شرکت امن پردازش هوشمند فرداد

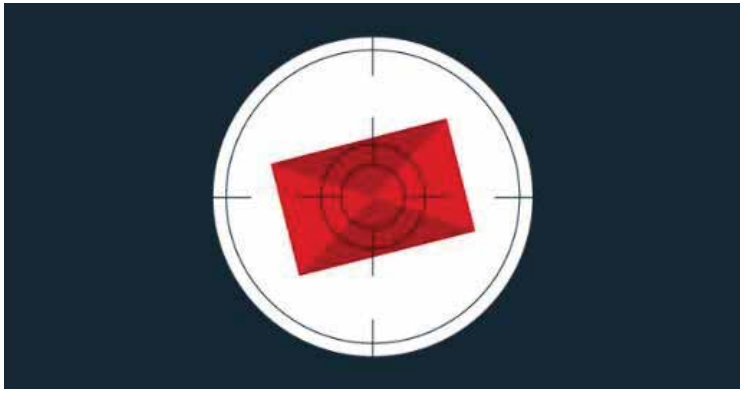
نگاهی به حوادث اخیر سایبری

حملات سایبری اخیر در ایران)۲۰۲۱(

حملات سایبری اخیر در ایران)۲۰۲۲(

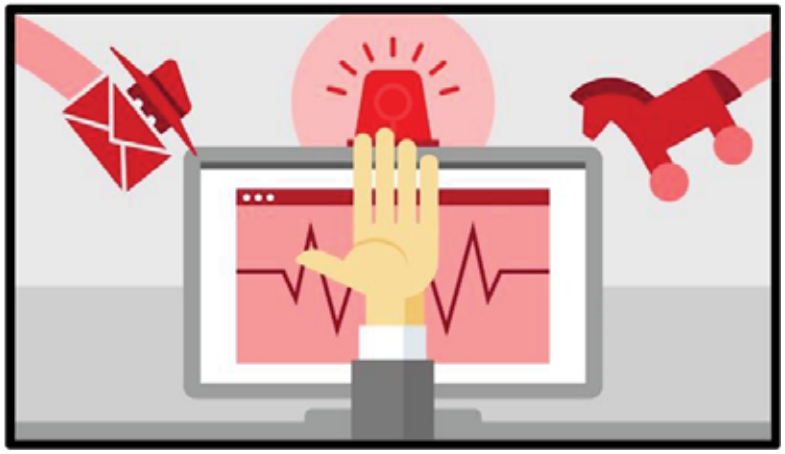
تهدید)Threat(

- هر عاملی که **بتواند** سبب به خطر افتادن یکی از **اصول سه‌گانه امنیت** شود.



حادثه سایبری)Incident(

هرگاه تهدیدی از حالت **بالقوه** به حالت **بالفعل** در آید گوئیم یک حادثه رخ داده است.

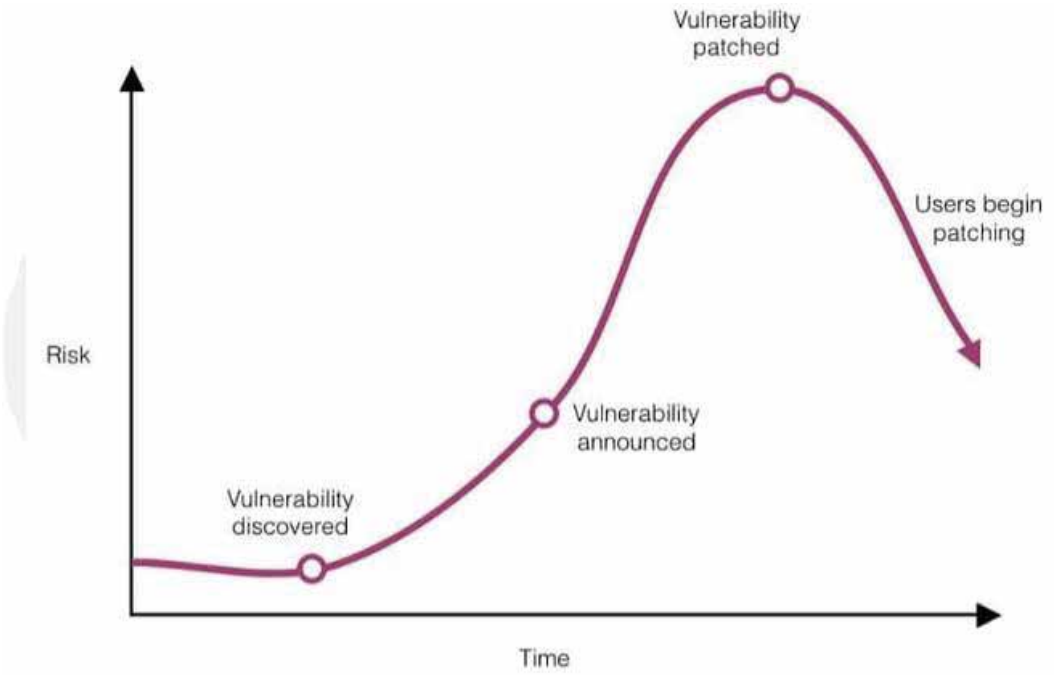


آسیب‌پذیری)Vulnerability(

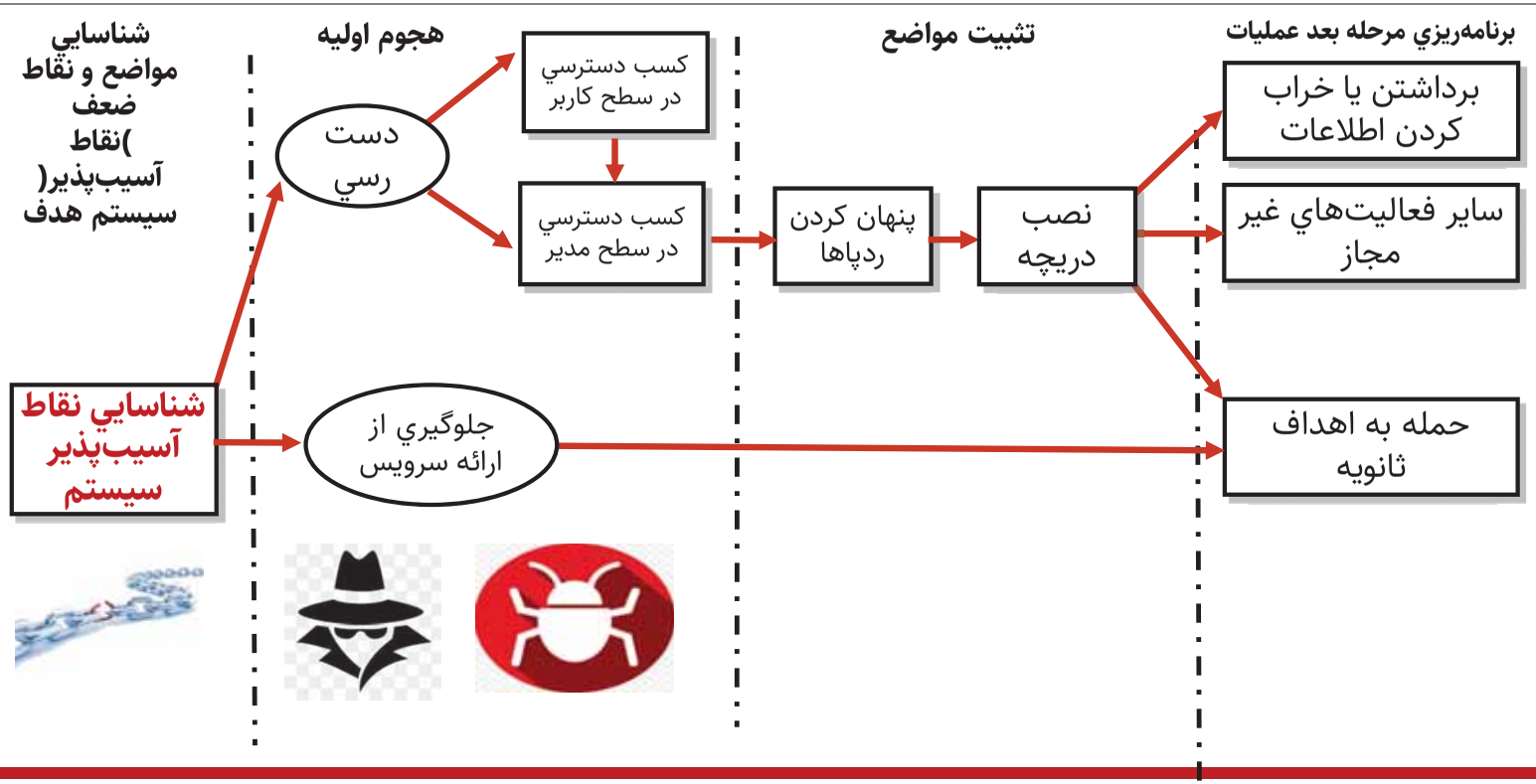
هرگونه ضعف در یکی از مولفه‌های شبکه)**سخت‌افزار**، **نرم‌افزار**، **پیکربندی** یا **امنیت فیزیکی**(که می‌تواند **مستقیماً** برای دسترسی یافتن به سیستم یا شبکه‌ای مورد سوءاستفاده قرار گیرد.

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

چرخه حیات آسیب‌پذیری



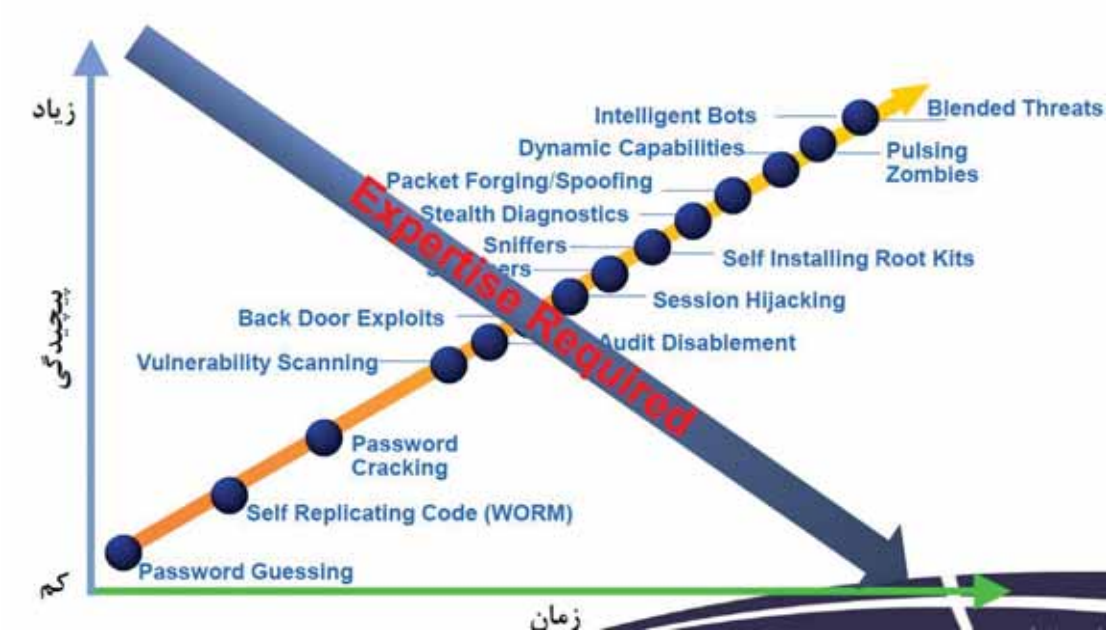
)روند كلي انجام يک حمله در محيط شبکه‌های رايانه‌ای(



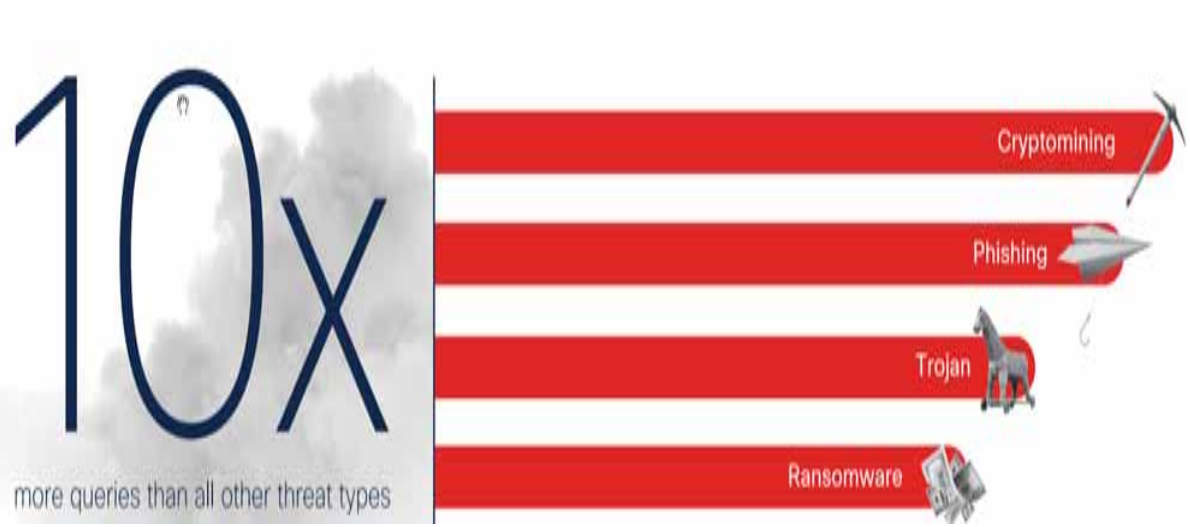
سیر تکاملی حملات

پیچیدگی بیشتر ابزارهای نفوذ

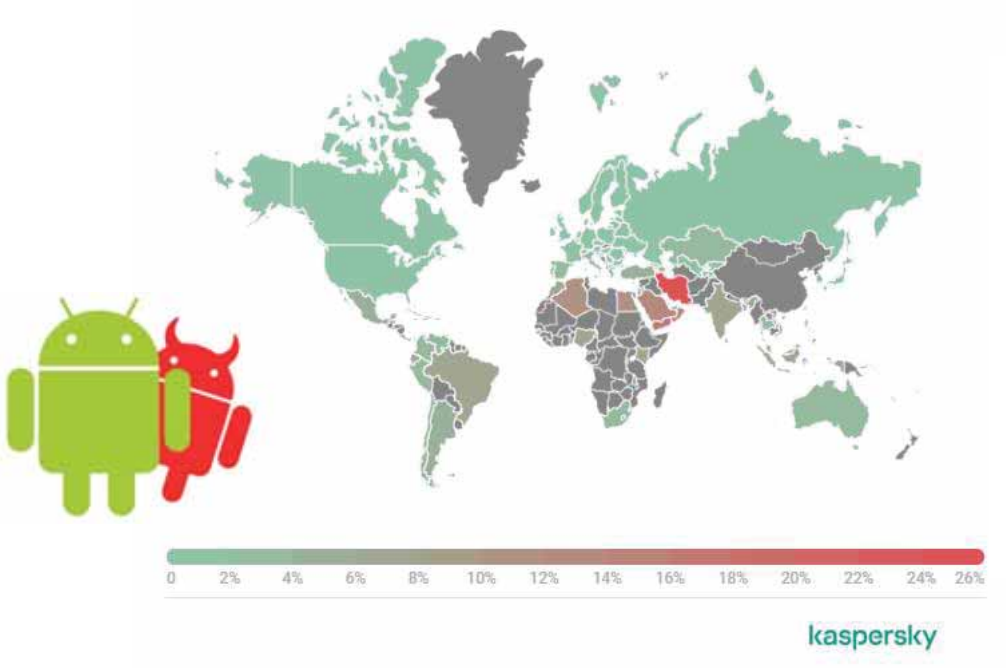
ساده‌تر شدن استفاده از آنها



تهدیدات پرتکرار در دو سال اخیر

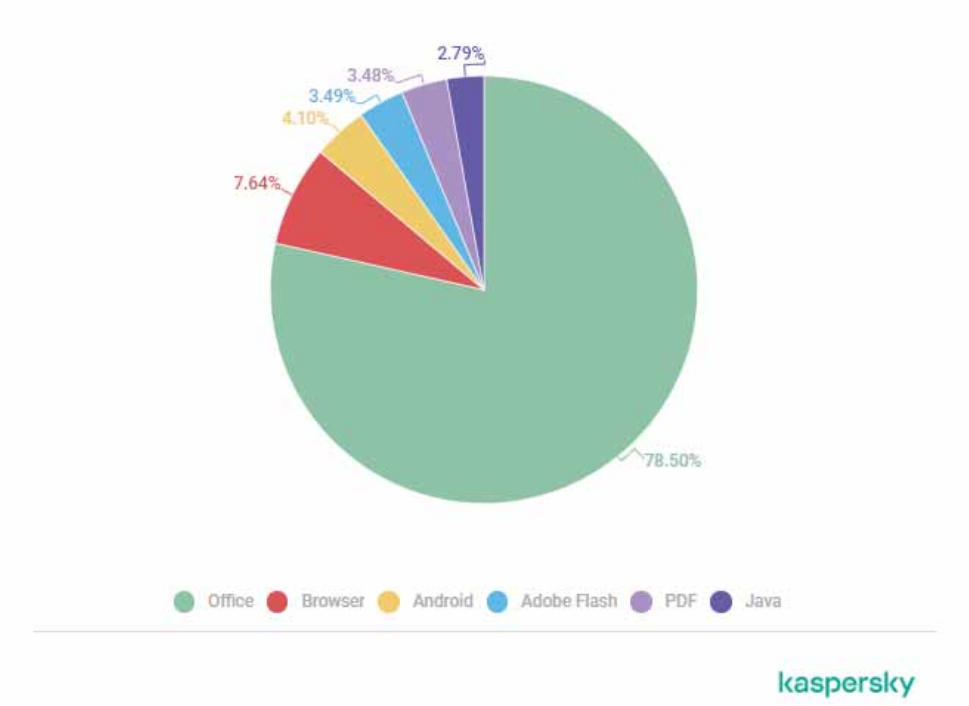


بدافزارهای اندرویدی



	Countries and territories*	%**
1	Iran	26.91
2	Yemen	17.97
3	Saudi Arabia	12.63
4	Oman	12.01
5	Algeria	11.49
6	Egypt	10.48
7	Morocco	7.88
8	Kenya	7.58
9	Ecuador	7.19
10	Indonesia	6.91

محبوب‌ترین برنامه‌ها برای اهداف خرابکارانه

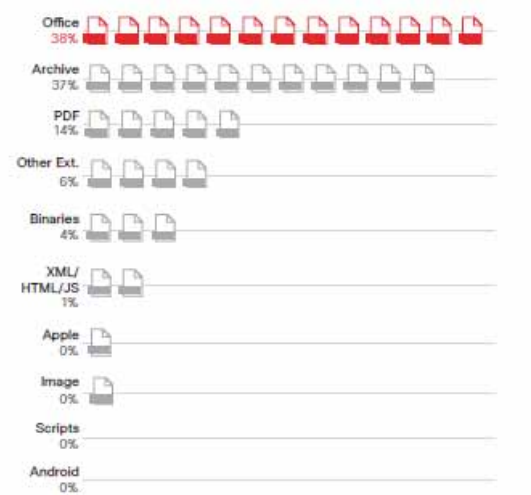


ایمیل قلابی

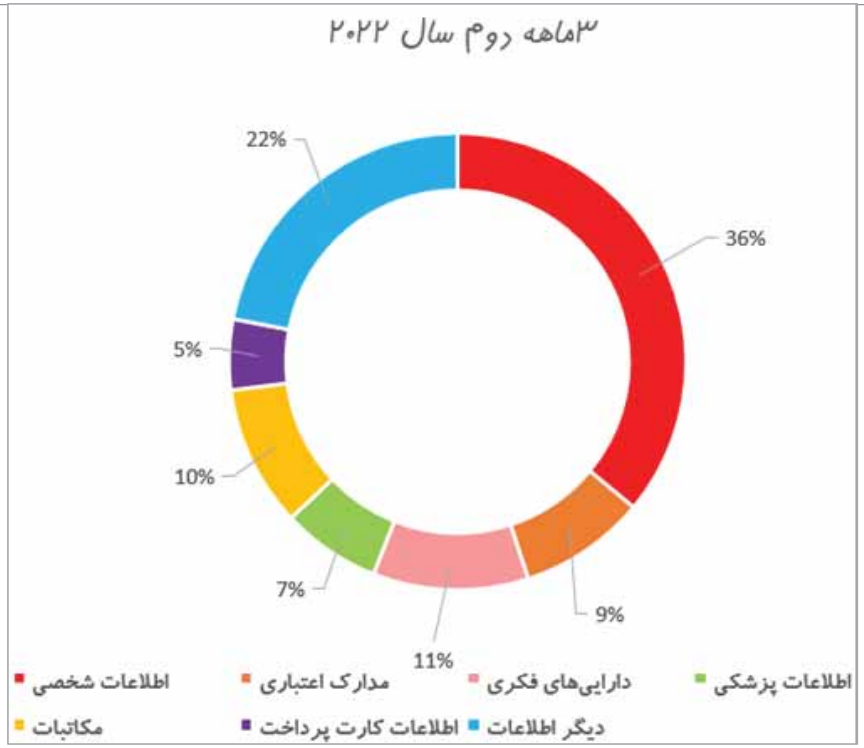
۹ درصد حملات سایبری با یک **ایمیل قلابی** آغاز می‌گردد.

مخرب‌ترین فرمت فایل

مایکروسافت آفیس بیشترین آمار در میان فرمت‌های گوناگون فایل که در ایمیل‌های هکری مورد سوء استفاده قرار گرفته است.

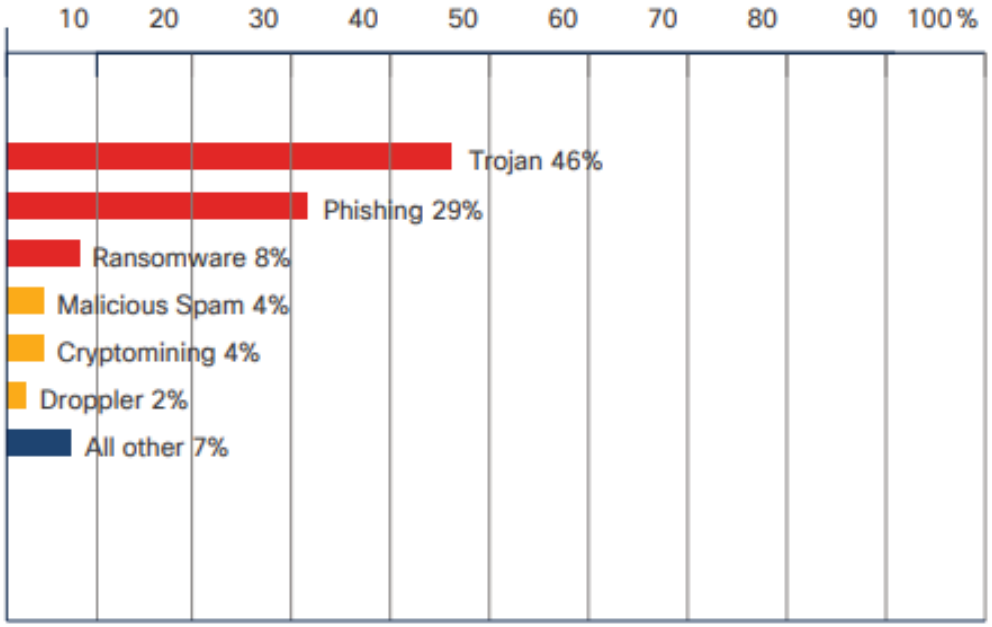


آمارگان داده‌های به سرقت رفته در سال ۲۰۲۲



منبع PositiveTechnology ✓

تهدیدات پرتکرار در بخش بهداشت و درمان



نگاهی دقیق تر به تهدیدات و حملات سایبری سازمانی

بدافزار
مهندسی اجتماعی
حملات وب

Security is Hard

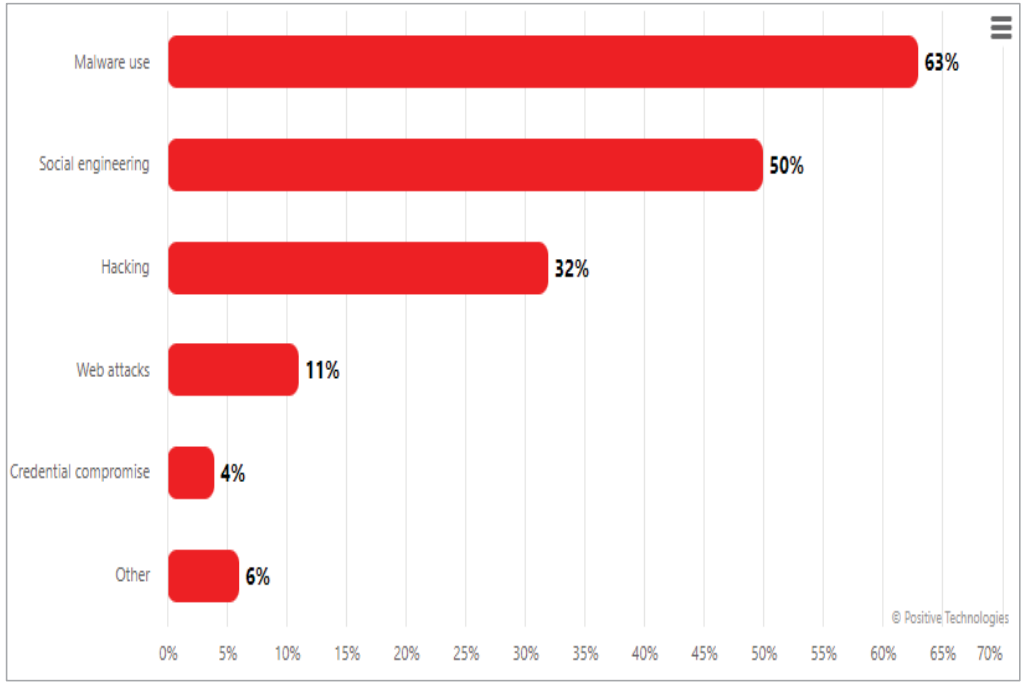
- "The three golden rules to ensure computer security are:
  - do not own a computer
  - do not power it on
  - and do not use it."

Robert H. Morris former Chief Scientist of the National Computer Security Center

- "Unfortunately the only way to really protect [your computer] right now is to turn it off, disconnect it from the Internet, encase it in cement and bury it 100 feet below the ground."

Prof. Fred Chang, former director of research at NSA

انواع حملات و تهدیدات رایج در سال ۲۰۲۱



بدافزارها

Malwares

بدافزارها (Malware)

- Malicious software
- نرم افزاری برای آلوده کردن سیستم‌های کامپیوتری یا تخریب آنها بدون اطلاع کاربر
  - Viruses
  - Worms
  - Trojan horses
  - Ransomware
  - Spyware
  - Rootkits

ویروس ها Viruses

- یک کد مخرب که روی ماشین هدف بدون اطلاع کاربر اجرا شده و آن را آلوده می‌کند.
- ویروس ها برای نصب، اجرا و انتشار نیاز به انجام یک Act توسط کاربر دارند.
- انواع :
  - Boot sector
  - Macro
  - Multipartite
  - Encrypted
  - Polymorphic
  - Metamorphic
  - Stealth
  - Armored
  - hoax

کرم‌ها Worms

- یک برنامه مخرب مانند ویروس با این تفاوت که می تواند بدون دخالت کاربر خود را تکثیر کند.
- کرم‌ها از آسیب‌پذیری‌های رفع نشده استفاده می‌کنند.
- کرم‌ها می‌توانند فعالیت عادی سیستم یا ترافیک شبکه را به شدت مختل کنند.
- کرم‌های معروف
  - Nimda
  - Conficker
  - ILOVEYOU
  - CodeRed
  - Stuxnet
  - WannaCry

Trojans

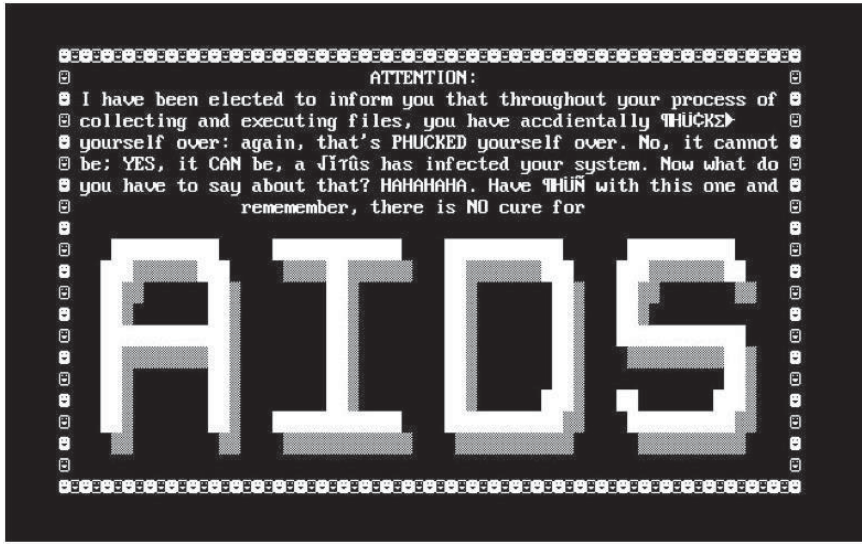
- یک برنامه مخرب که به عنوان بخشی از یک برنامه مفید و دلخواه کاربر طراحی شده است.
- تروجان ها یک سری عملیات مخرب را همزمان با یک عملکرد دلخواه اجرا می‌کنند.

- RAT (Remote Access Trojan)
- تروجان‌هایی که یک دسترسی راه دور به سیستم قربانی ارائه می‌کنند

- تروجان های معروف:
  - Zeus
  - Emotet

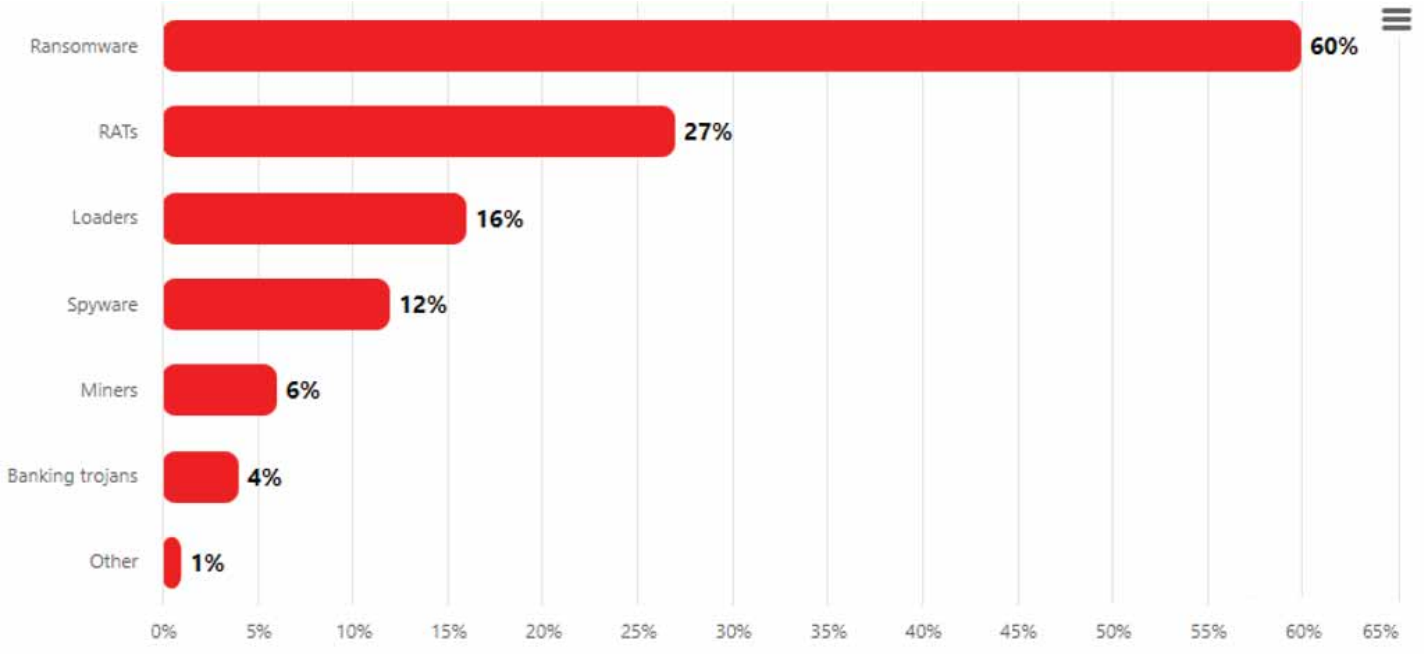
باج افزارها Ransomwares

- یک برنامه مخرب که از آسیب‌پذیری‌های سیستم یا برنامه‌ها استفاده می‌کند تا به سیستم قربانی دسترسی پیدا کرده و سپس فایل‌های آن را رمز کند.
- ضرورت داشتن یک برنامه پشتیبان‌گیری منظم



- Ryuk, 2019 and 2020
- SamSam, 2018
- WannaCry, 2017
- Petya, 2016
- AIDS Trojan or PC Cyborg, 1989

فراوانی آماری Malware



باج‌افزارهای رایج در سال ۲۰۲۱ و روش نفوذ آن‌ها

REvil:

- آسیب‌پذیری روز صفرم در Kaseya VSA Server Platform، تزریق کد آلوده، گسترش میان مشتریان Kaseya
- لزوم تست پلتفرم‌ها و اپلیکیشن‌ها

Conti(Ryuk):

- RaaS، Phishing Emails، فایل word به همراه embedded macro، سرویس‌های RDP
- جایزه برای دستگیری عوامل
- لزوم آموزش سازمانی، لزوم راه‌اندازی و رصد سامانه متمرکز مدیریت لاگ(SIEM)

باج‌افزارهای رایج دو سال اخیر ۲۰۲۱ و روش نفوذ آن‌ها

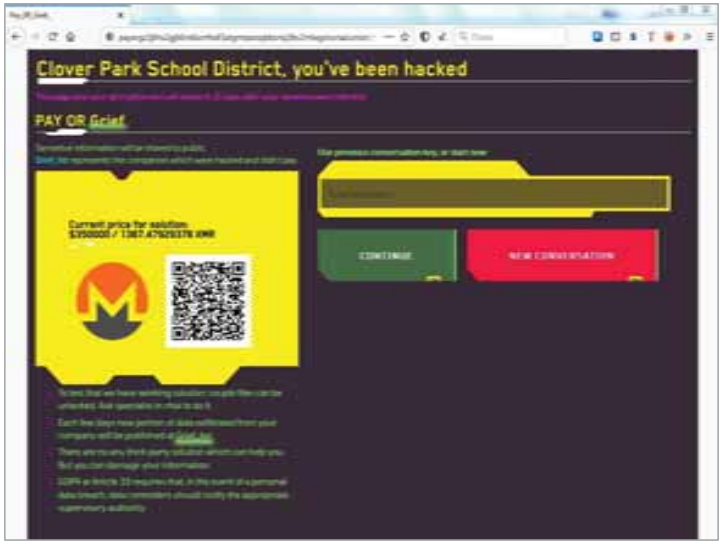
Clop:

- دسترسی اولیه به وسیله ارسال ایمیل‌های **phishing**، حدس گذرواژه **RDP** یا استفاده از آسیب‌پذیری‌های شناخته شده مانند
  - ✓ **SQLI (CVE-2021-27101)**
  - ✓ اجرای دستور بر روی سیستم‌عامل به وسیله درخواست **POST** دستکاری‌شده یا **web service** محلی (**CVE-2021-27102**، **CVE-2021-27104**)
  - ✓ **SSRF** به وسیله درخواست دستکاری‌شده **POST**
- لزوم آموزش سازمانی، بروزرسانی، تست وب و شبکه

باج‌افزارهای رایج در سال ۲۰۲۱
و
راه نفوذ آن‌ها

Pay Or Grief:

- دسترسی اولیه با ارسال ایمیل‌های حاوی فایل مخرب **Excel**
- لزوم آموزش سازمانی، لزوم تقویت واحد **SOC**



Avaddon:

- **RaaS**
- دسترسی اولیه با ارسال ایمیل حاوی فایل فشرده **JavaScript** و اجرای **payload** بدافزار

RaaS
باج‌افزار به عنوان سرویس

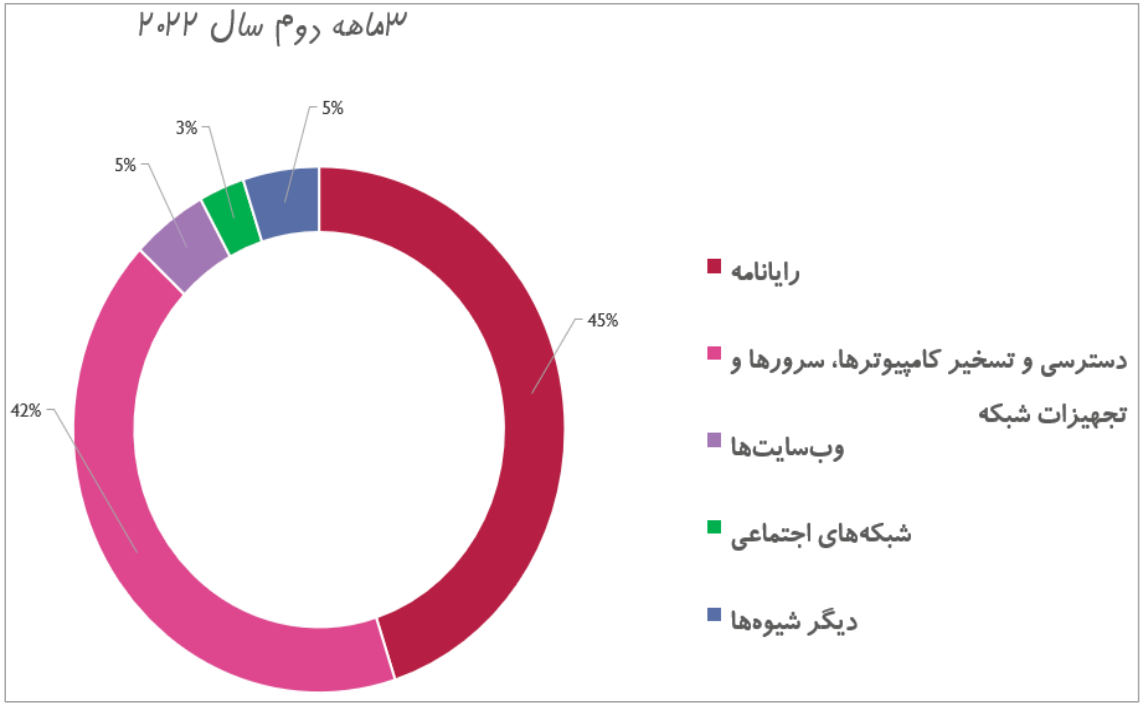
❖فروش باج افزار به عنوان سرویس:

✓افزایش سطح خطر
✓حملات با هدف مشخص و دقیق

علائم آلودگی

- کند شدن سیستم
- مشاهده مداوم خطا و صفحه آبی
- ری استارت شدن مداوم
- عدم دسترسی به فایل‌ها، برنامه‌ها یا هارد درایو
- نمایش پیغام‌های خطا بیش از حد معمول یا نا به جا
- اضافه شدن یا حذف آیکون ها
- اضافه شدن فایل یا فولدرها)ناپدید شدن(
- تغییرنام فایل ها)file.txt.exe(
- غیرفعال شدن آنتی ویروس‌ها
- غیرفعال شدن System Restore

شیوه‌های رایج گسترش بدافزارها



راه‌های انتقال بدافزار

- استفاده آسیب‌پذیری‌ها
- ارسال از طریق ایمیل
- استفاده از تکنیک‌های Phishing
- استفاده از فلش و ...
- دانلود از وب سایت ها
  - نرم افزارهای کاربردی
  - عادات رفتاری Watering hole

راهکارهای حذف بدافزار

همیشه از اطلاعات مهم خود پشتیبان داشته باشید

- تشخیص علائم آلودگی
- ایزوله کردن سیستم آلوده
- غیرفعال کردن System Restore
- اصلاح سیستم و حذف بد افزار
- تنظیم زمانبندی برای به روز رسانی و اسکن
- فعال کردن system Restore و ساخت یک اسنپشات
- آموزش و آگاهی رسانی کاربران

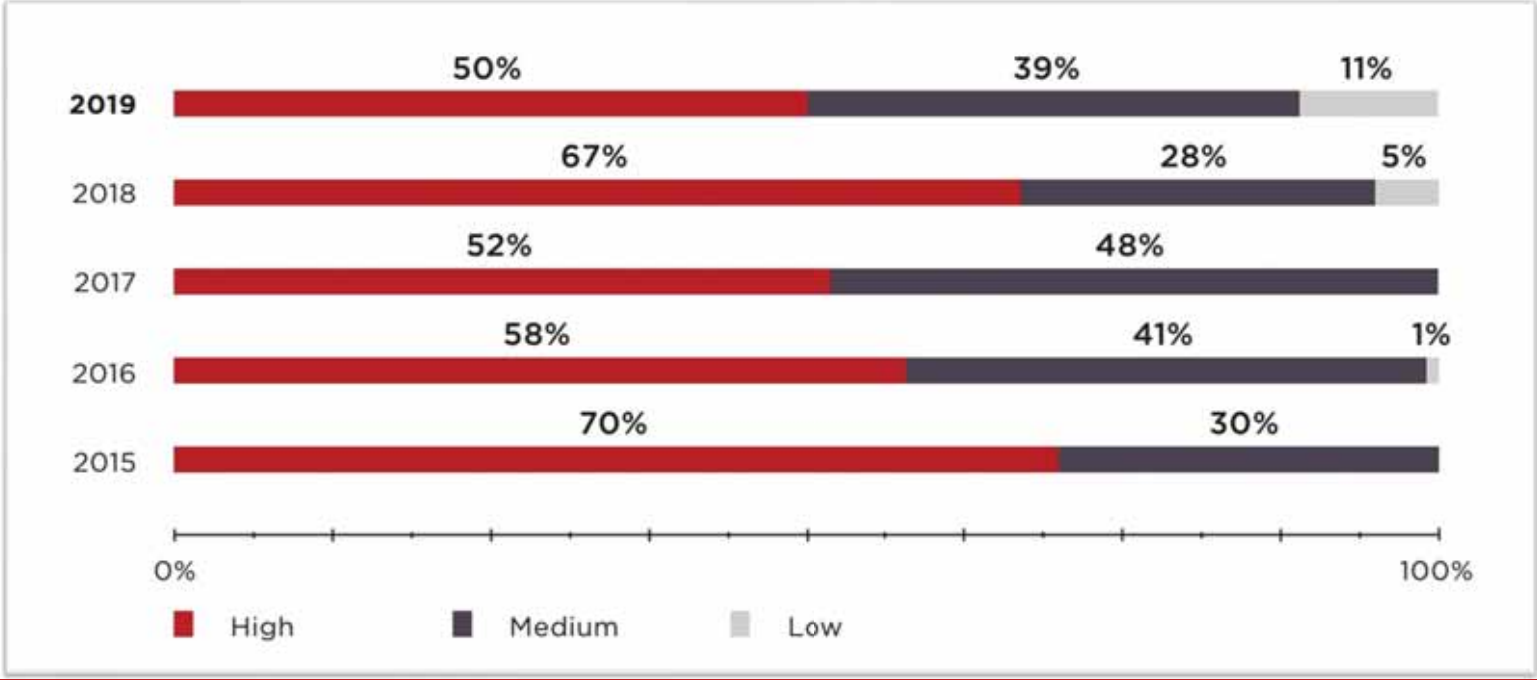
جلوگیری از آلوده شدن

- به روز بودن سیستم عامل
- استفاده از یک آنتی ویروس مناسب و بروز
- عدم استفاده از نرم‌افزارهای ناآشنا و کرک شده
- دانلود نرم‌افزارها از سایت‌های معتبر
- باز نکردن ایمیل‌های ناشناس و داشتن لیست سفید
- عدم استفاده از فلش یا هارد اکسترنال ناشناس
- آموزش و آگاهی رسانی به کاربران برای استفاده ایمن از اینترنت

آسیب‌پذیری‌های برنامه‌های کاربردی

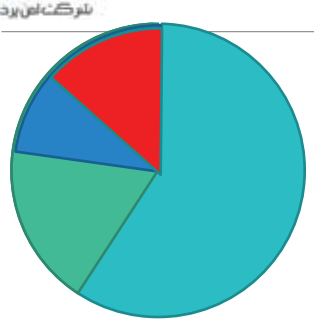
آسیب‌پذیری‌ها به زبان آمار
)آمار جهانی(

وبسایت ها با ماکزییم سطح خطر



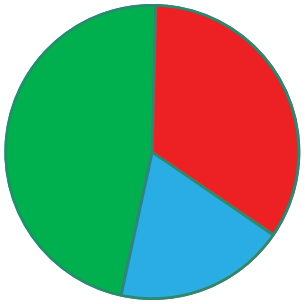
https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/
https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020

آسیب‌پذیری‌ها به زبان آمار
)آمار جهانی(



در سال 2019

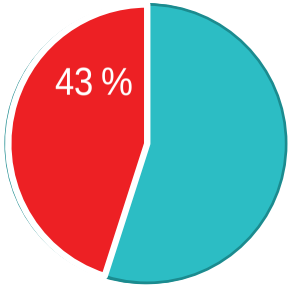
- دسترسی غیر مجاز 39%
  - کنترل کامل 16%
  - دسترسی به شبکه داخلی 8%



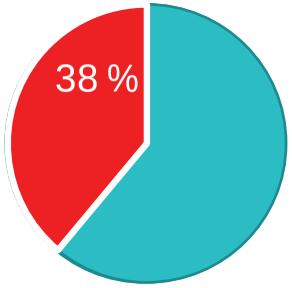
- افشای اطلاعات حساس 68%
  - اطلاعات افراد 47%
  - اطلاعات احراز اصالت 31%
  - سایر اطلاعات 22%

https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/
https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020

آسیب‌پذیری‌ها به زبان آمار
)آمار جهانی(



- 43% برنامه های اندرویدی آسیب‌پذیری با سطح خطر بالا دارند.



- 38% برنامه های مبتنی بر iOS آسیب‌پذیری با سطح خطر بالا دارند.

https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019

آسیب‌پذیری‌ها به زبان آمار
)آمار جهانی(

- در 89% از برنامه‌های آسیب‌پذیر، مهاجم جهت بهره‌برداری از آسیب‌پذیری نیاز به دسترسی فیزیکی ندارد.

- آسیب‌پذیری‌های مرتبط با احراز هویت:
  - 41% از برنامه‌های کاربردی احراز هویت را در سمت کلاینت انجام می دهند.
  - 18% از برنامه‌های کاربردی آسیب‌پذیری‌هایی مرتبط با دزدیدن نشست دارند.
  - 18% از برنامه‌های کاربردی دفعات تلاش برای احراز هویت را محدود نکرده‌اند.

https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019

Session hijacking

راهکارهای پیشگیری

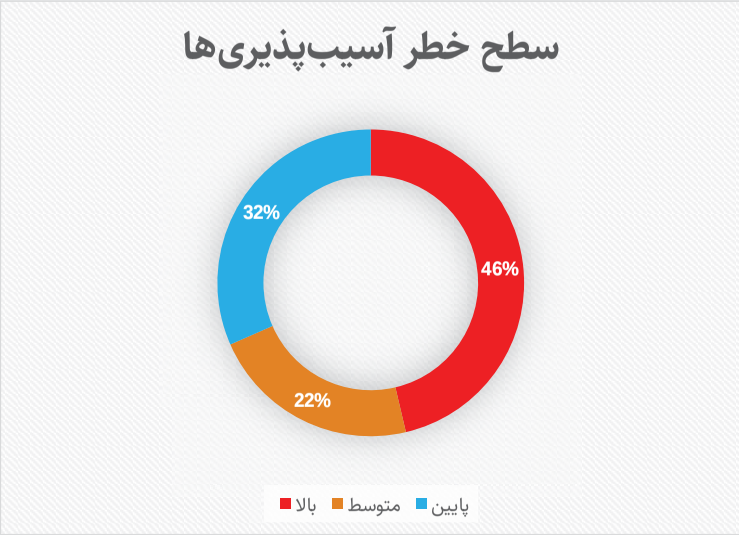
- HTTPS
- HTTPOnly
- System Updates
- Session Management
- Session Key
- Identity Verification
- Public Hotspot
- VPN
- Phishing Scam

آسیب‌پذیری‌ها به زبان آمار
)آمار داخلی(

18 سامانه با عمر کمتر از 5 سال

تمام سامانه‌ها حداقل یک آسیب‌پذیری با سطح خطر بالا دارند.

به طور متوسط هر سامانه 4.5 آسیب‌پذیری دارد.

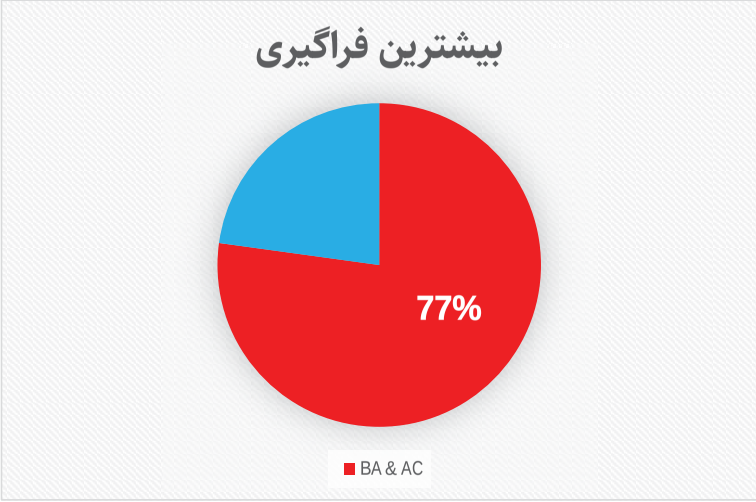


آسیب‌پذیری‌ها به زبان آمار)11(

)آمار داخلی(

بیشترین آسیب‌پذیری از لحاظ فراوانی : XSS

بیشترین آسیب‌پذیری از لحاظ فراگیری:



Broken Authentication

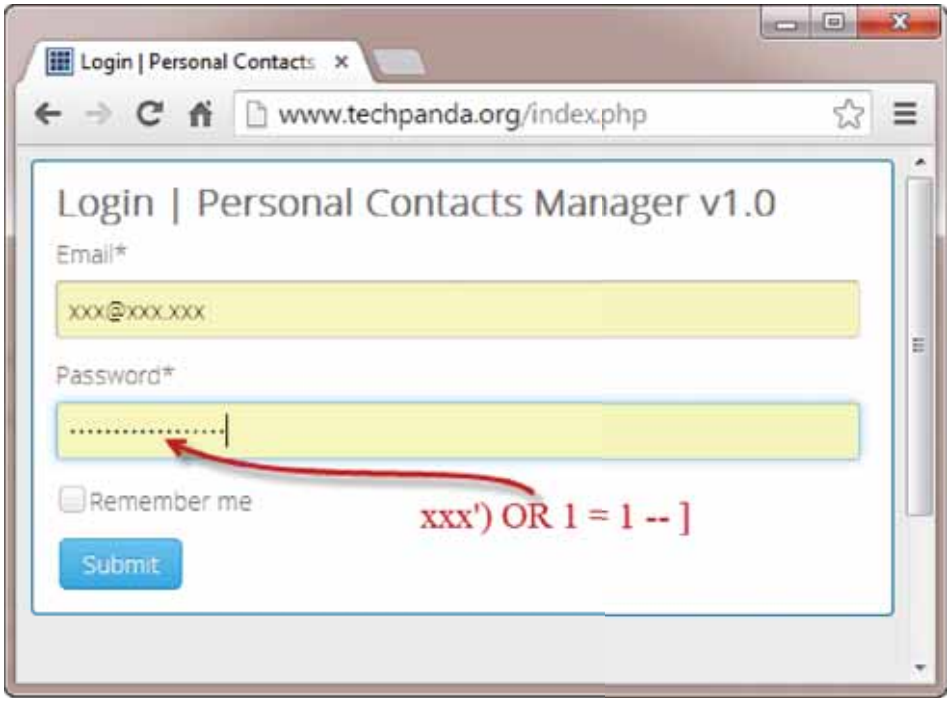
- Predictable login credentials
- User authentication credentials that are not protected when stored
- Session IDs exposed in the URL (e.g., URL rewriting)
- Session IDs vulnerable to session fixation attacks
- Session value that does not time out or get invalidated after logout
- Session IDs that are not rotated after successful login
- Passwords, session IDs, and other credentials sent over unencrypted connections

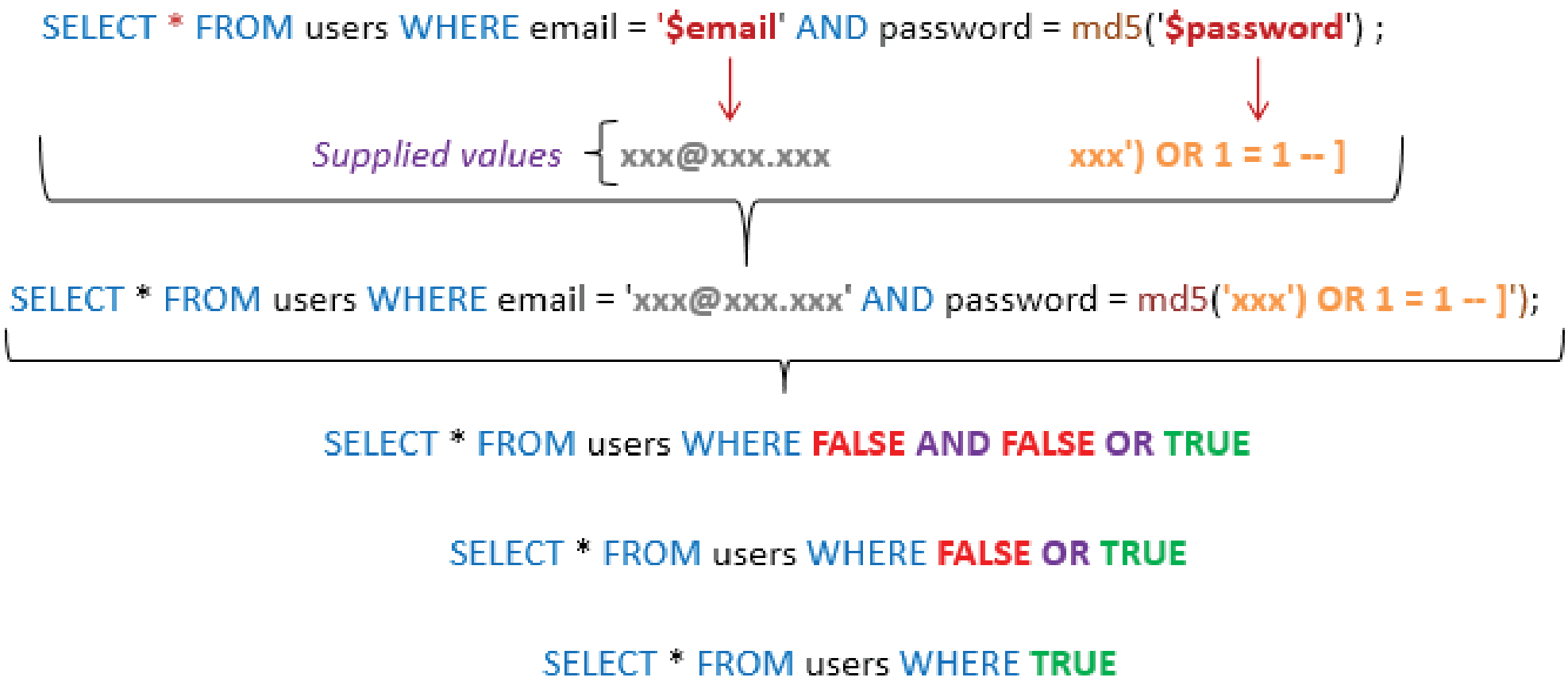
حملات تزریق کد

- عدم کنترل دقیق ورودی‌های کاربر
- تزریق کد یا دستور از طریق ورودی ها به سامانه

- SQLinjection
- XSS
- Command injection

تزریق SQL)۱(


Login | Personal Contacts
www.techpanda.org/index.php
Login | Personal Contacts Manager v1.0
Email*
xxx@xxx.xxx
Password*
Remember me
xxx') OR 1 = 1 --]
Submit


SELECT * FROM users WHERE email = '$email' AND password = md5('$password') ;
Supplied values
xxx@xxx.xxx
xxx') OR 1 = 1 --]
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 --]');
SELECT * FROM users WHERE FALSE AND FALSE OR TRUE
SELECT * FROM users WHERE FALSE OR TRUE
SELECT * FROM users WHERE TRUE

تزریق SQL)۲(

- پیشگیری از SQLi

- Use of Prepared Statements (with Parameterized Queries)
- Use of Properly Constructed Stored Procedures
- Allow-list Input Validation
- Escaping All User Supplied Input

- Enforcing Least Privilege

جمع بندی

- به روز رسانی سیستم‌ها و برنامه‌ها
- استفاده از برنامه‌های آنتی ویروس به روز شده
- ساخت لیست سفید برای ایمیل‌ها
- کسب آگاهی از روش‌های مهندسی اجتماعی
- کنترل ورودی‌ها)خروجی‌ها(
- رعایت نکات ساده اما حیاتی در احراز اصالت
- کسب اطمینان از صحت عملکرد مکانیزم‌های امنیتی
- آزمون نفوذ دوره‌ای

نمایش یک سناریو نفوذ واقعی

خدمات آزمون نفوذ

چالش‌ها

تست نفوذ یا ارزیابی امنیتی

تعریف ارزیابی امنیتی:

- جستجوی منظم و سیستماتیک برنامه‌ها، سیستم‌ها یا شبکه‌ها جهت یافتن نقاط آسیب پذیر و مستعد نفوذ.

تعریف تست نفوذ:

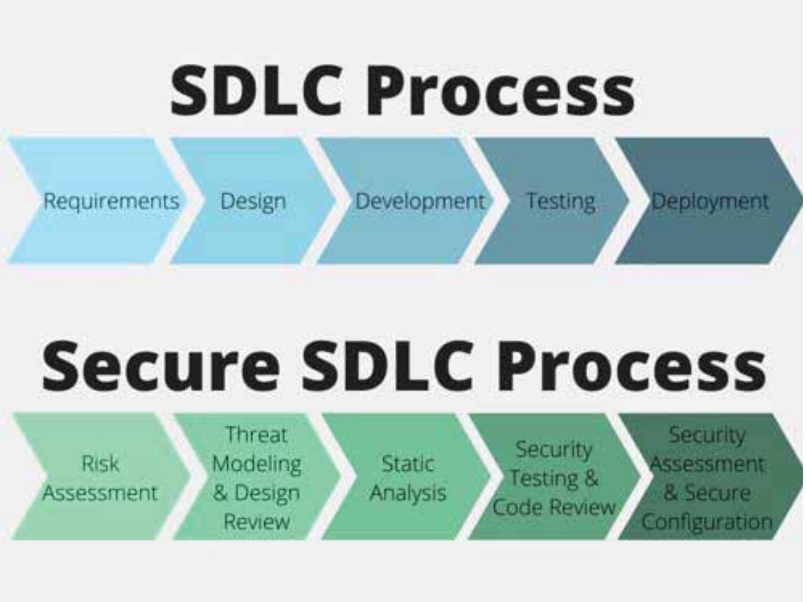
- تلاش در جهت بهره برداری از نقاط ضعف احتمالی برنامه‌ها، سیستم‌ها یا شبکه‌ها با هدف اثبات وجود آسیب‌پذیری و مشخص کردن میزان دقیق خسارت‌ها و پیامدهای آن.

مزایای ارزیابی امنیتی

- شناخت نقاط ضعف و آسیب‌پذیر
  - محافظت از دارایی‌ها)سرمایه، دانش، اسناد، حریم خصوصی و ...(
  - خوش بینی مشتریان، شرکاء، سهامداران
- برآورده کردن الزامات قانونی
- نفوذ ادبیات امنیت به درون سازمان یا کسب‌وکار
- شناخت میزان آگاهی داخلی سازمان نسبت به موضوع ا
  - تدوین برنامه های آموزشی

ارزیابی امنیتی : چه وقت؟

- در طول چرخه توسعه



- پس از استقرار
  - حداقل به صورت سالانه
  - پس از اعمال به روزرسانی‌ها و تغییرات

آزمون خودکار vs آزمون دستی

آزمون خودکار:

- سریع
- انجام جامع آزمون‌های تعریف شده
- مثبت غلط بالا
- عدم امکان انجام برخی آزمون‌ها

آزمون دستی:

- زمان و هزینه بیشتر
- نیاز به افراد متخصص و خبره
- نتایج دقیق تر
- انجام آزمون‌های خلاقانه

- آزمون خودکار
- آزمون خودکار و اثبات دستی
- آزمون دستی و اثبات دستی

ابزارهای آزمون خودکار توسط افراد خبره تنظیم می‌شوند و افراد خبره معمولا از ابزارهای خوکار مختلفی استفاده می‌کنند.

ارزیابی امنیتی برنامه کاربردی : اصلی یا پشتیبان

- سامانه اصلی
  - احتمال اختلال در عملکرد سامانه)کیفیت سرویس، صحت داده‌ها، ...(
  - زمان بیشتر آزمون
- پشتیبان
  - احتمال عدم آزمون سامانه در محیط واقعی
  - آزمون با سرعت و دقت بالاتر

مهاجم VS ارزیاب

- مهاجم
  - زمان نامحدود
  - تنها یک نقطه آسیب‌پذیر
- ارزیاب
  - زمان محدود
  - تمام آسیب‌پذیری‌ها
  - همکاری توسعه دهنده

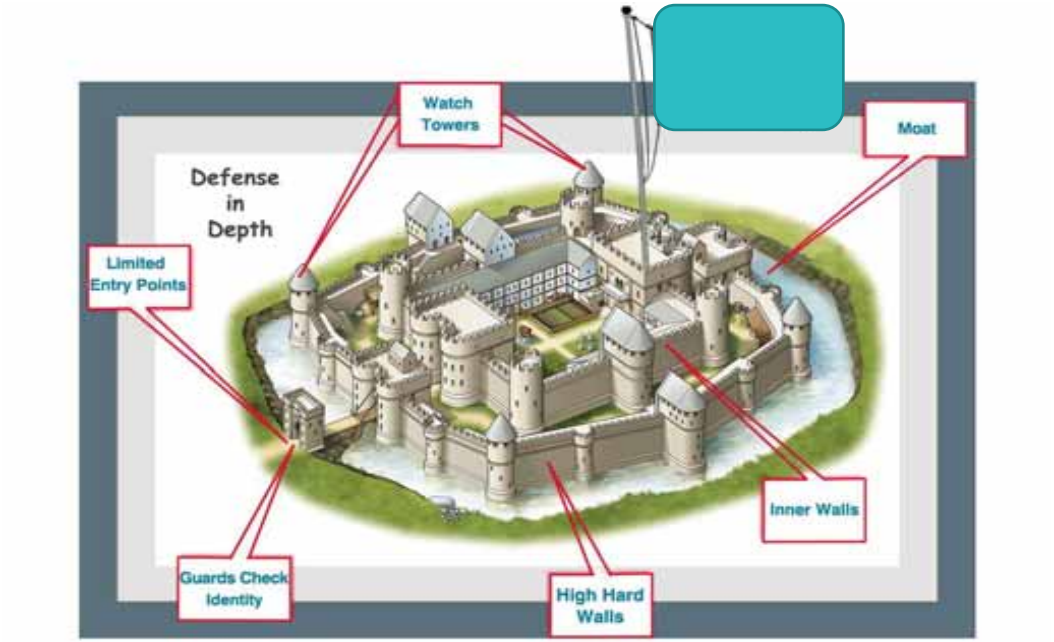
سخن آخر

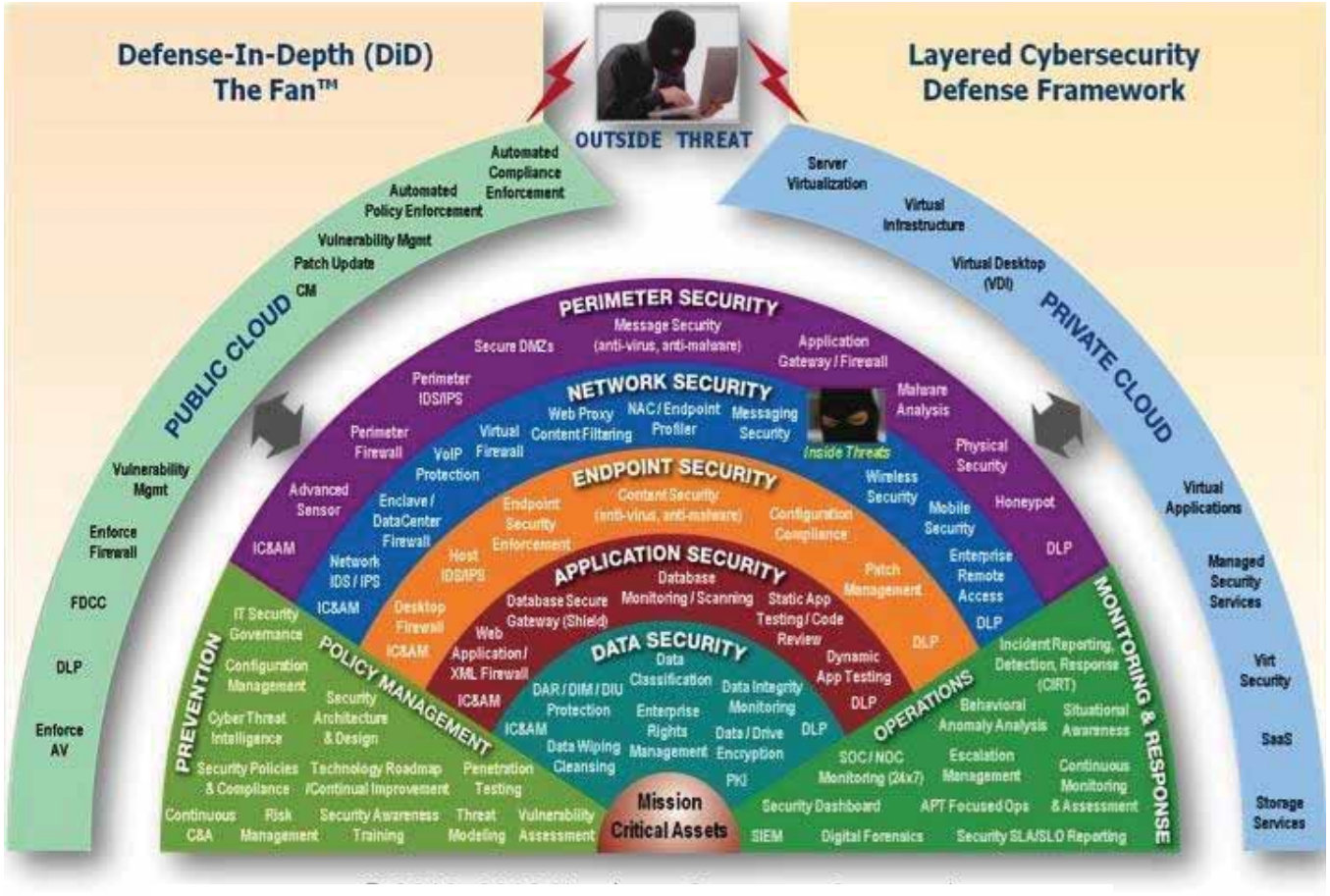
- ارزیابی امنیتی برنامه کاربردی :
  - نباید محدود به یکبار باشد.
  - آزمودن مولفه‌ها در حین توسعه نمی تواند جایگزین آزمون نهایی سامانه شود.
  - در هنگام ارزیابی برنامه کاربردی از فایروال و WAF استفاده نشود.

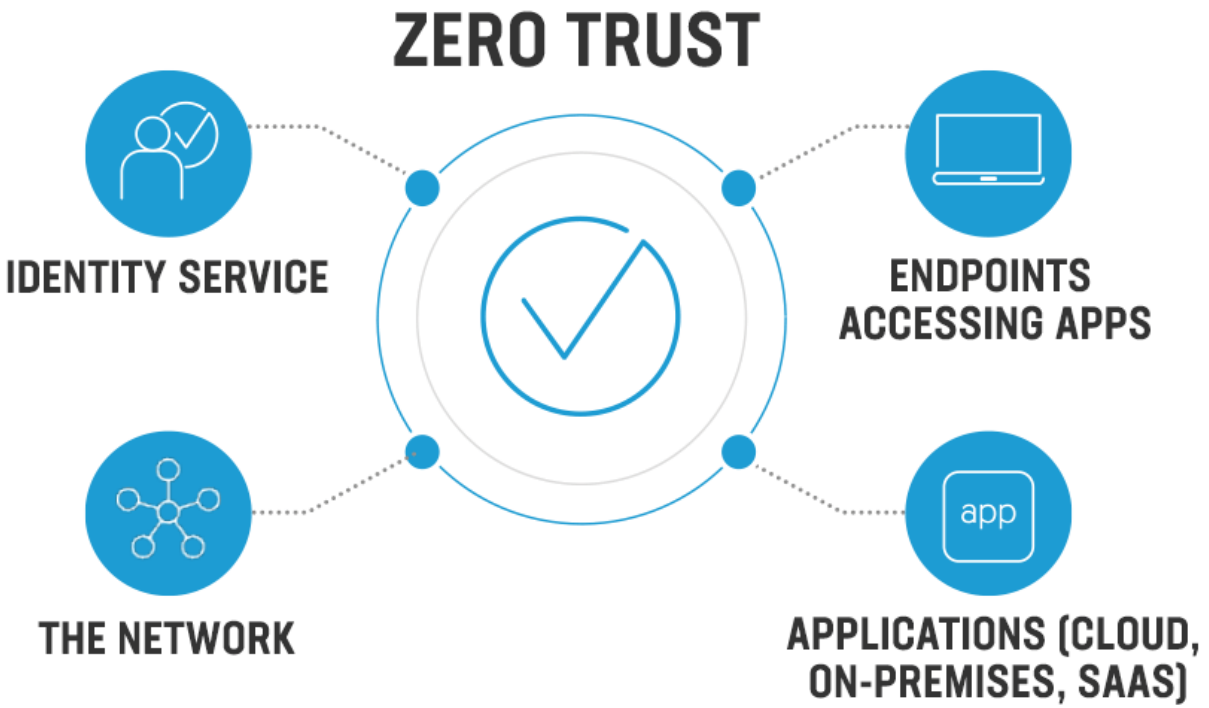
- همه‌ی امنیت، ارزیابی امنیتی برنامه کاربردی نیست.
  - کاربران
  - آموزش
  - طرح بازیابی کسب وکار

امنیت سایبری در سازمان

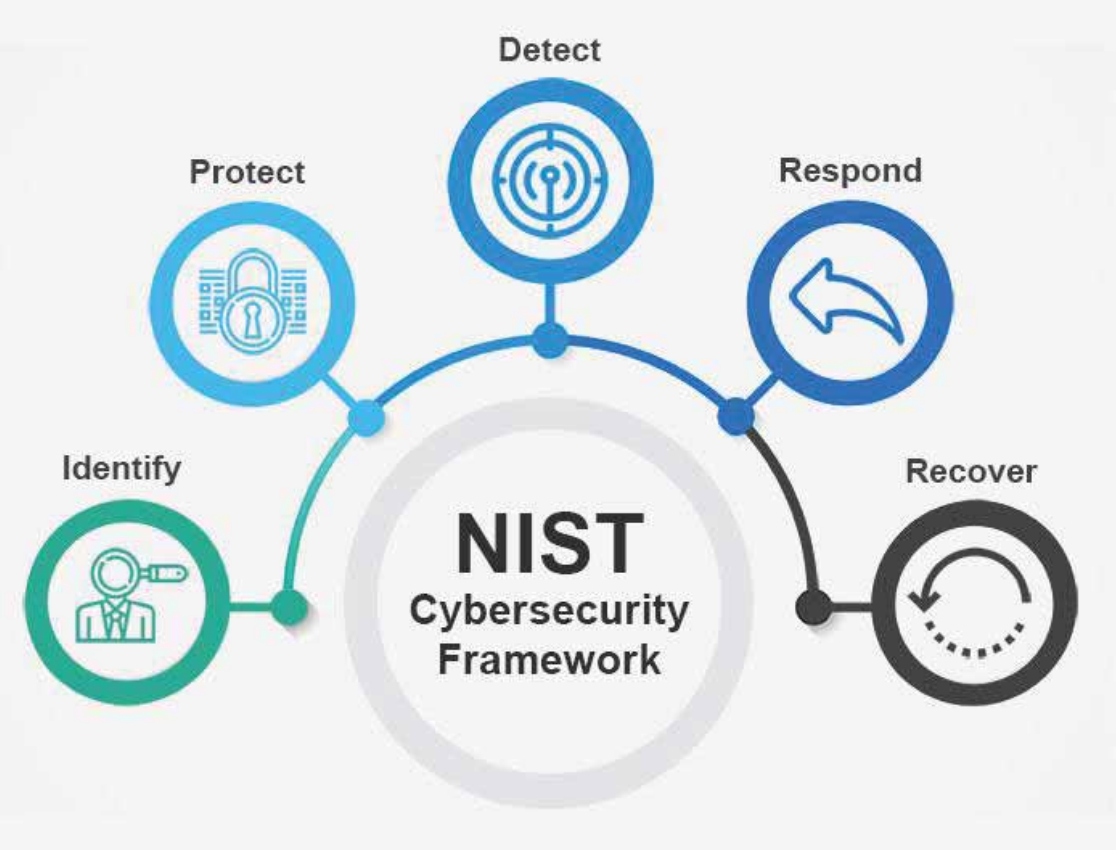
دفاع در عمق


Defense
in
Depth
Watch
Towers
Moat
Limited
Entry Points
Inner Walls
Guards Check
Identity
High Hard
Walls

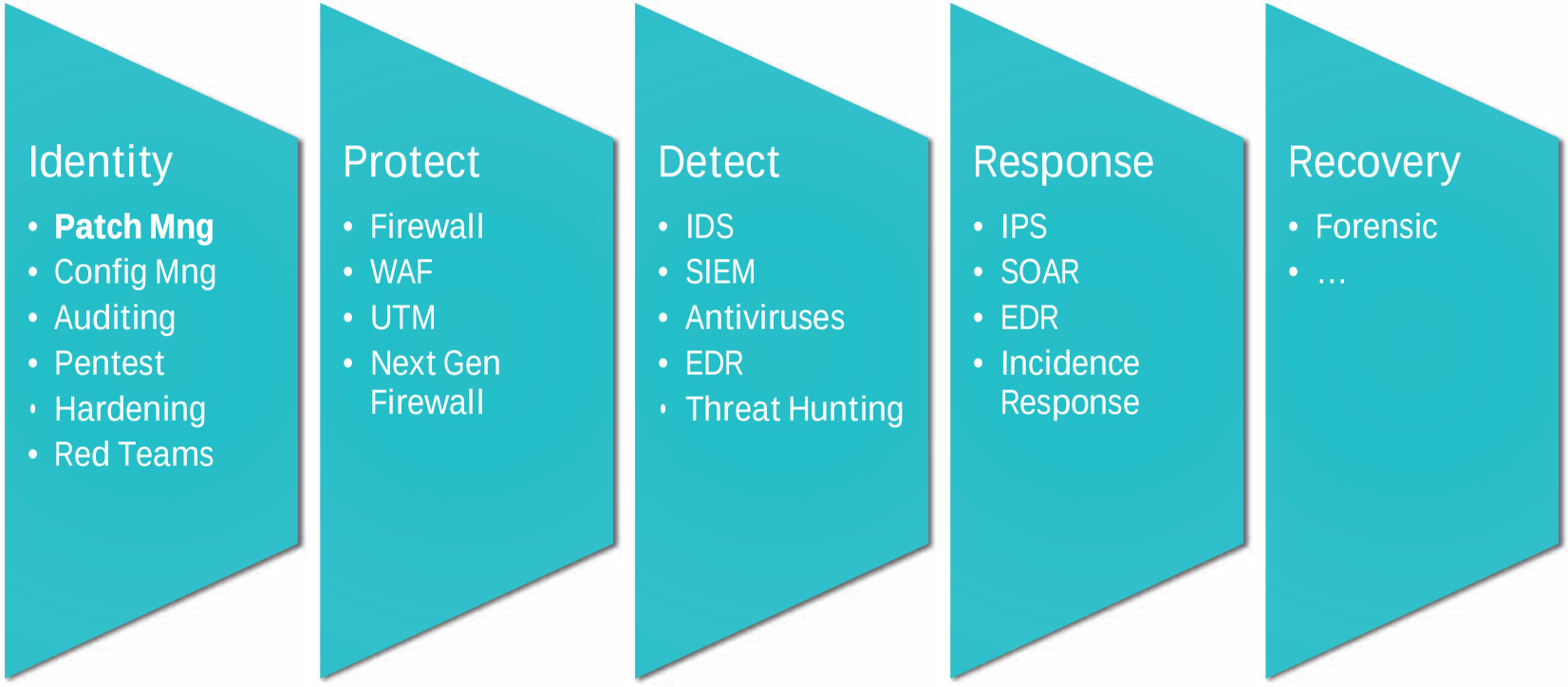

Defense-In-Depth (DiD)
The Fan™
Layered Cybersecurity
Defense Framework
OUTSIDE THREAT
PUBLIC CLOUD
PRIVATE CLOUD
Automated Compliance Enforcement
Automated Policy Enforcement
Vulnerability Mgmt
Patch Update
CM
Server Virtualization
Virtual Infrastructure
Virtual Desktop (VDI)
Virtual Applications
Managed Security Services
Virt Security
SaaS
Storage Services
Vulnerability Mgmt
Enforce Firewall
FDCC
DLP
Enforce AV
PERIMETER SECURITY
Message Security (anti-virus, anti-malware)
Secure DMZs
Application Gateway / Firewall
Perimeter IDS/IPS
NETWORK SECURITY
Web Proxy
NAC / Endpoint Profiler
Messaging Security
Malware Analysis
Perimeter Firewall
VoIP Protection
Virtual Firewall
Content Filtering
Inside Threats
Physical Security
Advanced Sensor
Enclave / DataCenter Firewall
ENDPOINT SECURITY
Content Security (anti-virus, anti-malware)
Wireless Security
Mobile Security
Honeypot
Endpoint Security Enforcement
Configuration Compliance
IC&AM
Network IDS / IPS
Host IDS/IPS
APPLICATION SECURITY
Database Monitoring / Scanning
Patch Management
Enterprise Remote Access
DLP
Database Secure Gateway (Shield)
Static App Testing / Code Review
Desktop Firewall
Web Application / XML Firewall
DATA SECURITY
Data Classification
Dynamic App Testing
IT Security Governance
Configuration Management
Security Architecture & Design
DAR / DIM / DIU Protection
Data Integrity Monitoring
Enterprise Rights Management
Data / Drive Encryption
Data Wiping Cleansing
PKI
PREVENTION
POLICY MANAGEMENT
OPERATIONS
MONITORING & RESPONSE
Incident Reporting, Detection, Response (CIRT)
Behavioral Anomaly Analysis
Situational Awareness
Cyber Threat Intelligence
Security Policies & Compliance
Technology Roadmap /Continual Improvement
Penetration Testing
SOC / NOC Monitoring (24x7)
Escalation Management
Continuous Monitoring & Assessment
Continuous C&A
Risk Management
Security Awareness Training
Threat Modeling
Vulnerability Assessment
Mission Critical Assets
Security Dashboard
APT Focused Ops
SIEM
Digital Forensics
Security SLA/SLO Reporting


ZERO TRUST
IDENTITY SERVICE
ENDPOINTS
ACCESSING APPS
app
THE NETWORK
APPLICATIONS (CLOUD,
ON-PREMISES, SAAS)


LOG COLLECTION
AGGREGATION CORRELATION
REPORTING
SIEM
SOC
RESEARCH & DEVELOPMENT
TICKETING
THREAT INTELLIGENCE
KNOWLEDGE BASE


Detect
Protect
Respond
Identify
Recover
NIST
Cybersecurity
Framework

زنجیره‌ی دفاعی سازمان



مروری بر ابزارها و تجهیزات و راهکارهای امنیتی

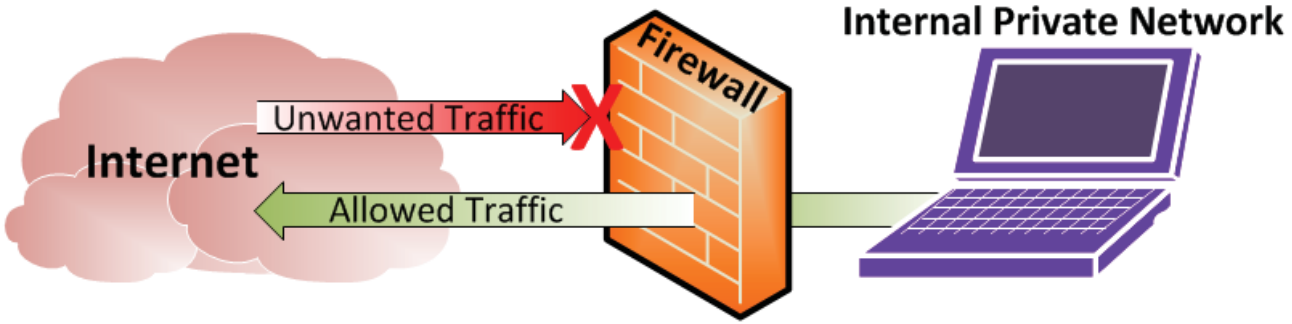
Firewall, IDS/IPS, SIEM, SOAR, EDR/XDR

دیواره آتش

Firewall

اهداف

تمام ترافیک باید توسط فایروال بررسی و تایید شود. چه ورود چه خروج
تنها ترافیک‌های مجاز اجازه ورود یا خروج دارند



محدودیت‌های فایروال

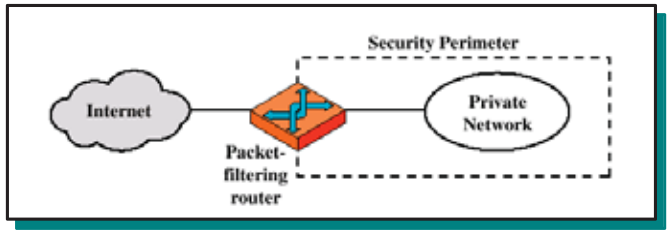
انفعال و عدم تشخیص روش‌هایی مبتنی بر دور زدن فایروال

دفاع در مقابل حملات درونی سازمان

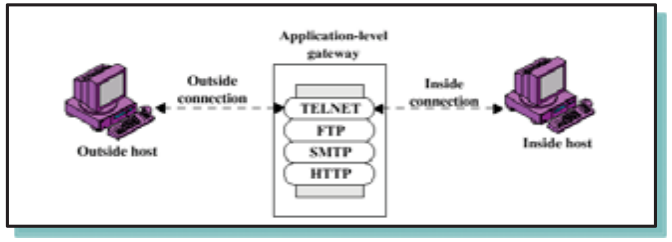
عدم تشخیص حملات مبتنی بر بدافزارها

انواع فایروال

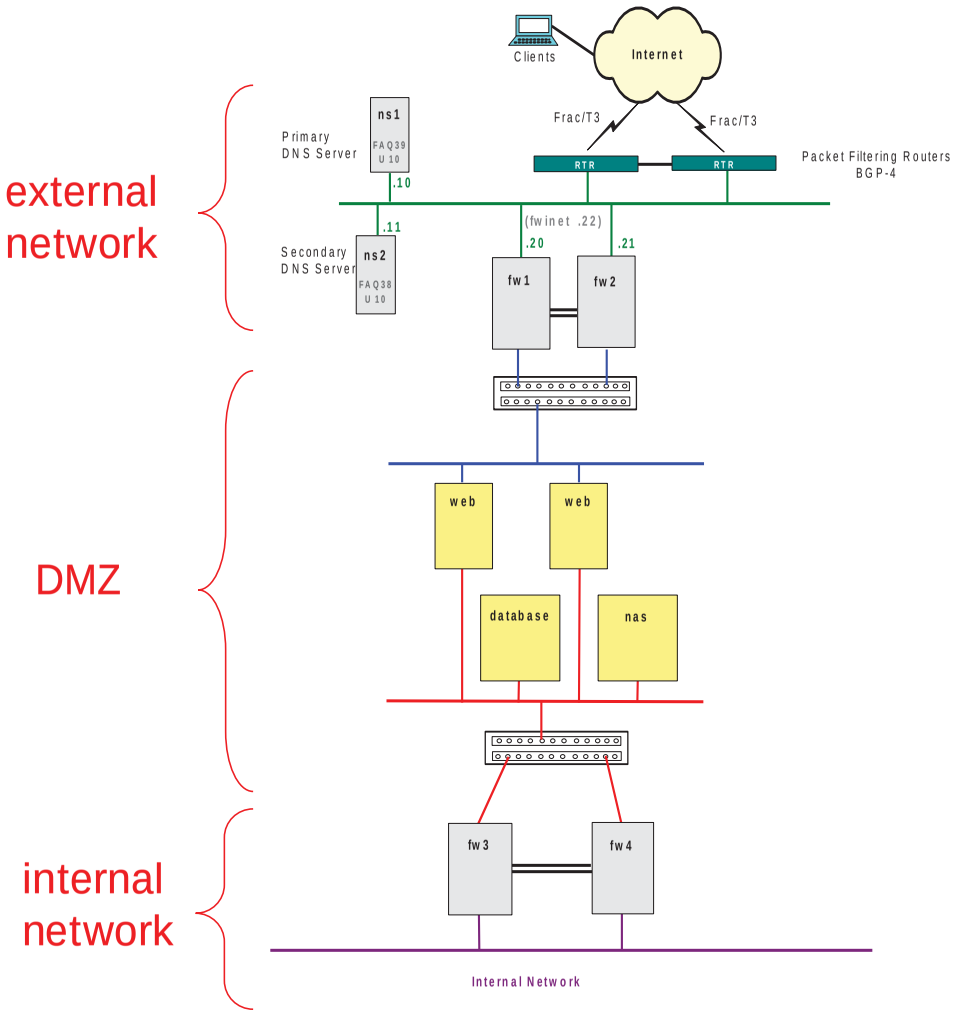
Packet Filtering Firewall



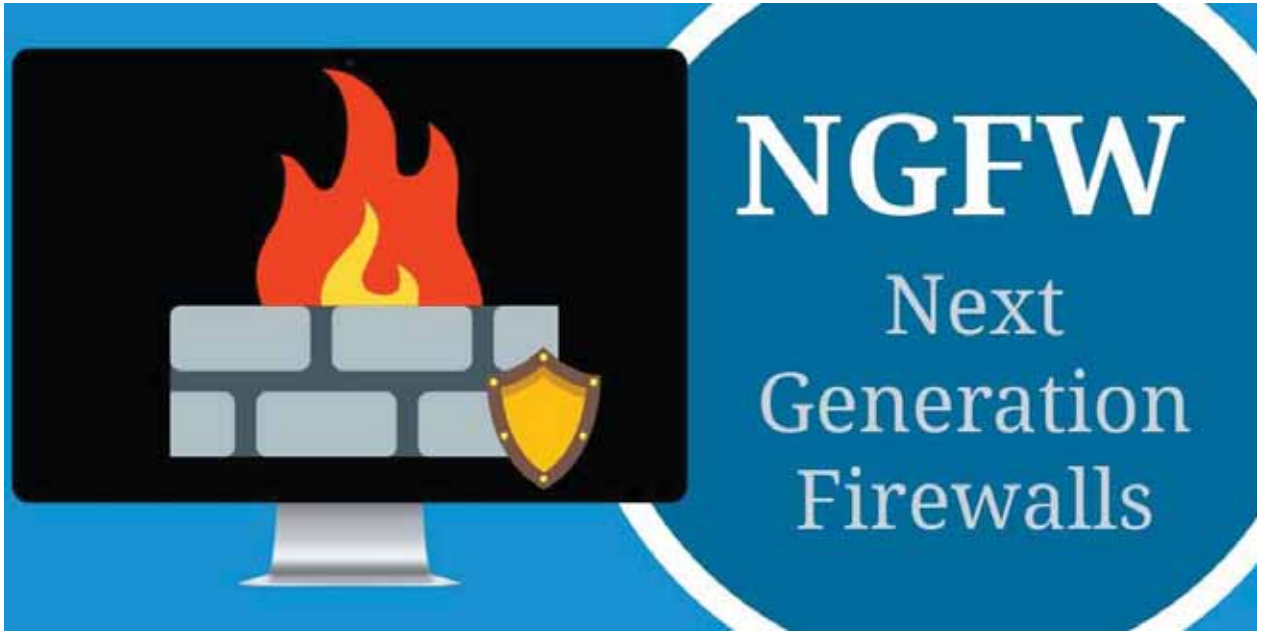
Application Level Gateway



Typical DMZ


external network
DMZ
internal network
Clients
Internet
Frac/T3
Frac/T3
RTR
RTR
Packet Filtering Routers
BGP-4
Primary DNS Server
ns1
FAQ39 U 10
.10
.11
(fwinet .22)
.20
.21
Secondary DNS Server
ns2
FAQ38 U 10
fw1
fw2
web
web
database
nas
fw3
fw4
Internal Network

NGFW



سیستم تشخیص نفوذ

Intrusion Detection System(IDS)

سیستم‌های تشخیص نفوذ

فایروال‌ها جلوی حملات خارجی را می‌گیرند

ترافیک‌های مجاز دارای حمله نیستند؟

سیستم‌های تشخیص نفوذ

واکنش غیرفعال در سیستم‌های تشخیص نفوذ سنتی

نیاز به بررسی نهایی به دلیل نقص سیستم جلوگیری از نفوذ

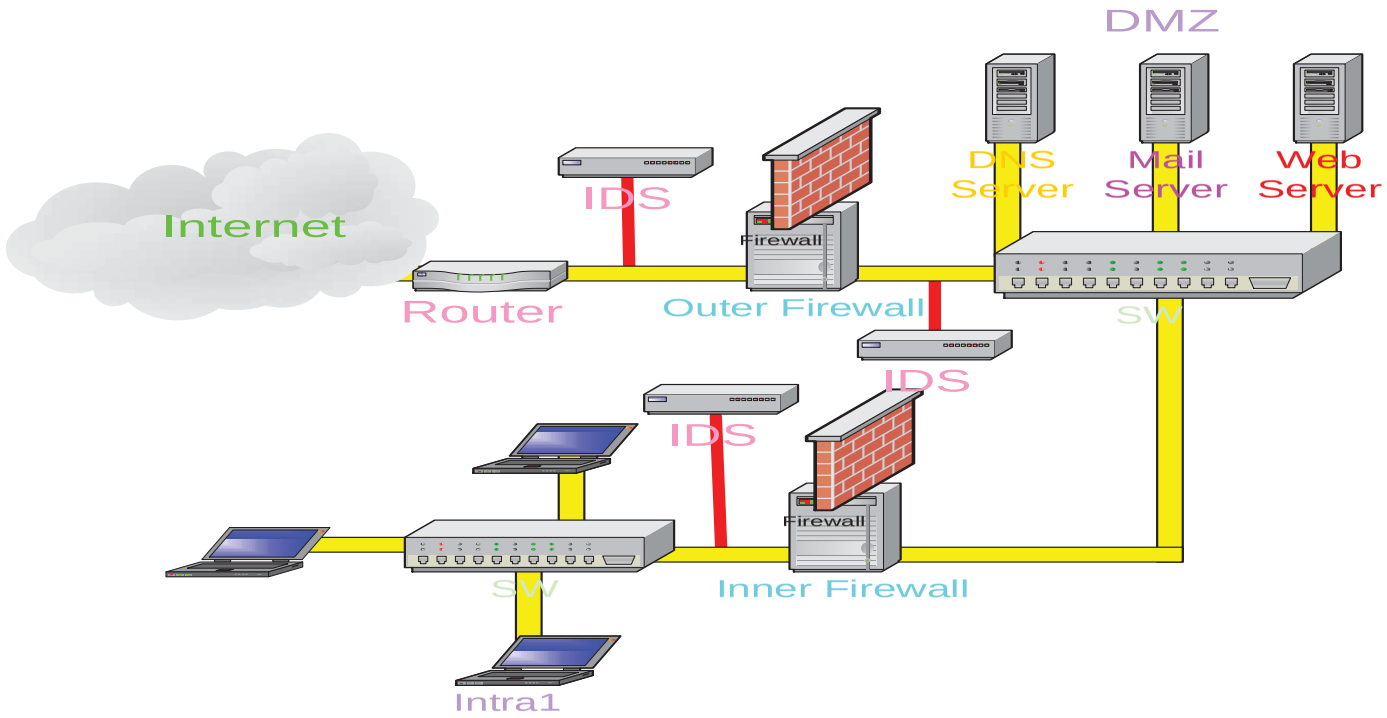
تشخیص نفوذ نسل جدید(NGIDS)

تشخیص حملات با استفاده از **امضا حمله**

تشخیص حملات بر اساس **ناهنجاریهای رفتاری**

شناسایی **رفتارهای مشکوک** در شبکه

IDS Placement



سامانه یکپارچه مدیریت تهدیدات

Unified Threat Management (UTM)

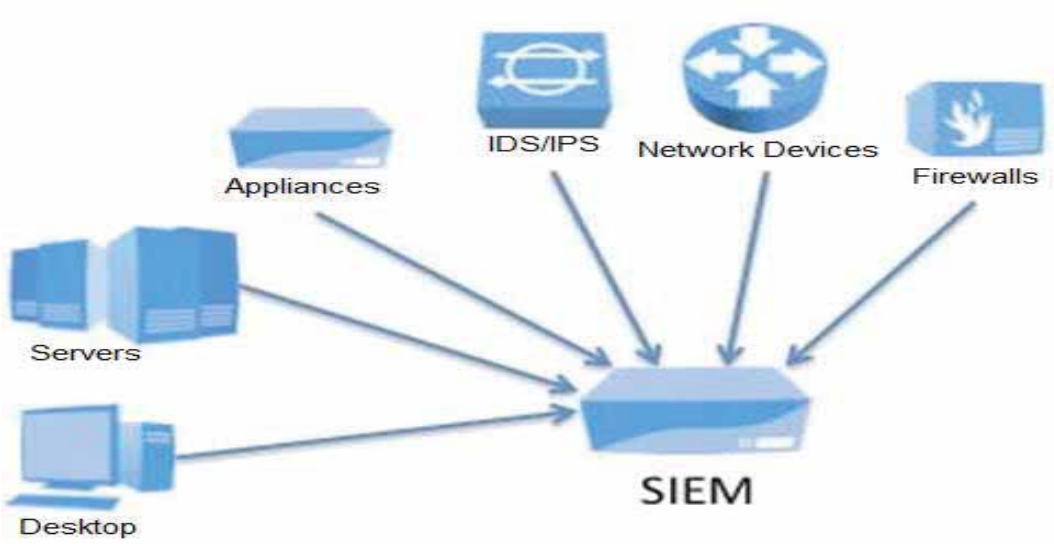
UTM

- بررسی تا لایه‌ی application
- فیلترینگ: فیلتر کردن محتوایی و آدرس (URL)
- اسکن ایمیل‌ها
- (DLP(Data loss Prevention
- اسکن با آنتی ویروس
- سرویس VPN

امنیت اطلاعات و مدیریت رویدادها

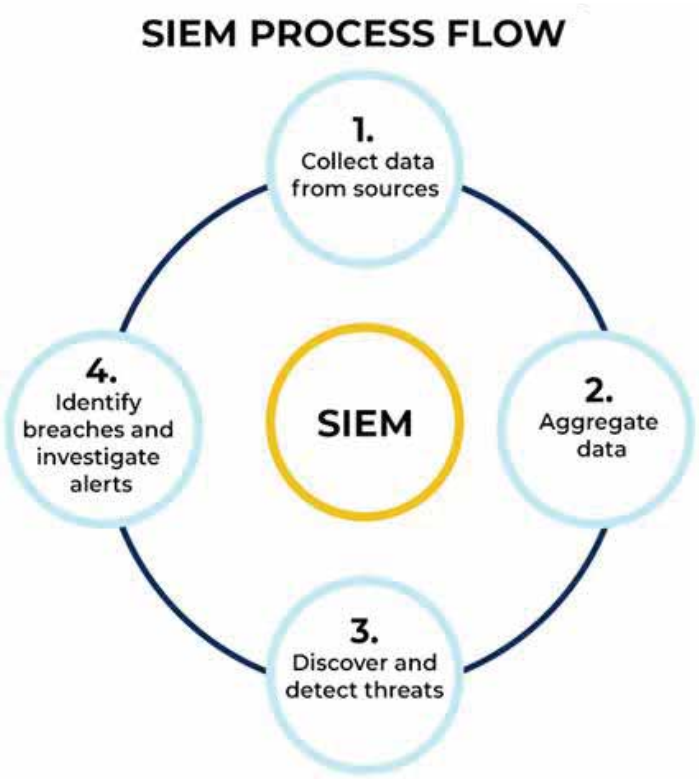
Security Information and Event Management (SIEM)

SIEM


IDS/IPS
Network Devices
Firewalls
Appliances
Servers
Desktop
SIEM

SIEM

- جمع‌آوری رویدادها و نرمال سازی
  - کاربردها، تجهیزات مختلف شبکه‌ای و حسگرهای امنیتی
- پالایش هشدارها، رخدادنماها و گزارش‌های بی مصرف
- تحلیل و همبسته‌سازی بلادرنگ رویدادها
- تطبیق رویدادها با سیاست‌های امنیتی و الگوهای حملات
  - سازمان و تطبیق با آسیب‌پذیری‌های سازمان
- تشخیص و اولویت بندی حوادث امنیتی
  - از میان میلیونها رویداد خام



شناسایی و پاسخ به حوادث نقاط پایانی

Endpoints Detection and Response (EDR)

EDR

- تشخیص فعالیت‌های مشکوک
- جمع آوری اطلاعات برای پاسخگویی به حوادث و تحقیق و بررسی
- تایید حملات و ایجاد هشدار سطح بالاتر
- زنجیره اتفاقات و اکتشاف داده‌های مهم
- انجام عمل متقابل مناسب

قابلیت‌های کلیدی

فایروال و IDS و IPS در سطح نقطه‌ی انتهایی

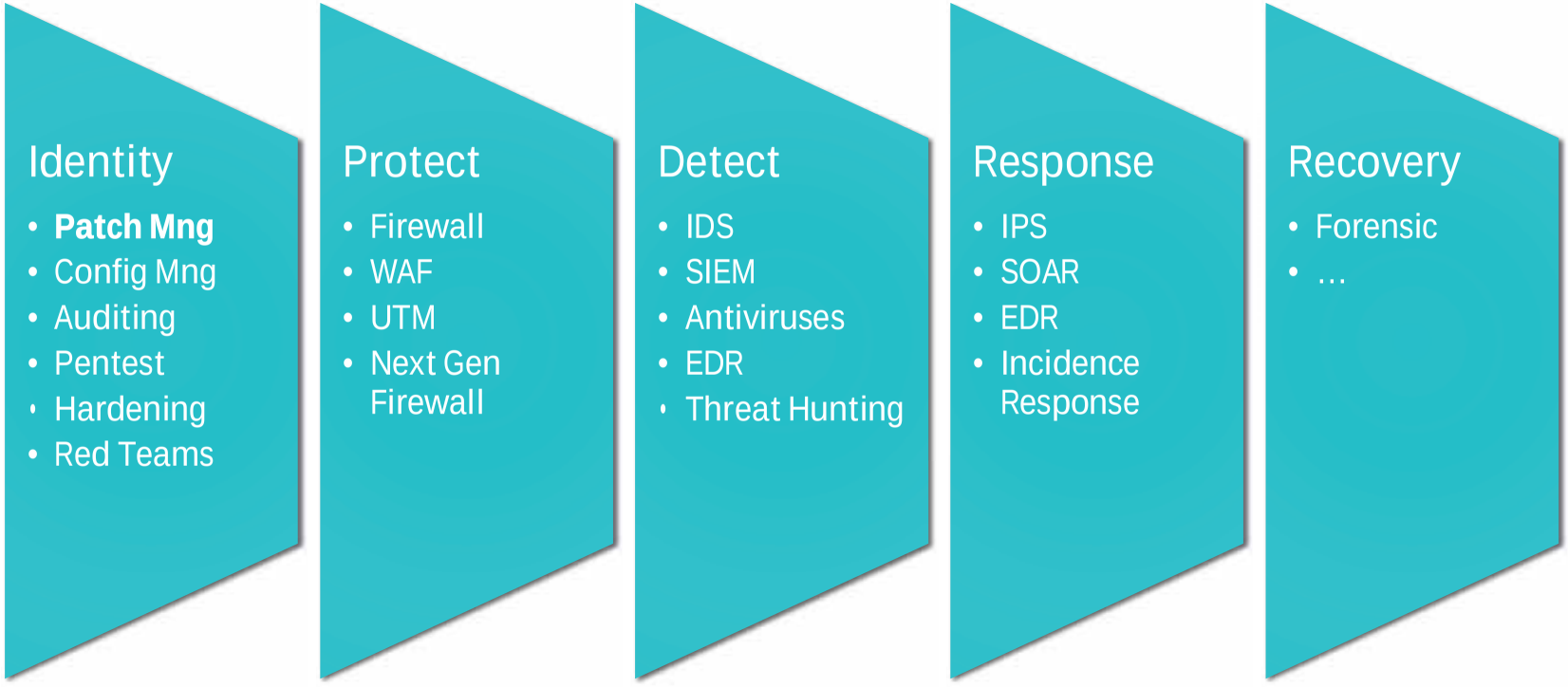
گزارش سطح ریجستری و پردازه‌های اجرا شده و سرویس‌ها

آنالیز رفتاری سیستم

ایجاد هشدارهای سطح بالا در سیستم

ایزوله کردن نقطه انتهایی

زنجیره‌ی دفاعی سازمان

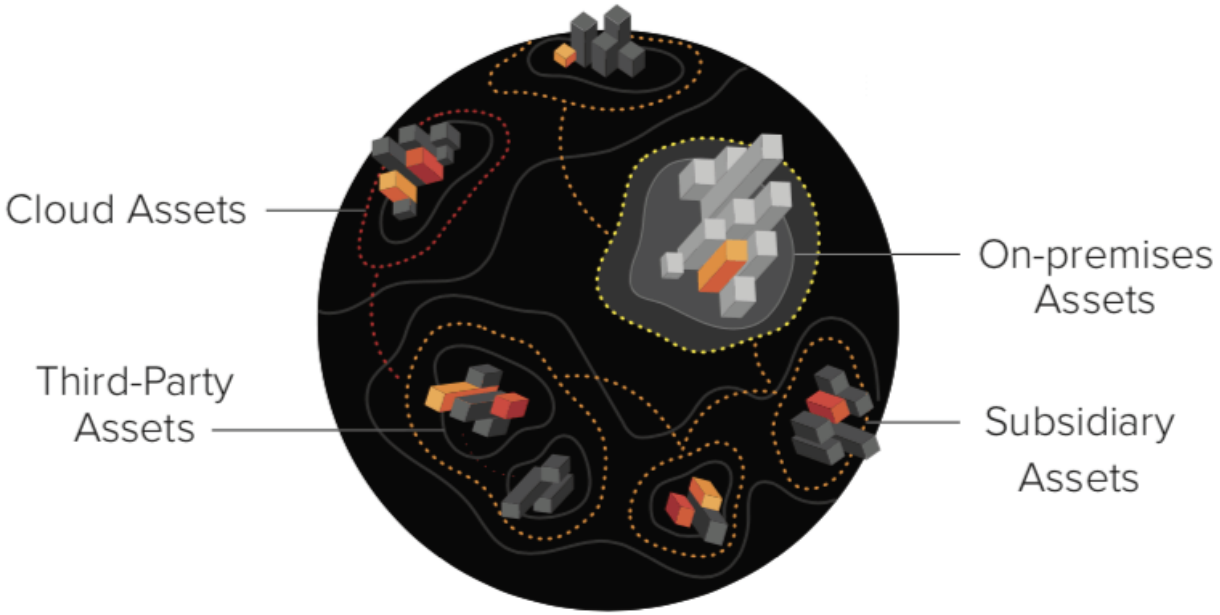


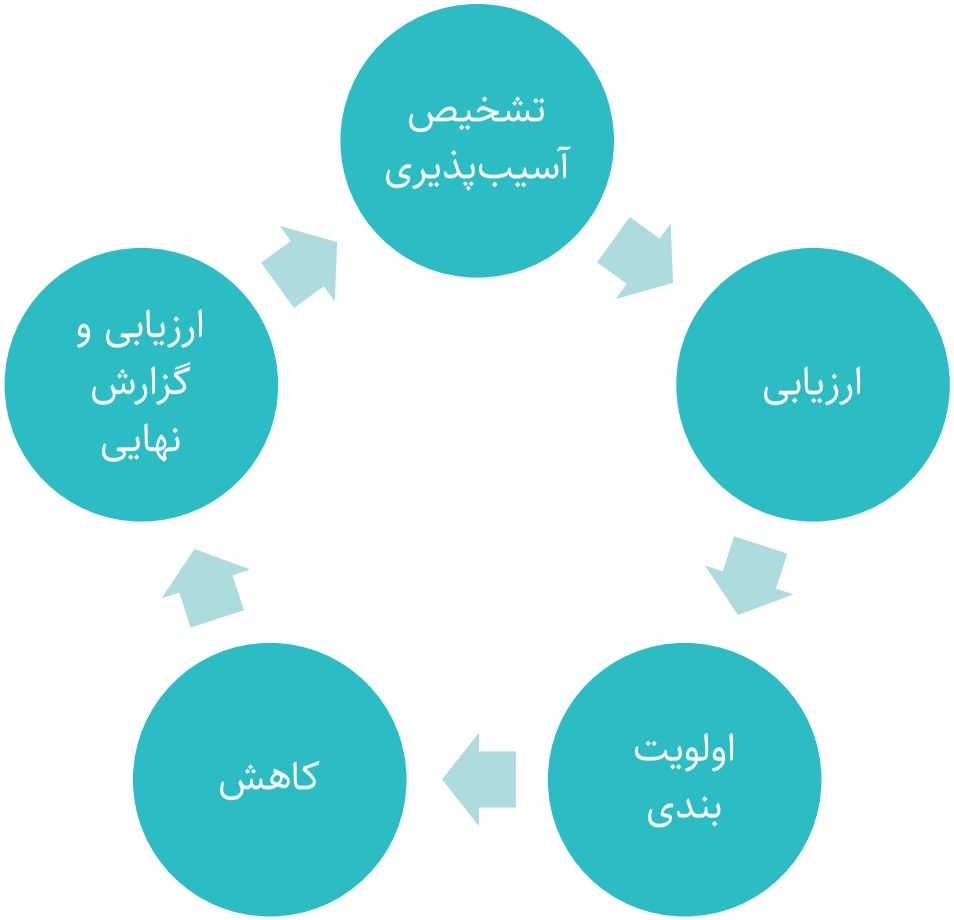
مدیریت ریسک و آسیب‌پذیری

Risk and Vulnerability Management (VM)

پیشگیری بهتر از درمان!

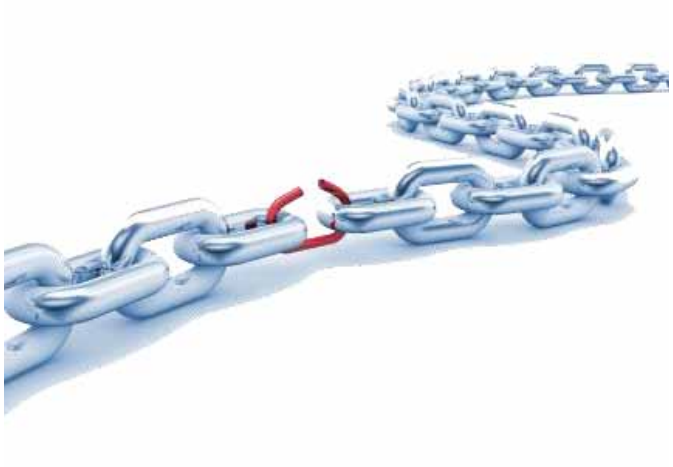
Attack Surface




تشخیص
آسیب‌پذیری
ارزیابی
اولویت
بندی
کاهش
ارزیابی و
گزارش
نهایی

عوامل آسیب‌پذیری

- انواع آسیب‌پذیری
  - آسیب‌پذیری‌های مربوط به برنامه‌ها
  - آسیب‌پذیری‌های مربوط به تنظیمات نامناسب
  - آسیب‌پذیری‌های روز صفر مخصوص مهاجمان مصمم
- آسیب‌پذیری در:
  - سرویس‌ها
  - سیستم‌عامل‌ها
  - نرم افزارها
  - تجهیزات شبکه



موارد فنی آسیب‌پذیری

مخازن آسیب‌پذیری (NVD(و شناسه آسیب‌پذیری

میزان خطرآفرین بودن CVSS)دو نسخه(

CPE: شناسه نرم افزارها

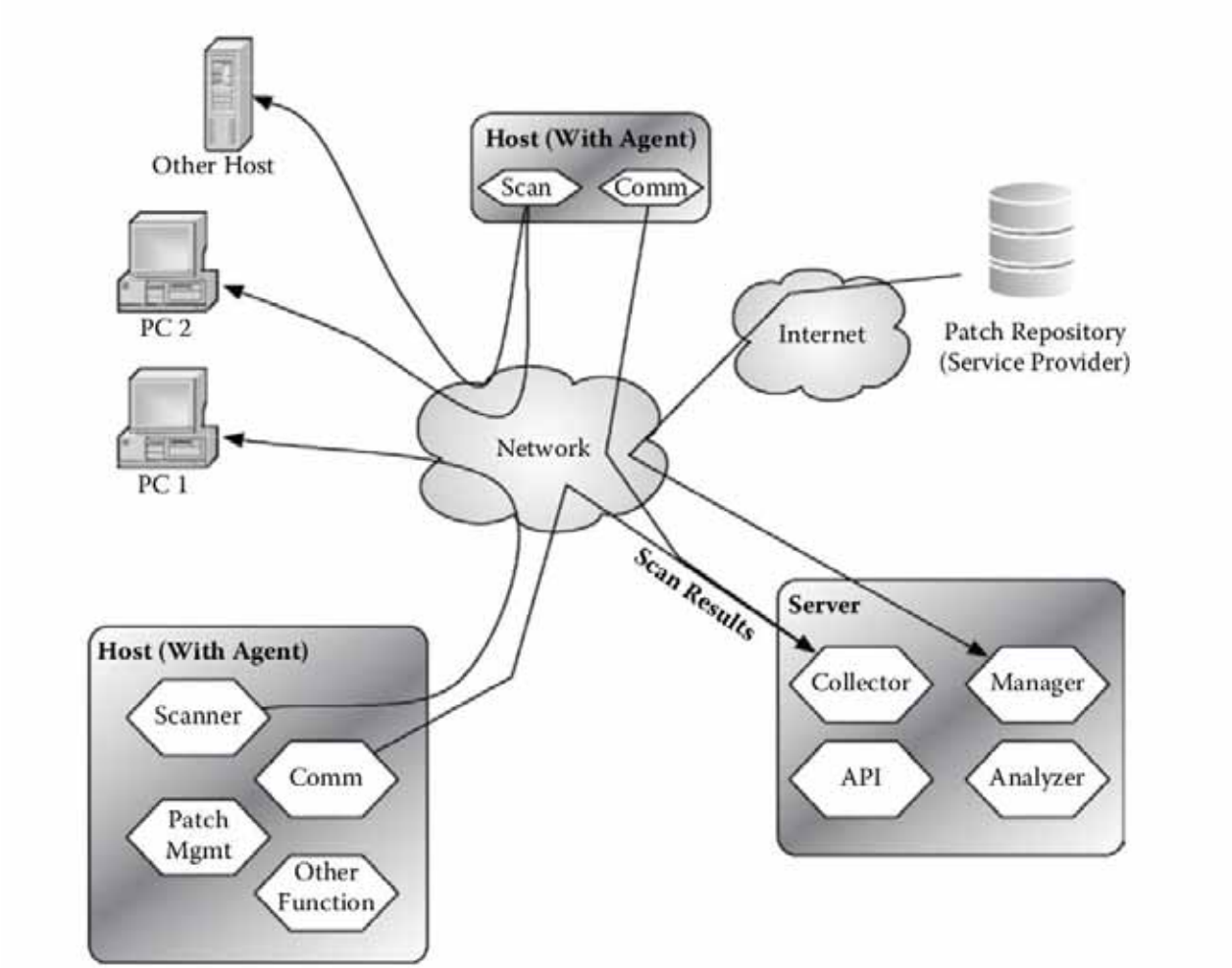
CIS: استاندارد configها

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CIS Center for Internet Security®

شناسایی و اسکن

- اسکن passive network
- اسکن active network
- استنتاجی
- مبتنی بر عامل کاربر


Other Host
Host (With Agent)
Scan
Comm
PC 2
PC 1
Network
Internet
Patch Repository
(Service Provider)
Scan Results
Server
Collector
Manager
API
Analyzer
Host (With Agent)
Scanner
Comm
Patch
Mgmt
Other
Function

چالش‌های تشخیص

تکنولوژی‌های مورد استفاده در ارزیابی آسیب‌پذیری

NVD

OVAL

SCAP

چالش‌های اولویت‌بندی

آیا معیار CVSS کافی است؟

نیازمند Asset Inventory

چالش‌های نهایی سازی ارزیابی

تنها وجود یک آسیب‌پذیری خطرآفرین است

ارزیابی نهایی با روشی به غیر از روش تشخیص

استفاده از ابزارها مانند NESSUS

چالش‌های کاهش

مدیریت وصله

مقاوم سازی)هاردنینگ(

معماری امن

مدیریت وصله