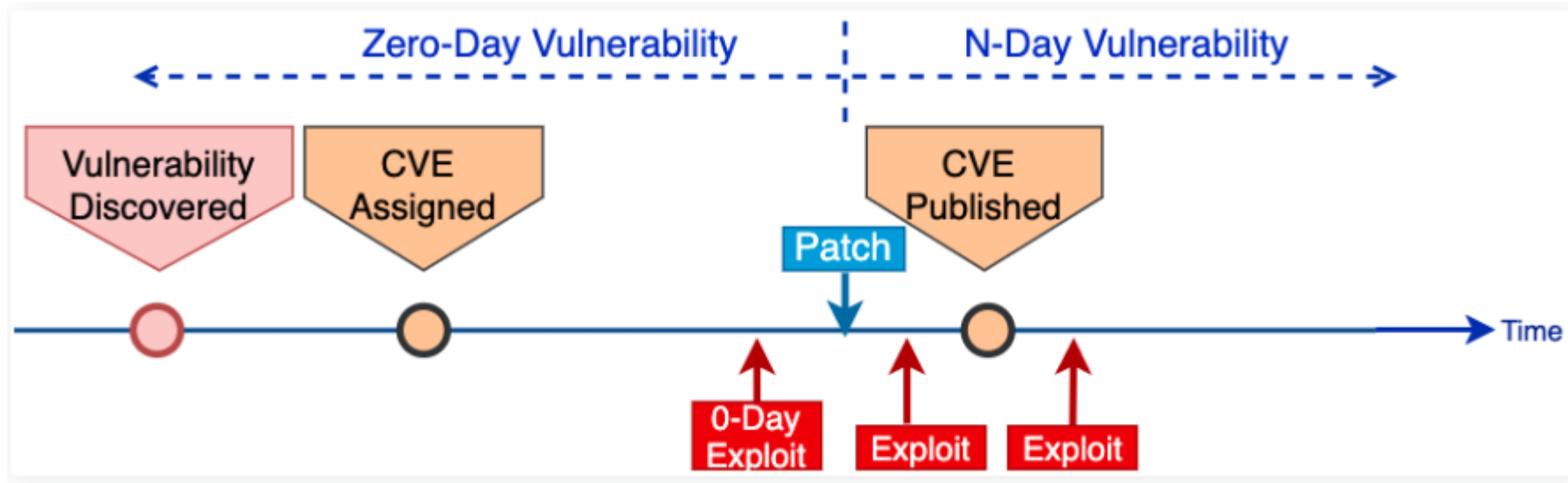
فولاد مبارکه

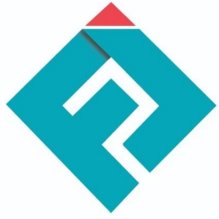
- استفاده از آسیب پذیری AD در انتشار



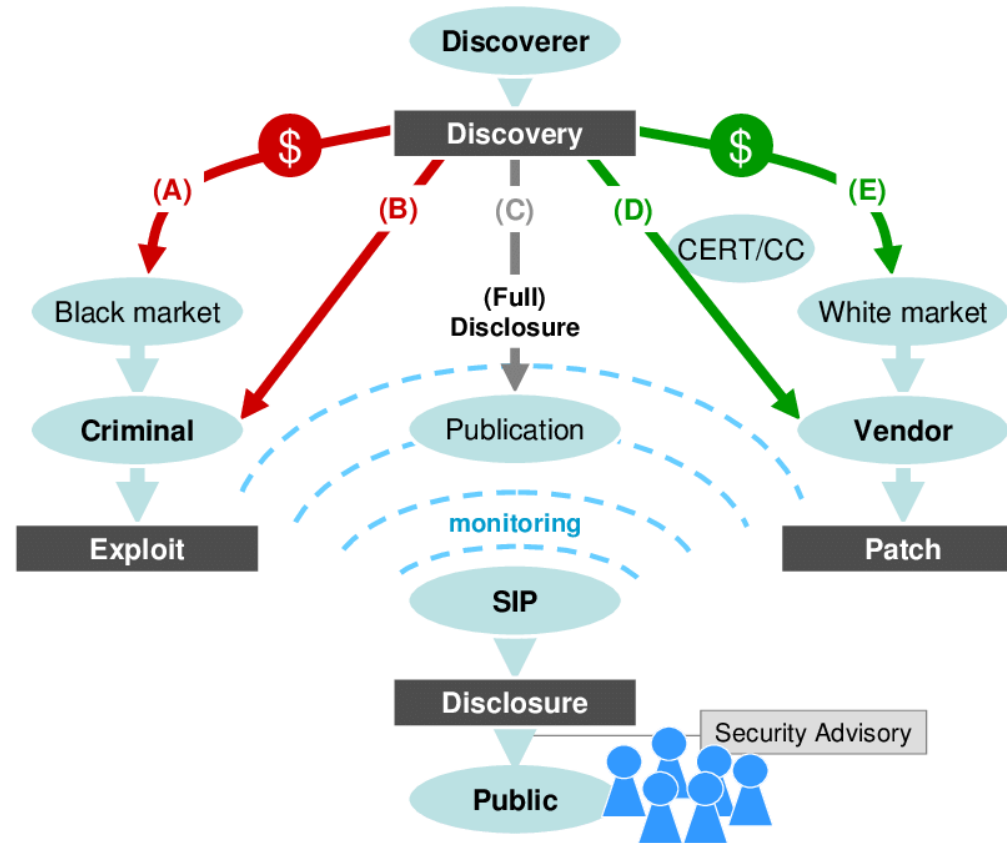
کشف / وصله / بهره برداری آسیب پذیری

- 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.





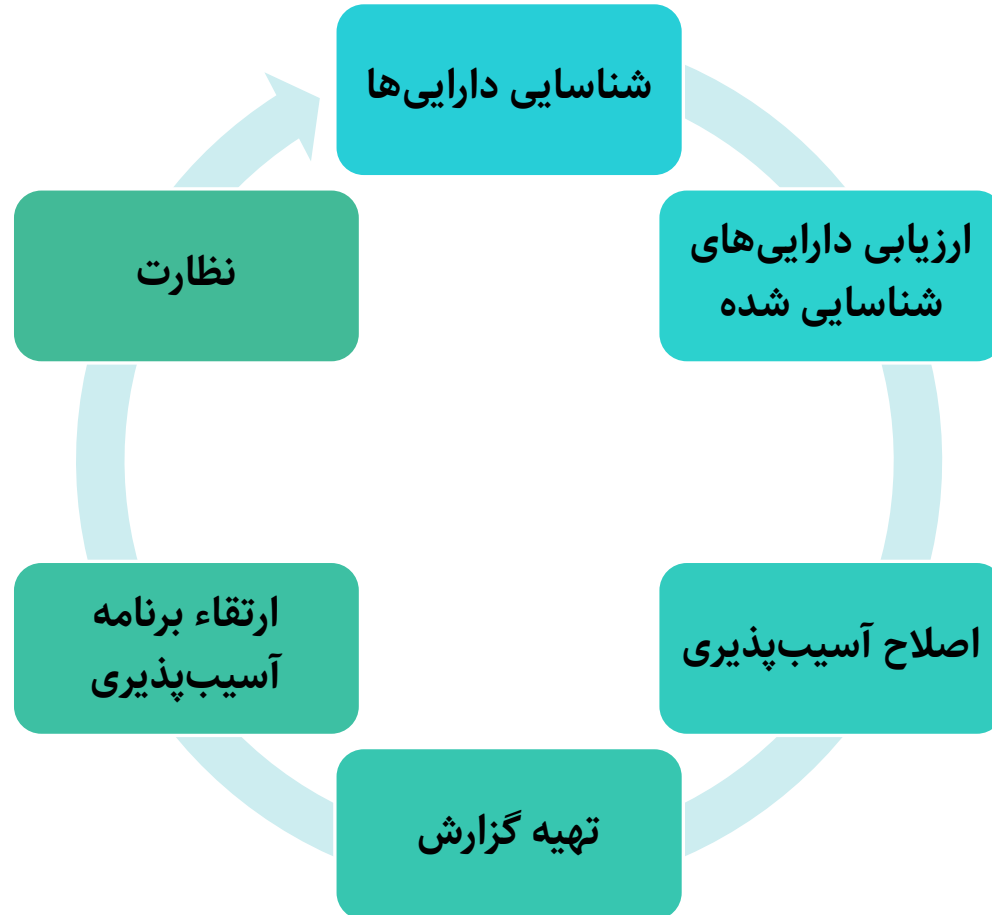
چرخه حیات آسیب پذیری و اکوسیستم امنیت سایبری

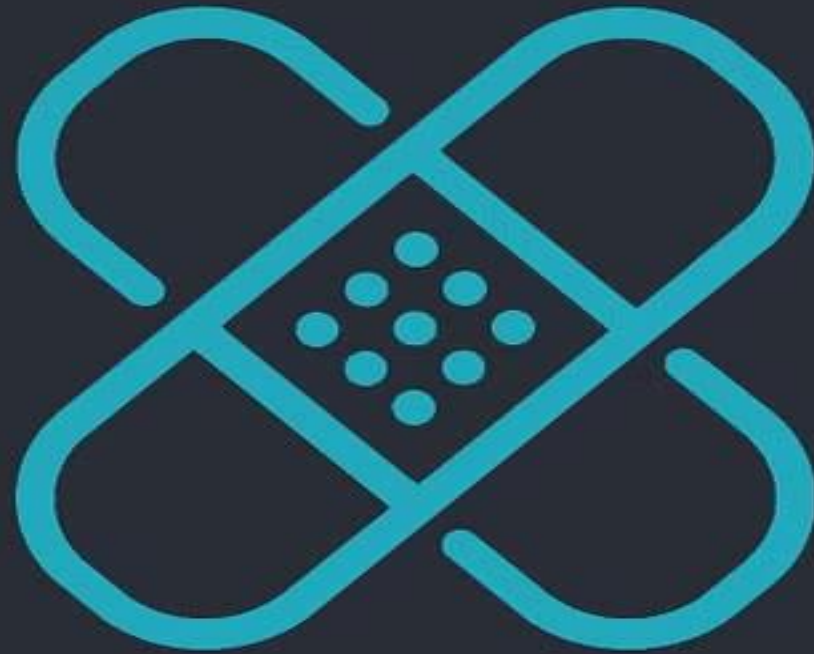


مراحل مهم در مدیریت آسیب پذیری

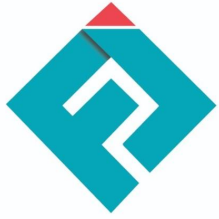


شرکت امن پردازش هوشمند فرداد





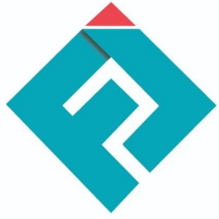
مدیریت وصله



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.

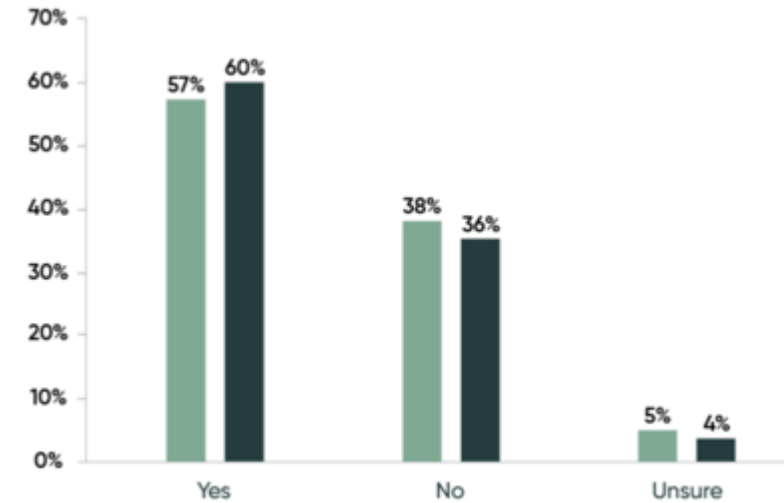


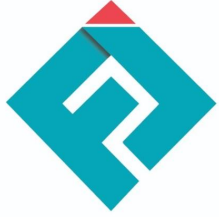


نگاهی به مطالعات در زمینه مدیریت وصله

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.





زنجیره‌ی سرویس های امنیتی

PROACTIVE

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

PROTECT

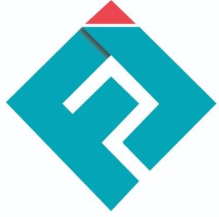
- UTM
- WAF
- Next Gen Firewall
- Firewall

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؟

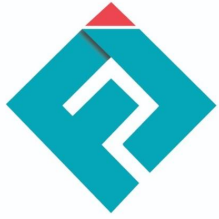
از کجا وصله‌های مطمئن دریافت کنم؟

زمانبندی اجرا و اعمال سیاست برای به‌روز کردن سیستم‌ها را چگونه انجام دهم؟

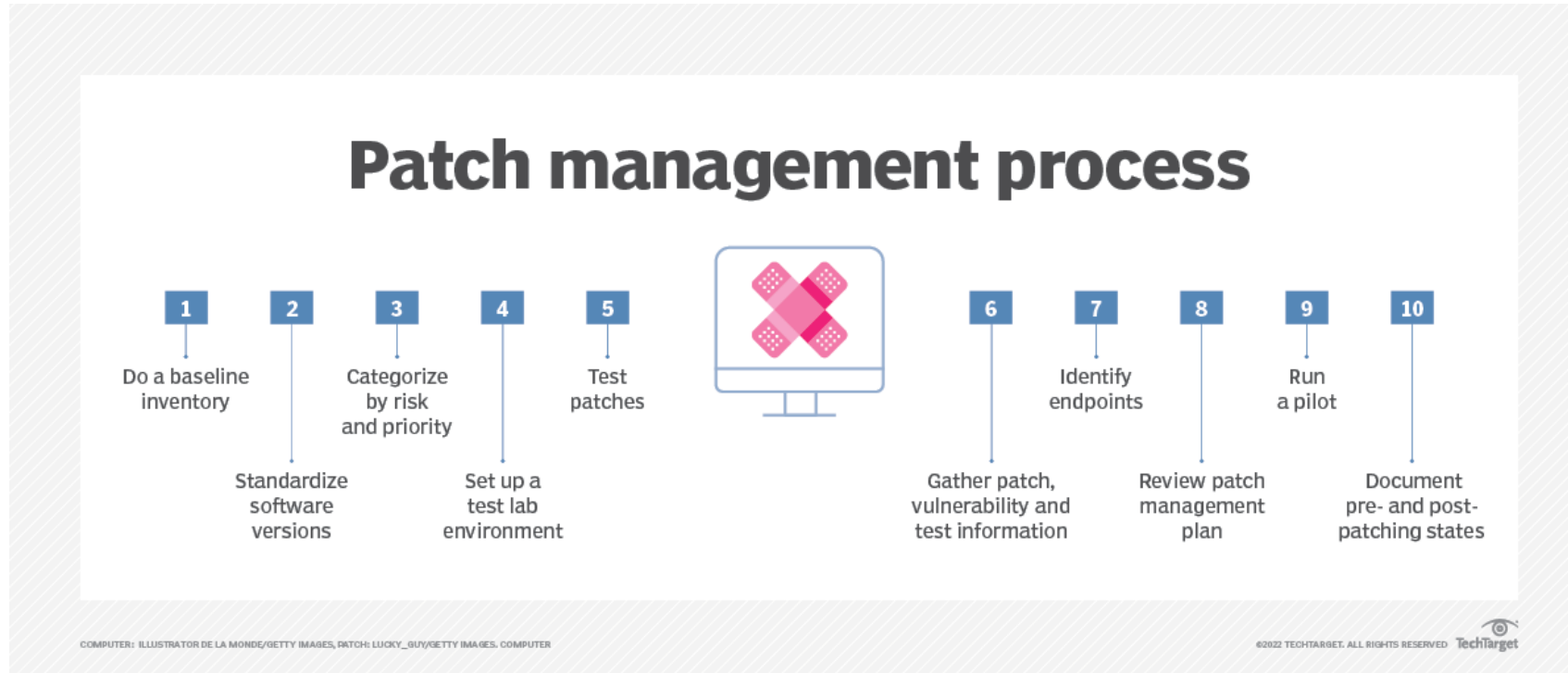
در صورت قطع و یا بروز اختلال در ارتباط اینترنت چگونه سامانه‌ها را به‌روز کنم؟

چگونه اطمینان پیدا کنم 100 درصد سامانه‌ها به‌روز شده‌اند؟

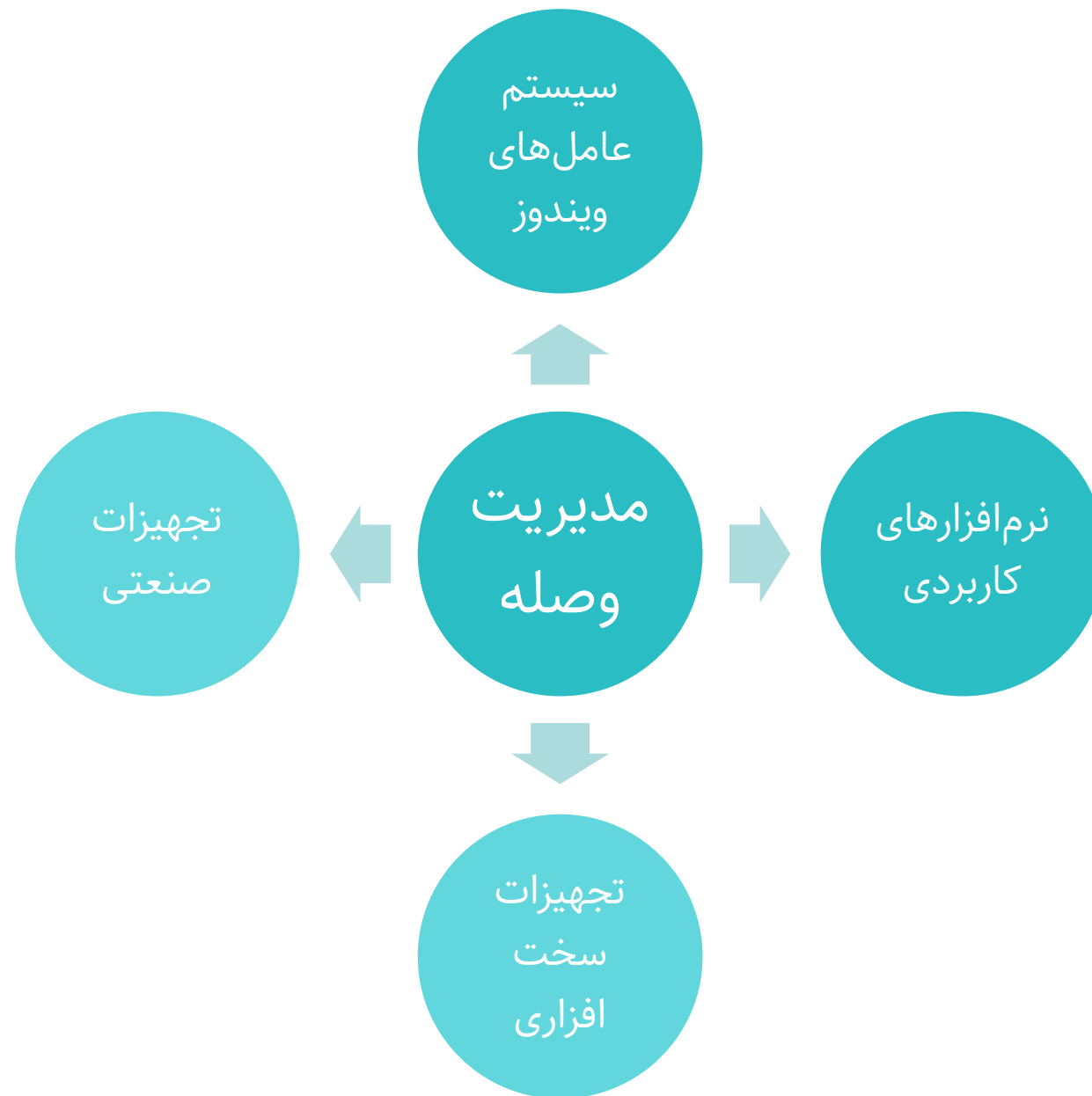
.....

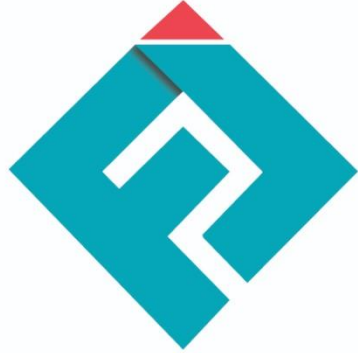


فرآیند مدیریت وصله



حیطه کاربری مدیریت وصله



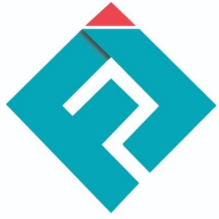


شرکت امن پردازش هوشمند فرداد
AMN PARDAZESH HOUSHMAND FARDAD Co.

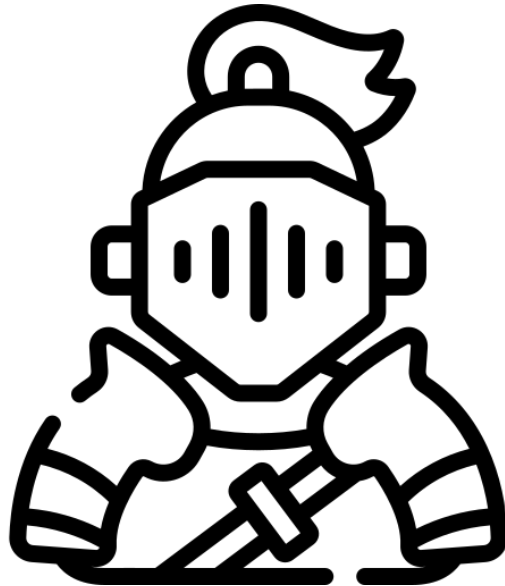


سامانه مدیریت وصله

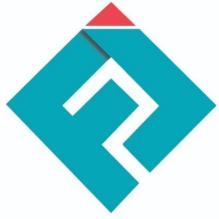
نصب و بروزرسانی خودکار سیستم عامل و انواع نرم افزارهای کاربردی به صورت
متمرکز



چرا سامانه مدیریت وصله فرید

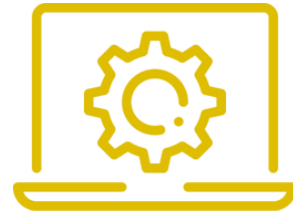


- ❖ گزارش‌های غلط برخی سامانه‌ها
- ❖ خدمات محصول
- ❖ مزایای محصول بومی
- ✓ اعتماد به وصله‌های ارسالی و شخصی‌سازی



ویژگی‌های اصلی

سیاست‌گذاری در نصب
وصله و بیان استثناها



پویش خودکار و
تشخیص نیازها

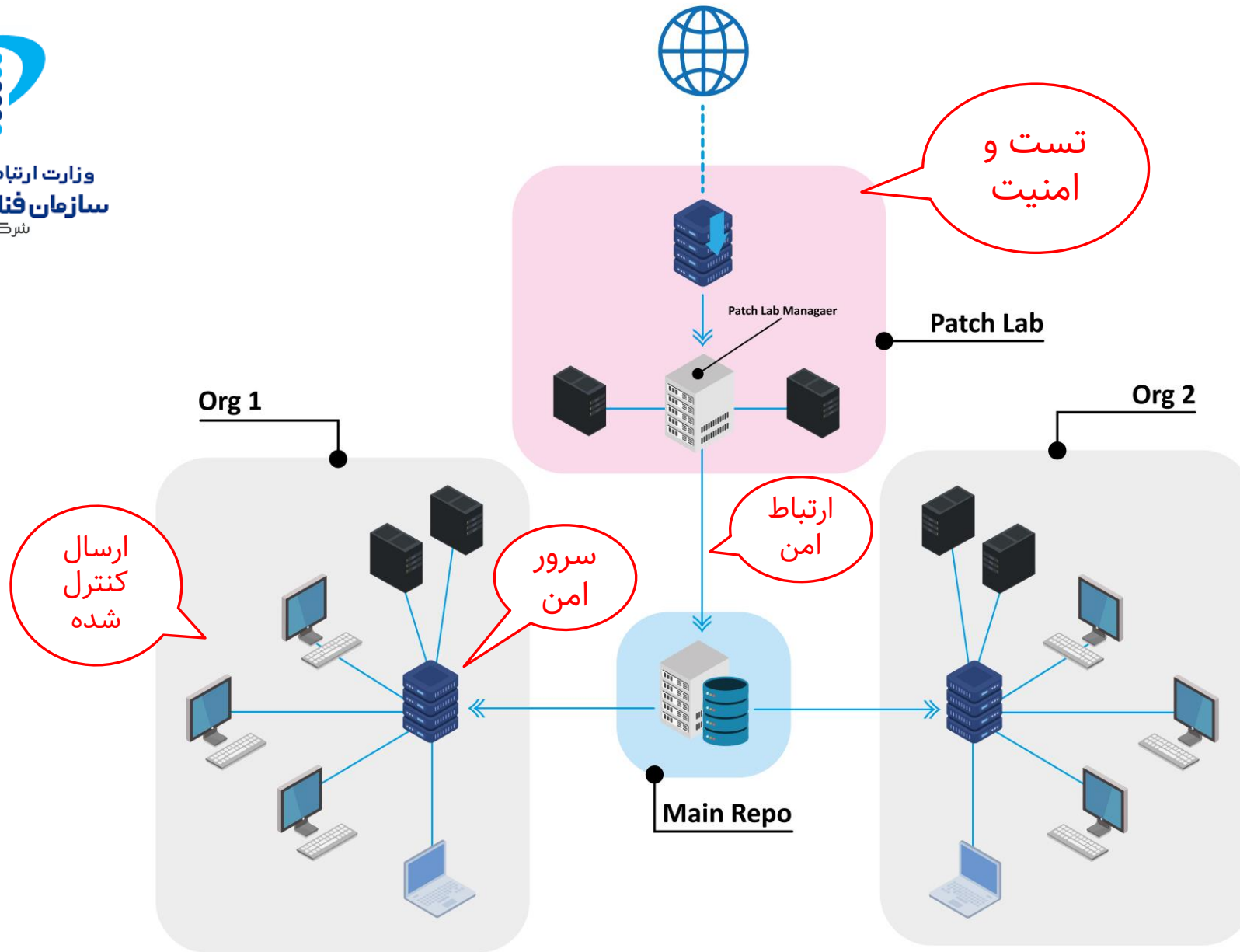


گزارش‌گیری



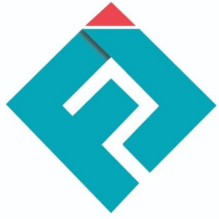
تست قبل از نصب





اجرای بلادرنگ دستورات پویس و نصب از راه دور

وصف	زمان پویس	نتیجه پویس Wus	فضای خالی (Gb)	آخرین اتصال	تغییر سخت افزار	در دسترس	بخش	شماره ساخت سیستم عامل	توضیح	نسخه عامل	سیستم عامل	آدرس سرویس گیرنده	سرویس گیرنده	عملیات
	1402/02/04 10:39:43	0 i	105.1	1402/02/09 16:28:29	✗	✓	کتابخانه	6.1.7601(Service.Pack.1)		1.6.91	windows server 2008 r2 64-bit	172.27.0.3	WIN-RCKF6KVE7JT	i 🔗
	1402/02/04 16:21:34	0 i	81.2	1402/02/09 16:28:28	✗	✓	اداره آموزش	10.0.15063		1.5.6	windows 10 64-bit	172.27.152.217	DESKTOP-HOOJRAP	i 🔗
	1402/02/09 16:04:06	0 i	87.1	1402/02/09 16:28:28	✓	✓	دانشکده مکانیک	6.1.7601(Service.Pack.1)		1.5.6	windows 7 64-bit	172.21.115.203	mech-bs-gir3	i 🔗
	1402/02/04 11:26:35	0 i	58.9	1402/02/09 16:28:27	✗	✓	دانشکده نساجی	6.1.7601(Service.Pack.1)		1.6.91	windows 7 64-bit	172.21.18.96	blue-PC	i 🔗
	1402/02/09 09:11:16	0 i	641.4	1402/02/09 16:28:24	✗	✓	دانشکده عمران	6.2.9200		1.6.5	windows 10 64-bit	172.21.66.33	civil-A100	i 🔗
	1402/02/05 18:55:09	0 i	88.4	1402/02/09 16:28:17	✗	✓	دانشکده نساجی	6.2.9200		1.6.91	windows 10 64-bit	172.21.18.99	DESKTOP-DISN625	i 🔗
			72.4	1402/02/09 16:28:11	✗	✓	دانشکده مکانیک	6.2.9200		1.6.91	windows 10 64-bit	172.21.119.49	DESKTOP-17SU2ED	i 🔗
	1402/02/04 10:46:54	0 i	184.4	1402/02/09 16:28:11	✓	✓	دانشکده مهندسی شیمی	6.1.7601(Service.Pack.1)	دکتر شمس	1.6.91	windows 7	172.21.100.237	Drshams-PC	i 🔗
			75.9	1402/02/09 16:28:05	✗	✓	سازمان مرکزی	6.2.9200		1.6.91	Windows 11 64-bit	172.27.34.107	DESKTOP-LADKM2S	i 🔗
	1402/02/06 10:23:49	0 i	216.2	1402/02/09 16:28:05	✓	✓	دانشکده کامپیوتر	6.2.9200	خانم صادقی - آموزش	1.6.91	windows 10 64-bit	172.21.52.93	ECE-MrsSadeghi	i 🔗
	1402/02/04 10:43:21	0 i	24.3	1402/02/09 16:28:02	✓	✓	اداره آموزش	6.1.7601(Service.Pack.1)		1.6.91	windows 7 64-bit	172.27.152.224	Amoozesh_10_3	i 🔗
			144.4	1402/02/09 16:27:55	✓	✓	دانشکده مکانیک	6.2.9200		1.6.91	windows 10 64-bit	172.21.115.190	DESKTOP-G0EH307	i 🔗
	1402/01/14 09:10:37	0 i	79.6	1402/02/09 16:27:45	✗	✓	دانشکده عمران	6.2.9200		1.6.91	windows 10 64-bit	172.21.64.86	Civil-Head	i 🔗
	1401/09/22 09:19:54	0 i	111.9	1402/02/09 16:27:40	✓	✓	دانشکده مهندسی شیمی	10.0.17134	سایت کارشناسی خواهران	1.5.6	windows 10 64-bit	172.21.97.96	che-b8	i 🔗
	1402/02/04 15:02:34	0 i	52.9	1402/02/09 16:27:33	✗	✓	دانشکده مهندسی شیمی	6.2.9200	سایت دکتری خواهران	1.6.91	windows 10 64-bit	172.21.97.59	che-pg1	i 🔗



شرکت امن پردازش هوشمند فرداد

به روزرسانی انواع سیستم عامل ها و نرم افزارها

The screenshot displays two software update windows on a Windows desktop. The desktop background is a green forest scene. The taskbar at the bottom shows icons for Start, Internet Explorer, Mail, and other applications. The system tray in the bottom right corner shows the date and time as 16:31:22 on 1402/2/9.













ویندوز نرم افزاری (Windows Update) Table:

تاریخ انتشار	جدید	صرف نظر	معماری	نسخه نهایی	نام	آیکون	وبرایش
1401/11/08	×	×	64 بیتی	6.20	Winrar	[Icon]	[Link]
1401/03/29	×	×	64 بیتی	6.11	Winrar	[Icon]	[Link]
1400/09/06	×	×	64 بیتی	6.10.2	Winrar	[Icon]	[Link]
1401/11/08	×	×	64 بیتی	6.20	Winrar	[Icon]	[Link]
1401/03/29	×	×	64 بیتی	6.11	Winrar	[Icon]	[Link]
	×	×	64 بیتی	6.10.2	Winrar	[Icon]	[Link]
	×	×	64 بیتی	3.0.18	VLC media player	[Icon]	[Link]
	×	×	64 بیتی	3.0.17.4	VLC media player	[Icon]	[Link]
	×	×	64 بیتی	3.0.16	VLC media player	[Icon]	[Link]

نرم افزار (Software Update) Table:

تاریخ آخرین تغییر	صرف نظر	نام	آیکون	وبرایش
10-03-12 1402/02/09	×	WinSCP	[Icon]	[Link]
10-03-10 1402/02/09	×	Advanced Installer	[Icon]	[Link]
10-03-14 1402/02/09	×	Cacti	[Icon]	[Link]
10-04-24 1402/02/09	×	Adobe Flash Player ActiveX	[Icon]	[Link]
10-04-21 1402/02/09	×	FLV Media Player	[Icon]	[Link]
10-04-17 1402/02/09	×	Tera Copy	[Icon]	[Link]
10-03-16 1402/02/09	×	Solidworks	[Icon]	[Link]
10-04-04 1402/02/09	×	Adobe Flash Player Plugin Chrome	[Icon]	[Link]

بخش بندی و مدیریت کاربران

عملیات	نام	شبکه ها	استثنائات شبکه ها	سرویس گیرنده های ثبت نام نشد
   <input type="checkbox"/>	سازمان مرکزی	172.19.26.0/24 172.30.26.0/24 172.27.32.0/20 172.19.130.0/24		0
   <input type="checkbox"/>	دانشکده کامپیوتر	172.19.32.0/24 172.21.48.0/20		1
   <input type="checkbox"/>	دانشکده برق	172.19.13.0/24 172.30.13.0/24 172.20.32.0/20 172.21.32.0/20		0
   <input type="checkbox"/>	دانشکده فیزیک	172.19.18.0/24 172.30.18.0/24 172.20.176.0/20		0

سیستم
سیستم عامل
مدت زمان کار
فرآیندها
پردازشگر

Linux 5.4.74patchman
3 days, 6:53:40.181416
264

حافظه
1.6GB/7.8GB

دیسک
133.0GB/195.9GB

شبکه

آپلود
1.79Kb

دانلود
1.71Kb

مخزن
سرویس گیرنده ها
گزارش ها

نصب عامل کاربر
عیب یابی



مخزن



سرویس گیرنده‌ها



گزارش‌ها



نصب عامل کاربر



گزارش نرم‌افزارها و سخت‌افزارهای سازمان

معماری	نسخه	نرم‌افزار	سیستم عامل	آدرس سرویس گیرنده	سرویس گیرنده
32	5.0.96.2	zotero	windows 7	172.27.2.46	lib-baby
32	5.2	zoiper5	windows 7 64-bit	0.0.0.0	Tarahi-pc
32	5.2	zoiper5	windows 10 64-bit	172.21.18.2	Tabibi-PC
64	7.26.1	zoc terminal 7.2 (64-bit)	windows 10 64-bit	192.168.201.4	DESKTOP-0CEMTKM
32	7.7.4	zoc terminal 7.0	windows 7 64-bit	172.17.32.131	Fedra-Ghassemi
32	4	ziryab 4	windows 7 64-bit	172.21.160.10	tr-PC
32	3	ziryab 3	windows 7 64-bit	172.21.160.10	tr-PC
32	0	zimatec studio v5.3.1.3	windows 10 64-bit	172.21.148.163	math-18
32	4.0.4	zeromq 4.0.4	Windows 8.1	172.21.33.85	behzad1
32	0	zero assumption recovery version 9	windows 10 64-bit	172.21.18.2	Tabibi-PC
32	3.2.2.611	zebradesigner 3	windows 7 64-bit	172.27.6.41	lib-ghasri
64	3.2.2.611	zebradesigner 3	windows 7 64-bit	172.27.6.41	lib-ghasri

نرم‌افزارهای سازمان

دریافت آکسل

1 - 50 از 106250 عضو

تعداد در صفحه 50

1 2 3 4 5 ...



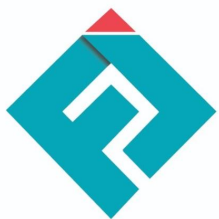
نرم‌افزارهای سازمان

سیستم
 Linux 5.4.74patchman
 سیستم عامل
 3 days, 6:59:45.200464
 مدت زمان کار
 264
 فرآیندها
 پردازشگر

حافظه
 1.6GB/7.8GB

دیسک
 133.0GB/195.9GB

شبکه
 آپلود 2.28Kb
 دانلود 914b



ویژگی‌های سازمانی

سازمان‌های بزرگ

ساختار
سلسله مراتبی

مخازن
جایگزین

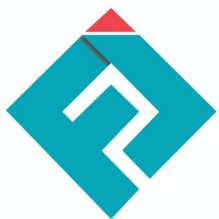
سازمان‌های متوسط

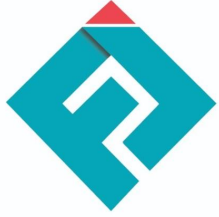
تعریف بخش‌ها
و زیرشبکه

مدیریت کاربران

سازمان‌های کوچک

اتصال به اکتیو
دایرکتوری





سوالات متداول

❖ نرم افزارهای کرک

❖ تجهیزات شبکه مانند ESXI، ماشین های آن

❖ مشکلاتی که با به روزرسانی پیش می آید؟

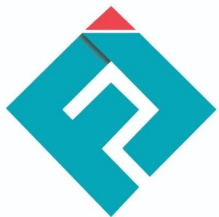
❖ ایجاد استثنا در به روزرسانی ممکن است؟

❖ به روزرسانی سرورها

❖ لینوکس



پیش نمایش



شرکت امن پردازش هوشمند فرداد

با تشکر از توجه شما

؟