RCII

مرکز تحقیقات صنایع انفورماتیک

ارائه دهنده راهکارهای جامع
طراحی و امن سازی
زیرساخت های ارتباطی

www.rcii.ir

مرکز تحقیقات صنایع انفورماتیک

در راستای اهمیت ویژه پیاده سازی معماری امنیتی و امن سازی سرویس‌ها و زیرساختهای ارتباطی، لیست خدمات و سرویسهای زیر توسط مرکز تحقیقات صنایع انفورماتیک قابل ارائه می باشد. این مرکز دارای رتبه ۱ شورای عالی انفورماتیک و مجوز "آزمون و ارزیابی امنیتی – افتا" بوده و بیش از یک دهه در حوزه ارتقای امنیت سرویس ها و زیرساخت های ارتباطی کشور فعال می باشد.

رتبه ۱ شورای عالی انفورماتیک در حوزه های

- امنیت فضای تولید و تبادل اطلاعات
- خدمات فنی مهندسی و نظارت بر اجرای طرح های انفورماتیک، فناوری اطلاعات و ارتباطات
- آموزش و پژوهش

مجوز تست نفوذ از افتا

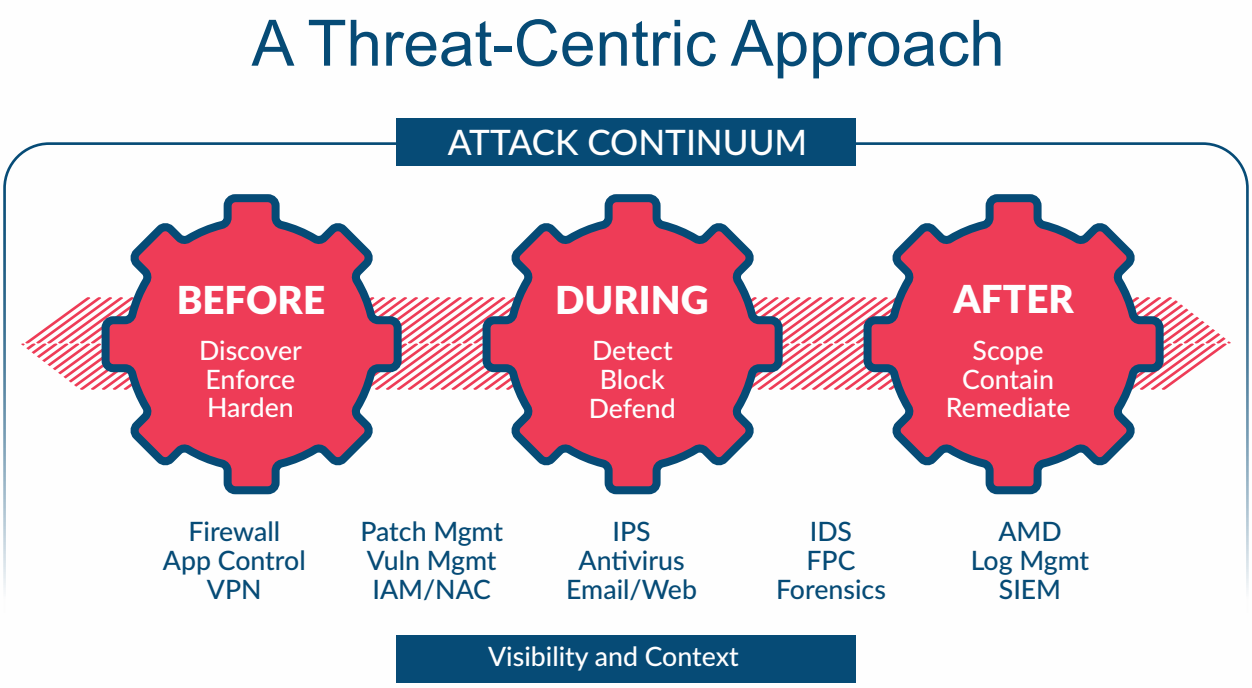
بزرگترین آزمایشگاه تخصصی ارزیابی امنیتی حوزه فناوری اطلاعات و ارتباطات تا EAL4

تنها آزمایشگاه امنیت دارنده گواهینامه ISO17025 در کشور

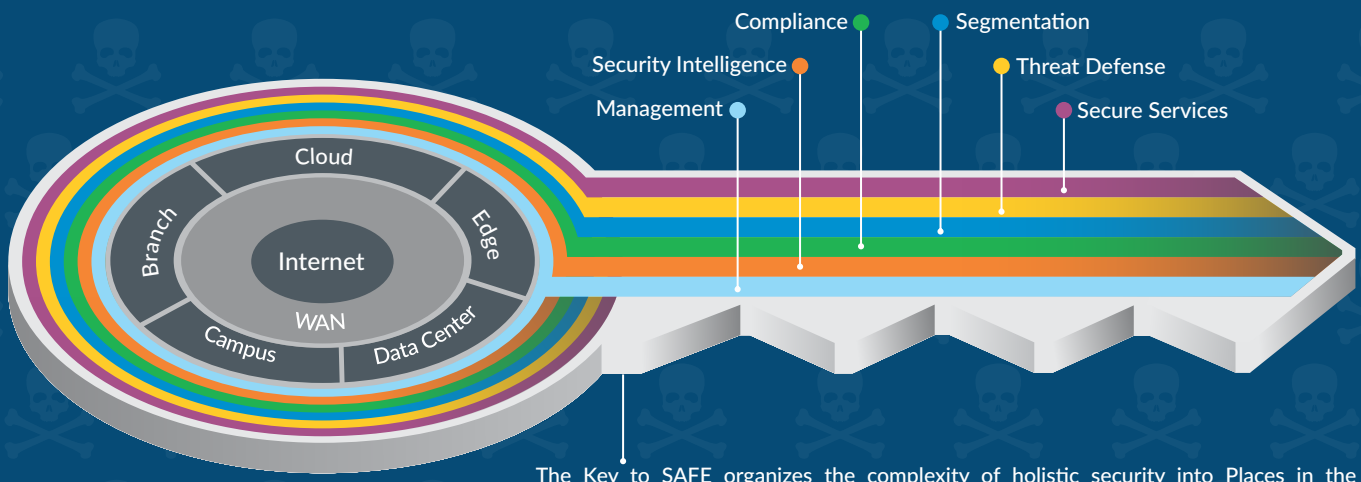
سرویس ها و خدمات مرکز تحقیقات صنایع انفورماتیک

طراحی و بهینه سازی ساختار و معماری امنیتی سرویس ها و زیرساخت های ارتباطی

نیازمندی های امنیتی بلاک های مختلف تشکیل دهنده زیرساخت ازجمله :
شبکه داخلی (Campus LAN)، شبکه گسترده ارتباطی (WAN)، مرکز داده (Datacenter) و لبه شبکه (Internet Edge) و سرویس های موجود در هر یک از این بخش ها، تشـــــکیل دهنده معماری کلان امن سازی خواهند بود. در این راستا معماری و چارچوب های امنیتی، منطبق با الگوهای امنیتی سایبری و استانداردهای طراحی ارایه شده توسط کمپانی های برتر و پیشـــــرو در صنعت امنیت، توسط این شرکت قابل ارائه به سازمان ها و نهادهای کوچک و بزرگ می باشد. برای تدوین معماری امنیتی سازمان خود، متخصصین ما با خدمات زیر در کنار شما هستند.



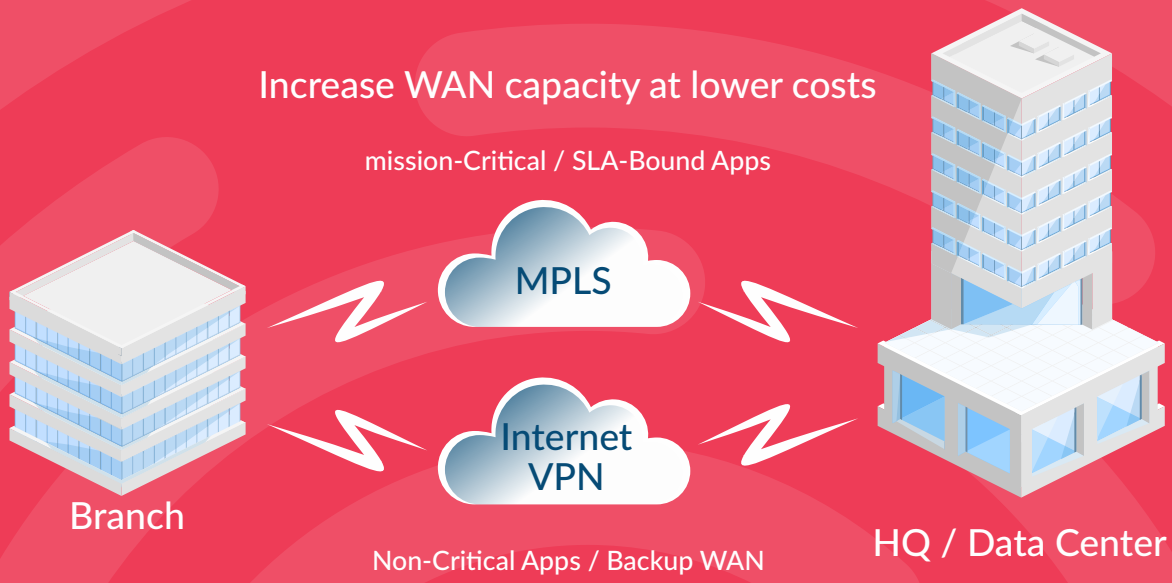
- ارائه راهکارهای جامع امنیت زیرساخت
- طراحی شبکه های گسترده کشوری (WAN) با رویکرد امنیتی و عملیاتی



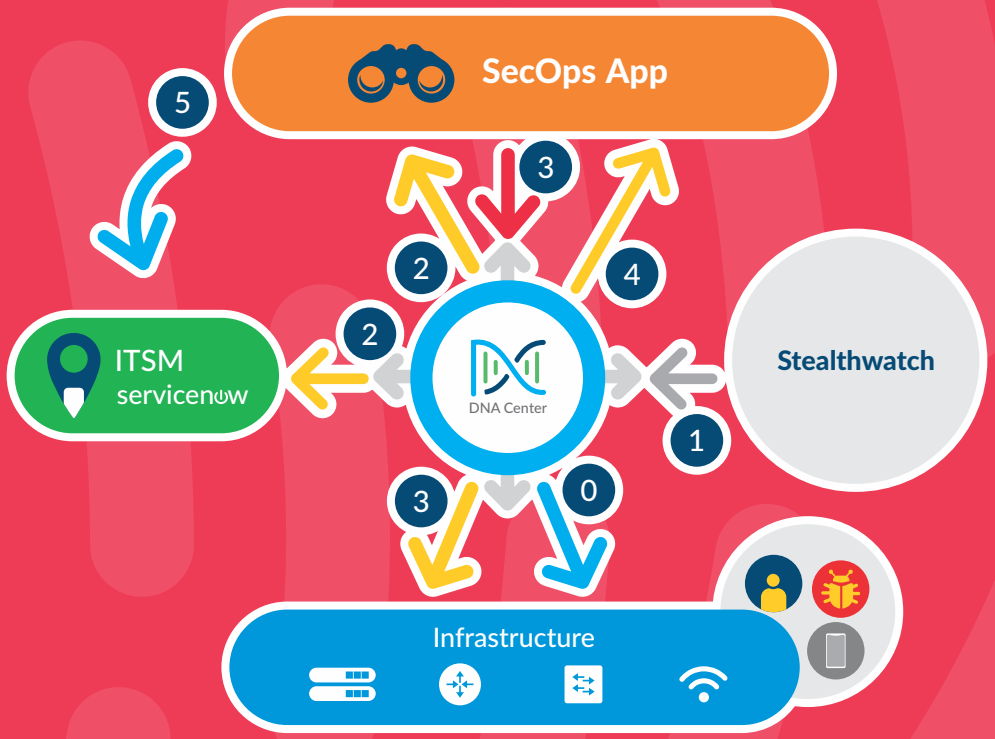
The Key to SAFE organizes the complexity of holistic security into Places in the Network (PINs) and Secure Domains. PINs are reference examples of locations found in networks, and Secure Domains are the taxonomic areas used to protect them

Rethink Your WAN

Increase WAN capacity at lower costs



- طراحی Internet Edge با رویکرد امنیتی و عملیاتی
- طراحی بلاک DMZ با رویکرد عملیاتی و امنیتی
- طراحی شبکه های Campus با رویکرد امنیتی و عملیاتی



0 DNA Center provisions ETA telemetry on network devices

1 Stealthwatch detects threats and alerts DNA Center

2 DNA Center Communicates Incident to ITSM and SecOps App

3 SecOps Sends Request to DNA Center to isolate threat

4 DNA Center confirms containment with SecOps App

5 Security Operations confirms containment to ITSM

Your branch is more critical than ever

- طراحی زیر ساخت ارتباطات مراکز داده نسل جدید
- اصلاح معماری نرم افزارها و برنامه های کاربردی
- طراحی برنامه های کاربردی (موبایل، تحت وب و کلاینت/سـرور) مطابق با استانداردهای امنیتی مطرح روز دنیا

80%

of employees now in the branch[1]

Branch

HQ / Data Center

77%

CIOs/IT leaders use cloud-based infrastructure[2]

5.3x

growth in business Internet video traffic from 2012 to 2017[3]

6x

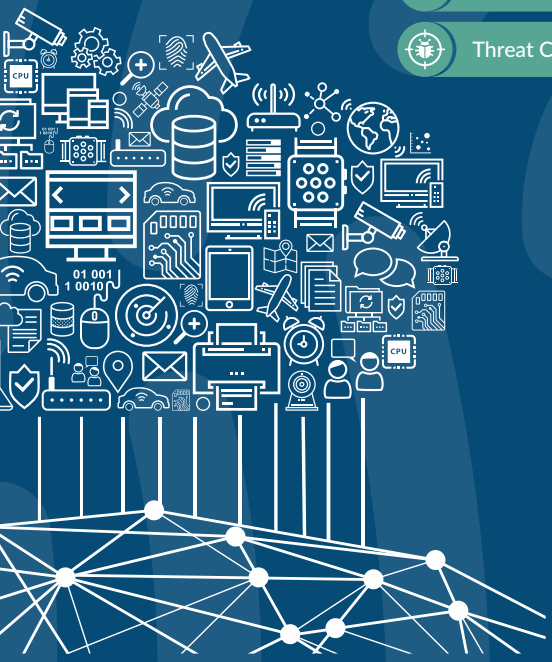
mobile traffic growth predicted by 2015[4]

ارائه راهکارهای احراز هویت و کنترل دسترسی کاربران و پیاده سازی مکانیزم های کنترلی هنگام اتصال به منابع حساس و حیاتی سازمان

آیا می دانید، مطابق با آمارها و گزارشات جهانی اعلام شده، درصد بالایی از تهدیدات و مخاطرات سازمان ها، کاربران داخلی پیمانکاران و کاربران مهمان هستند؟؟ ریسک امنیتی مرتبط با کاربران داخلی وابسته به عواملی همچون سطوح دسترسی بالا، عدم کنترل و مدیریت صحیح دسترسی ها و امکان دسترسی با سرعت های بالا به سرویس دهنده ها و مراکز داده می باشد.تکنولوژی که در صنعت فناوری اطلاعات برای مرتفع کردن این چالش عرضه شده است **Network Admission Control (NAC)** می باشد. برای پیاده سازی این مکانیزم و مرتفع کردن مخاطرات کاربران داخلی، می توانید به ما و راه کارهای ما اطمینان کنید. برخی از خدمات قابل ارائه در این زمینه در ادامه قابل مشاهده می باشد.

- احراز هویت کاربران شبکه داخلی قبل از اتصال به شبکه
- تعیین سطوح دسترسی به منابع اشتراکی شبکه در نزدیکترین نقطه به مبدا ترافیک
- بررسی وضعیت امنیتی سیستم های کاربران (به عنوان مثال می توان ابتدا از به روز بودن نسخه آنتی ویروس روی سیستم اطمینان حاصل کرد سپس مجوز دسترسی به منابع شبکه اعطا شود.)
- ارائه دهنده سرویس **Radius** و **Tacacs+** در قالب یک سرویس
- امکان برقراری یکپارچگی با سیستم های تشخیص نفوذ

Device admin	support device administration using the TACACS+security protocol to control and audit the configuration of network devices.
Asset Visibility	can reach deep into the network to deliver superior visibility into who and what is accessing resources.
Guest Access	fully customizable branded mobile and desktop guest portals , whit dynamic visual workflows to easily manage quest user experience.
Access Control	consistent access control in to wired , wireless and vpn networks. 802 . 1XMAC, web authentication and easy connect for admission control.
BYOD Access	simplifies BYOD management whit built-in CA and 3rd party MDM integration for on boarding and self-service of personal mobile devices.
Segmentation	topology independent software-defined segmentation policy to contain network threats by using Cisco TrustSec technology
Threat Control	context sharing with partner eco-system to improve their overall efficacy and accelerate time to containment of network threats.



- قرنطینه کردن سیستم های مشکوک به آلودگی ها و بدافزارها
- شناسایی و تشخیص هویت کلیه کاربران و سیستم های کاری متصل به شبکه

- شناسایی و تشخیص هویت دستگاه های IoT
- تعیین سطوح دسترسی دستگاه های IoT منطبق با هویت و پروفایل رفتاری آن ها
- قابلیت یکپارچگی با ساختار Software Defined Network (SDN)
- گزارشگیری از فعالیت کاربران در شبکه و بسیاری قابلیت ارزشمند دیگر

ارائه راهکارهای مقابله با حملات نفوذی و پیکربندی سیستم های تشخیص نفوذ نسل جدید

در معماری های امنیتی انتخاب تکنولوژی های تشـــــــخیص نفوذ یکی از ارکان پیاده سازی موارد امنیتی می باشد. حملات سایبری دارای ابعاد و ویژگی های متفاوتی هستند حملات نفوذی و دسترسی های غیر مجاز از رایج ترین حملاتی هستند که علیه سرویس دهنده های حیاتی اجرا می شود از اینرو برای انتخاب صحیح سیستم تشخیص نفوذ پارامترهای مشخصی باید در نظر گرفته شود. مطابق با استانداردهای جهان و سهم بازار، یکی از قدرتمند ترین و موثرترین راهکارهای موجود، تکنولوژی NGIPS می باشد. این مجموعه می تواند به شما در انتخاب راهکار موثر و کارآمد، بهینه سازی و پیاده سازی راهکار خدمات فنی و مهندسی ارائه نماید.

perimeter or outer layer defense

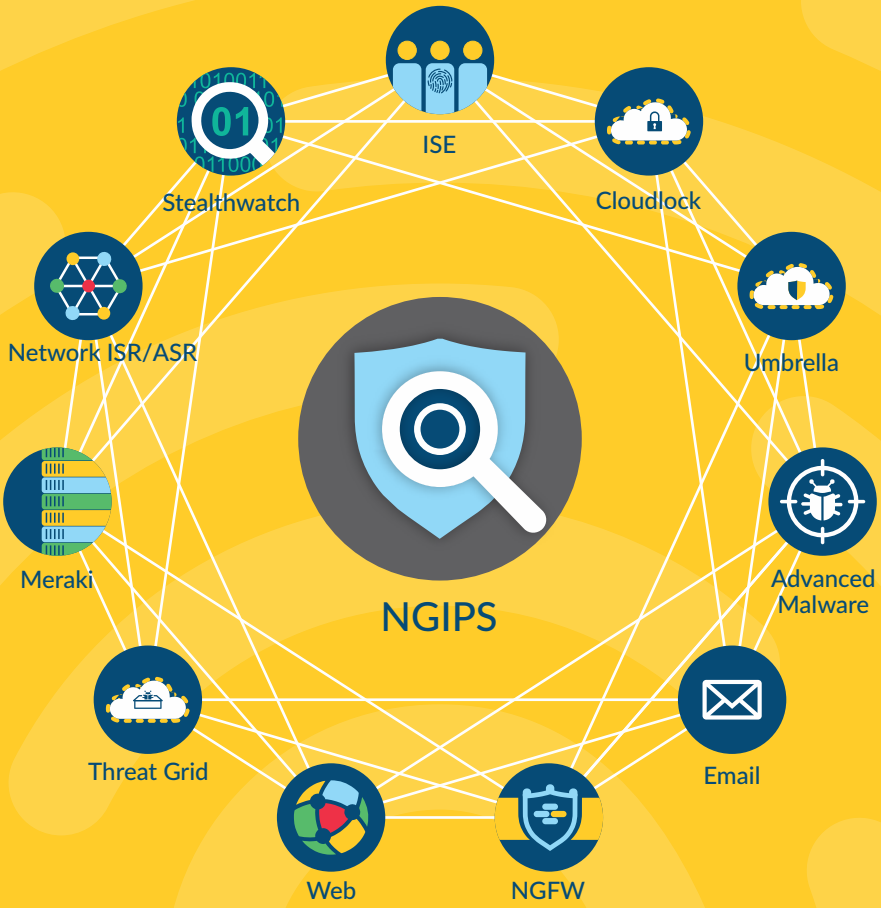
ATP(advance threat protection)
Email and web security
IPS/IDS(INTRUSION PREvention system/intrusion Detection system)

Mid layer defense

NGFW(nextgen firewall) or UTM(unified threat management)
Data forensic
Security event monitoring(SIEM)

Internal Defense

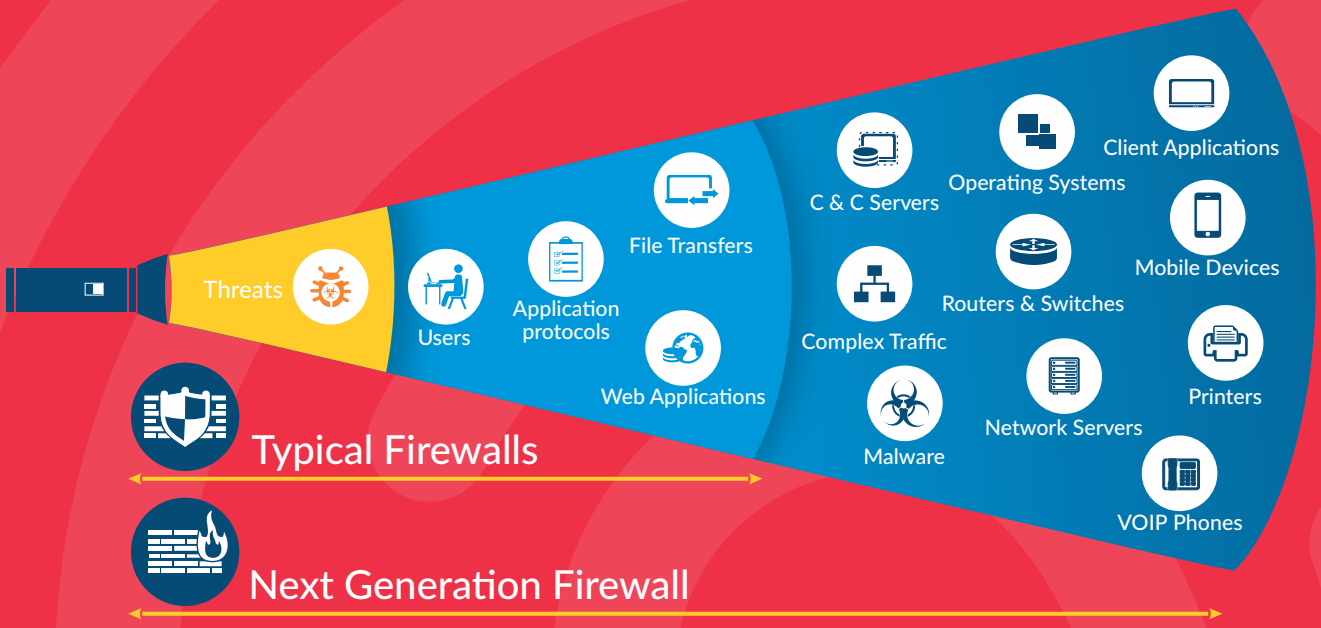
Host security
Data at rest and data in motion , DLP(Data leakage prevention)



ارائه راهکارهای طراحی و پیاده سازی فایروال های نسل جدید

پرکاربردترین اجزای سیستم های امنیتی فایروال ها می باشند. الگوریتم های مختلفی اساس عملکرد فایروال ها را تشکیل می دهند. مطابق با استانداردهای جهان و سهم بازار، یکی از قدرتمند ترین و موثرترین راهکارها، تکنولوژی NGFW می باشد. از اینرو بنا به نیازمندی های سازمان و الزامات امنیتی بخش ها و سرویس های مختلف در زیر ساخت می توان فایروال های متفاوتی را استفاده کرد. راهکار پیشنهادی مرکز در زمینه فایروال های نسل جدید در بر گیرنده قابلیت های امنیتی زیر می باشد:

- ارائه قابلیت برترین سیستم تشخیص نفوذ کارآمد و موثر
- ارائه قابلیت سیستم ضد بدافزار با رویکرد متد Retrospective
- ارائه قابلیت شناسایی و شناخت برنامه های کاربردی و Application های جاری در شبکه (Application Visibility And Control)

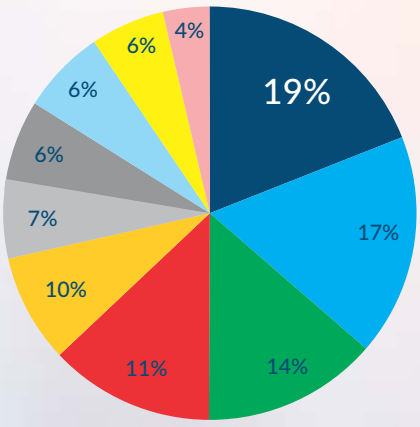


- ارائه قابلیت کنترل و محدود کردن فعالیت گروه های مختلف URL
- ارائه سرویس Threat Intelligence از منابع معتبر جهانی

این مرکز با اســـــتناد به الگوها و اســـــتانداردهای طراحی، آماده ارائه خدمات طراحی در زمینه انتخاب فایروال های مناســـب و نحوه جایگیری آن ها در زیرســـاخت های ارتباطی می باشـــد.

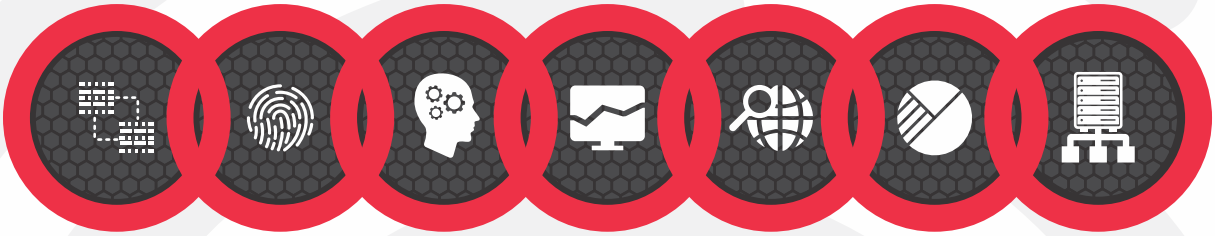
ارائه راهکارهای مقابله با بدافزارها و پیاده سازی سیستم های تشخیص بدافزار

Top 10 Malware - Breakdown



روزانه شاهد اخبار مرتبط با نفوذ بدافزارها و پیامدهای ناشی از این چالش امنیتی می باشیم.
در این راستا سازمان ها نیازمند راهکاری تازه نفس و همه جانبه برای مقابله با این چالش جدی و بزرگ امنیتی می باشند.
چالش امنیتی خانواده Ransomwareها را هیچ یک از کارشناسان امنیتی فراموش نکرده و نخواهند کرد. مرکز تحقیقات صنایع انفورماتیک با تجربه بی نظیر در راستای تحلیل و رفتارشناسی بدافزارها، در مقابله با این تهدیدات در کنار شما خواهد بود.

مخاطرات و گزارش های امنیتی منتشـــــر شده در رابطه با توسعه و گســـــترش بدافزارها، این حوزه را به پرخطرترین حوزه تبدیل کرده است. کلیه صنایع و حوزه های بانکداری و خدماتی با بدافزارها درگیر هســـــــتند. برای محافظت از دارایی های ســـــرویس های ارتباطی در برابر Malware ها باید راهکاری جامع و چند لایه تدوین و پیکربندی گردد. راهکارهای ترکیبی می توانند در این راســـتا موثر عمل نمایند که هم در ســـطح کاربران نهایی و هم در ســـطح زیرســـاخت قابل پیکربندی و یکپارچه سازی باشند. مرکز تحقیقات ارائه دهنده راهکارهای نوین مقابله با بدافزارها با رویکرد بازگشـــــــــــت به عقب "Retrospective" و نه "Single Point" می باشد.

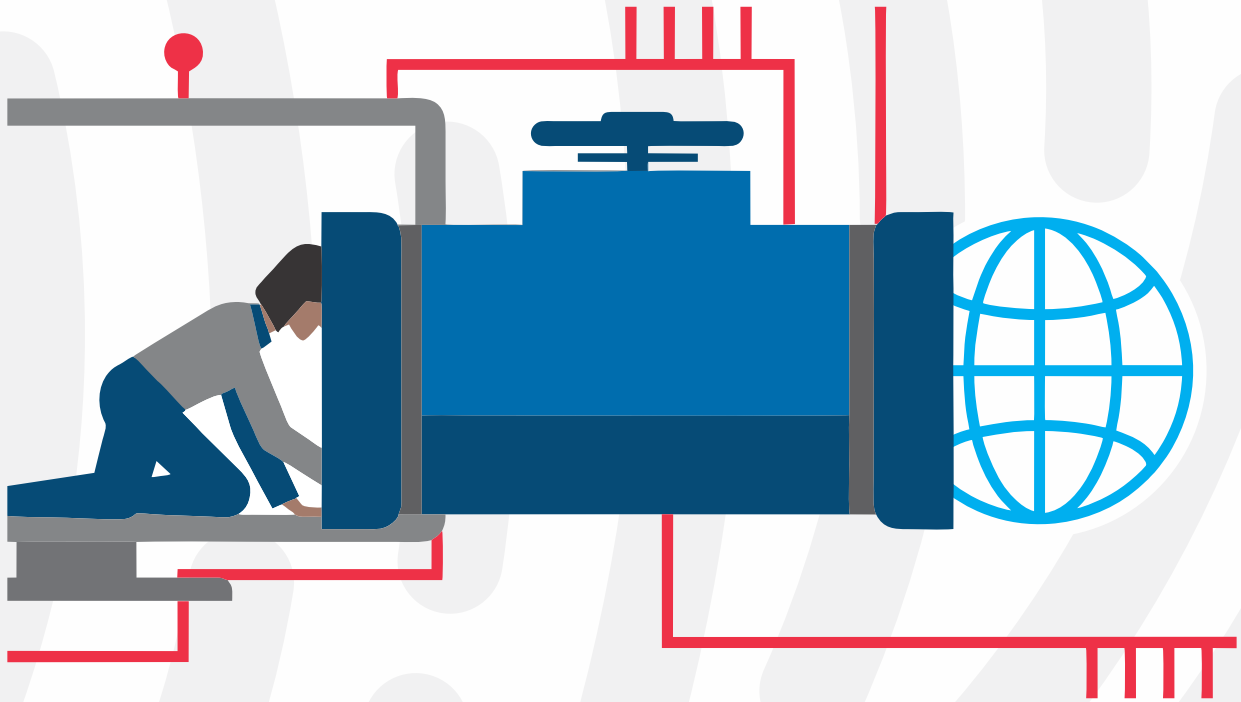


One-to-One Signature | Fuzzy Finger-Printing | Machine Learning | Indications of Compromise | Dynamic Analysis | Advanced Analytics | Device Flow Correlation

Reputation Filtering | File Sandboxing

ارائه راهکارهای دسترسی های از راه دور

از هر مکانی با هر وسیله ای به منابع اشتراکی سازمان خود به صورت امن دسترسی داشته باشید.



امن سازی سرویس های و زیرساخت های ارتباطی شبکه

با کمترین هزینه و بدون نیاز به خرید تکنولوژی، اولین قدم امن ســـــازی را بردارید. مطابق با معماری Defense In Depth (DID)اولین لایه ســاختارهای امنیتی هاردنینگ و رعایت اصــول پایه ای امنیتی در ســـرویس ها می باشـــد. از اینرو مرکز تحقیقات صنایع انفورماتیک راهکارهایی را به منظور امن سازی اولین لایه محافظتی تدوین کرده است. راهکارها در برگیرنده حوزه های زیر می باشد.

Security Hardening

Patch Known Vulnerabilities	Closed Unused Network Ports	Enforce Password Complexity	Manage user Privileges	Remove unneeded Services	Remote Default Accounts

- ارائه الزامات و دستورالعمل های امن سازی سیستم عامل ها
- ارائه الزامات و دستورالعمل های امن سازی سرویس دهندهگان وب
- ارائه الزامات و دستورالعمل های امن سازی پایگاه های داده
- ارائه الزامات و دستورالعمل های امن سازی سیستم عامل های موبایل
- ارائه الزامات و دستورالعمل های امن سازی پلتفرم های تشکیل دهنده زیرساخت های ارتباطی
- ارائه الزامات و دستورالعمل های امن سازی سرویس های مجازی سازی
- ارائه الزامات و دستورالعمل های امن سازی برنامه های کاربردی سمت کاربر

بررسی و ارزیابی آسیب پذیری ها

سند معماری کلان امنیتی خود را بسازید.
نقطه شـروع چرخه امن سـازی، ارزیابی و شـناخت وضـعیت فعلی و آنالیز میزان فاصـله با اسـتانداردهای مدون می باشـد. خروجی ها و نتایج این ارزیابی می تواند تعیین کننده بدنه و اسلوب اصلی معماری امنیتی سازمان باشد. در این راستا مرکز تحقیقات صنایع انفورماتیک با بیش از ده سال سابقه در زمینه ارزیابی امنیتی کلیه محصـــــولات و سرویس های حوزه IT او OTمی تواند مطابق با قالب ها و اسـتانداردهای جهانی، سـامانه های و زیرسـاخت های ارتباطی سـازمان و مجموعه شـما را بررسی و تحلیل نموده و نقاط آسیب پذیر و درجه حســـاسیت و پتانســـیل تخریب پذیری را در هر یک از آنها تعیین نماید. ارزیابی دقیق آسیب پذیری ها می تواند راهکارهای امن سازی را بسـیار موثرتر و کارآمدتر نماید. به لیسـت خدمات در ادامه اشاره شده است.

ارزیابی آسیب پذیری زیرساخت های ارتباطی

- ارزیابی و بررســـی معماری امنیتی موجود در زیرســـاخت اینترانت (WAN)، اینترنت (Internet Edge) مراکز داده (Data Center) و شبکه های محلی
- ارزیابی و بررسی آسیب‌پذیری‌های تجهیزات سوئیچینگ/ مسیریابی و ارتباطات لایه دو/ سه
- ارزیابی و بررسی آسیب‌پذیری‌های تجهیزات امنیت شبکه مانند فایروال، UTM، WAF، IDS/IPS، VPN
- ارزیابی و بررسی آسیب‌پذیری‌های سیستم عامل‌های تجهیزات شبکه

ارزیابی آسیب پذیری برنامه های کاربردی تحت وب

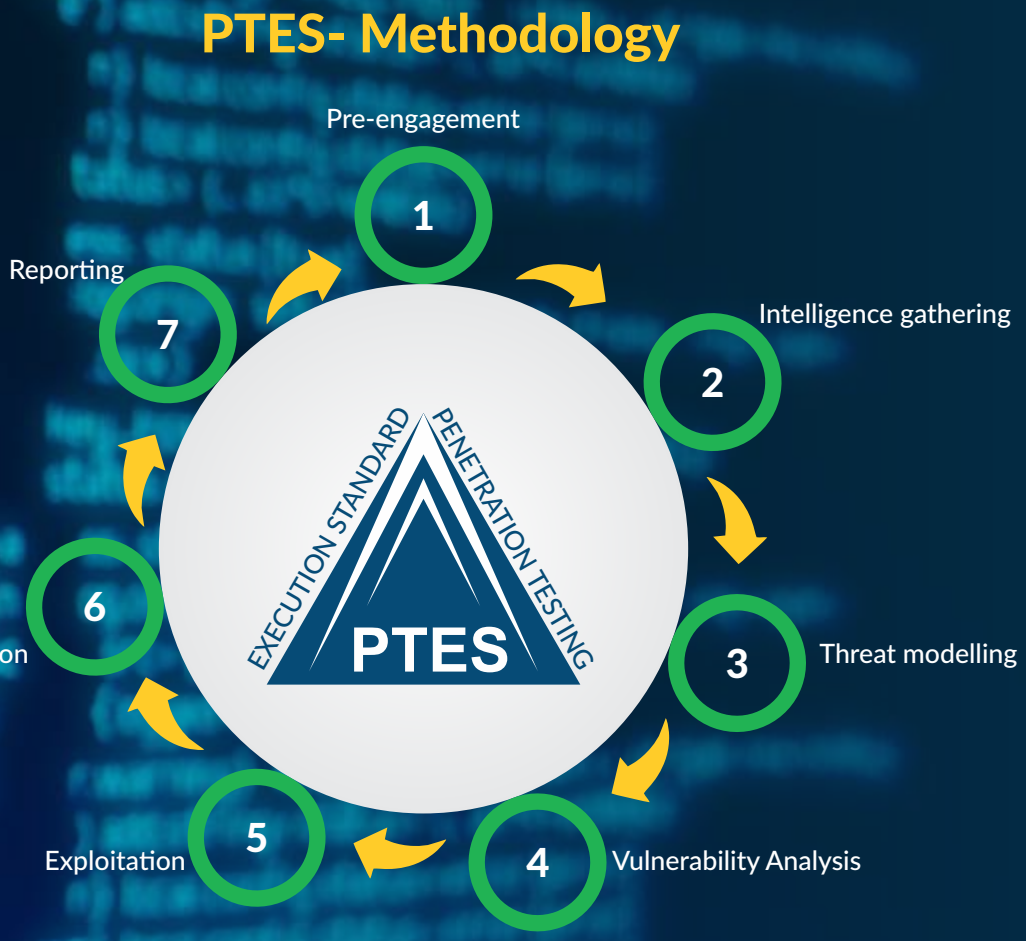
- شناسایی و تحلیل آسیب پذیری مکانیزم احرازهویت
- شناسایی و تحلیل آسیب پذیری مکانیزم مدیریت نشست
- شناسایی و تحلیل آسیب پذیری مکانیزم کنترل دسترسی
- شناسایی و تحلیل آسیب پذیری مکانیزم اعتبارسنجی داده های ورودی
- شناسایی و تحلیل آسیب پذیری مکانیزم مدیریت خطاها
- شناسایی و تحلیل آسیب پذیری مکانیزم محافظت از داده‌ها
- شناسایی و تحلیل آسیب پذیری مکانیزم مدیریت فایل ها و منابع
- شناسایی و تحلیل آسیب پذیری های ناشی از پیکربندی ناامن
- شناسایی و آسیب پذیری وب سرویس ها
- شناسایی و تحلیل الگوریتم های رمزنگاری و پروتکل های ارتباطی ضعیف

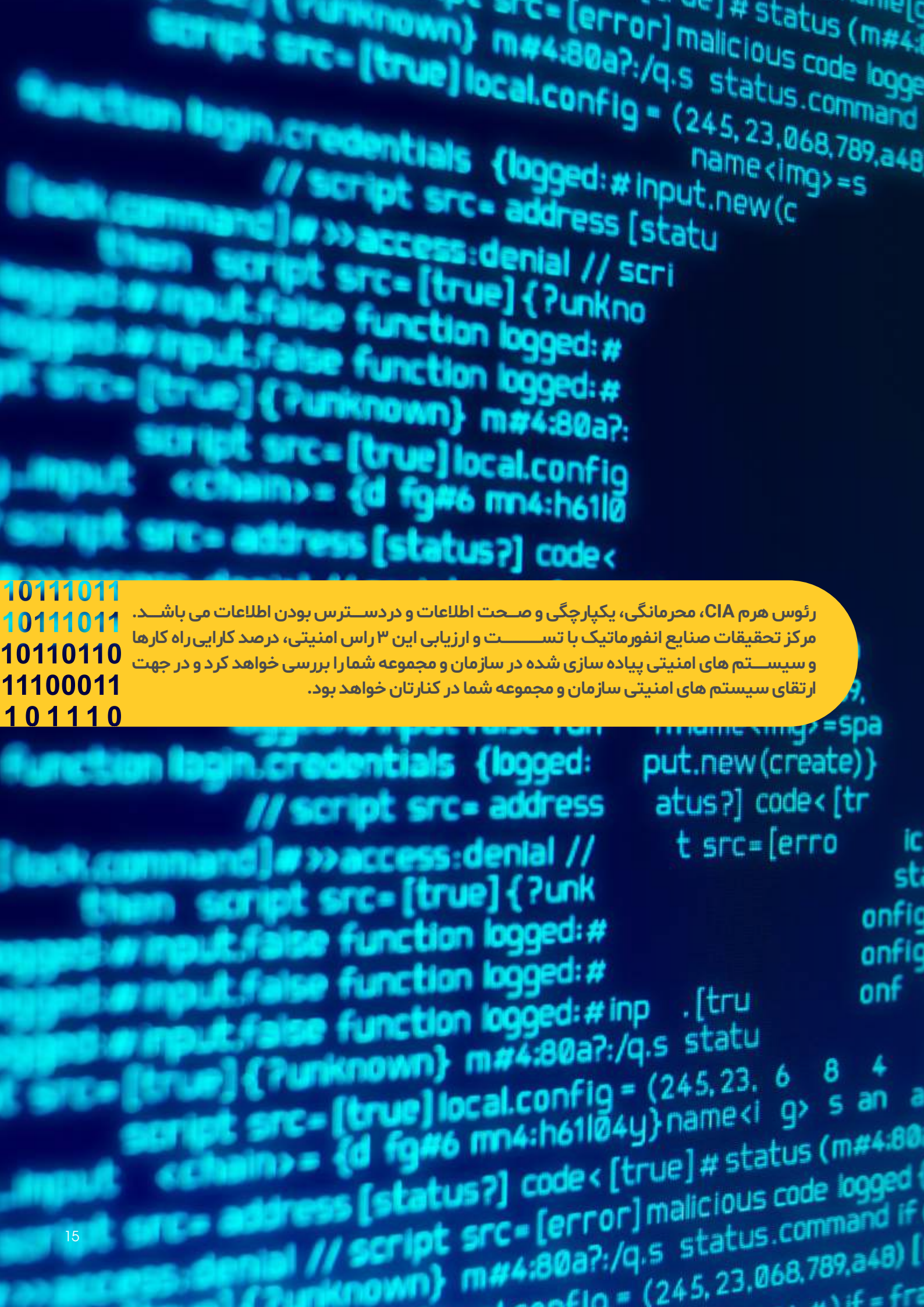
ارزیابی آسیب پذیری برنامه های کاربردی موبایل

- شناسایی و تحلیل آسیب‌پذیری ذخیره‌سازی داده و حریم خصوصی
- شناسایی و تحلیل آسیب‌پذیری مکانیزم احرازهویت و مدیریت نشست
- شناسایی و تحلیل آسیب‌پذیری ارتباطات شبکه‌ای
- شناسایی و تحلیل آسیب‌پذیری تعاملات با پلتفرم
- شناسایی و تحلیل پیکربندی ناامن هنگام build برنامه‌ی کاربردی
- بررسی میزان مقاومت برنامه کاربردی در برابر تکنیک‌های مهندسی معکوس

تست نفوذ

با ما معماری امنیتی خودرا محک بزنید.
درک بهتر و عمیقتر ریســـــــــک ها و مخاطرات امنیتی موجود در سرویس دهنده ها و زیرساخت های ارتباطی کســب و کارها و برنامه ریزی راهکارها و استراتژی های مرتفع کردن تهدیدات، هدف سطح بالا و اصلی فرآیند تســت نفوذ می باشد. در جریان تســت نفوذ هرم امنیتی CIA کســب و کار شما بررسی و تحلیل خواهد شد.

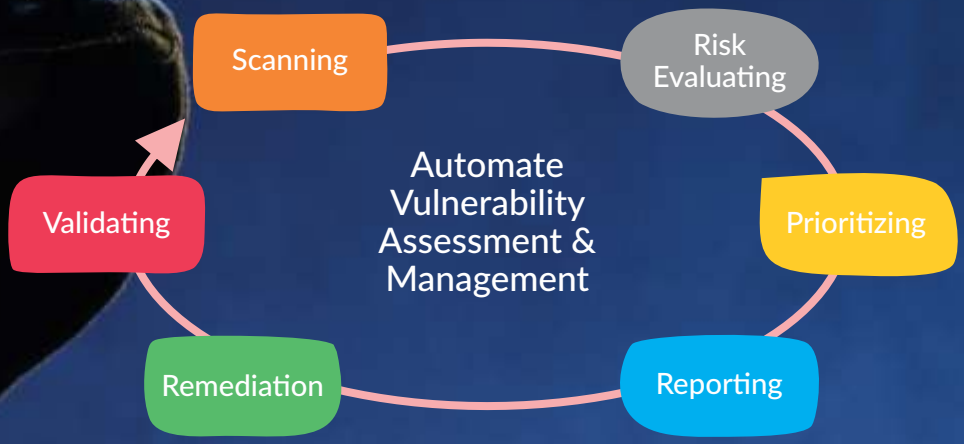




10111011
10111011
10110110
11100011
101110

رئوس هرم CIA، محرمانگی، یکپارچگی و صحت اطلاعات و دردسترس بودن اطلاعات می باشد.
مرکز تحقیقات صنایع انفورماتیک با تست و ارزیابی این ۳ راس امنیتی، درصد کارایی راه کارها
و سیستم های امنیتی پیاده سازی شده در سازمان و مجموعه شما را بررسی خواهد کرد و در جهت
ارتقای سیستم های امنیتی سازمان و مجموعه شما در کنارتان خواهد بود.

یکی از سرویس های که به صورت یکپارچه در معماری امن سازی و یا به صورت مجزا توسط مرکز تحقیقات صنایع انفورماتیک قابل ارائه می باشد، تســـــت نفوذ است. این مرکز در فرایند تســـــت نفوذ علاوه بر ابزار خودکار از روش های غیر خودکار manual نیز استفاده می کند. تجربه ارزیابی امنیتی محصــولات و سرویس های مختلف، تجربه بســیار ارزشمند و گســترده ای را در زمینه تســت نفوذ برای این مرکز به ارمغان آورده است. متدولوژی ها و استانداردهای OWASP،PTES و OSSTMM در این راستا به عنوان مرجع مورد استفاده می باشند.



نظارت بر اجرای طرح های امنیتی زیرساخت های ارتباطی

پیاده سازی صحیح و مطابق با استاندارد و بهره برداری حداکثری از تکنولوژی های امنیت شبکه، نیازمند تجربه و تخصـــــــص می باشد. مرکز تحقیقات صنایع انفورماتیک با تکیه بر بیش از یک دهه سابقه در زمینه طراحی سرویس های امنیت شبکه و امن سازی سرویس دهنده ها، در اجرای پروژه های زیرساخت های ارتباطی و پروژه های امنیت زیرساخت و سرویس دهنده ها در کنار شما خواهد بود.

لیست سرویس های ارائه شده، در حوزه های زیرساخت، سرویس دهندگان داخلی/خارجی سرویس گیرندگان یا کاربران داخلی و برنامه های کاربردی موبایل معتبر می باشد.

با ما میزان اثربخشی و کارایی سیستم های امنیت شبکه خود را بررسی و آنالیز نمایید

در صورت نیاز به کسب اطلاعات بیشتر با کارشناسان ما تماس حاصل نمایید

کریمخان زند، خیابان شهید عضدی
(آبان جنوبی) نبش رودسر، پلاک ۳
+۹۸ ۲۱ ۸۸۹۲۵۹۴۳-۵۰
+۹۸ ۲۱ ۸۸۹۳۷۶۵۸
www.rcii.ir

مرکز تحقیقات صنایع انفورماتیک

ارائه دهنده راهکارهای جامع طراحی و امن سازی زیرساخت های ارتباطی

کریمخان زند، خیابان شهید عضدی
(آبان جنوبی) نبش رودسر، پلاک ۳
+۹۸ ۲۱ ۸۸۹۲۵۹۴۳-۵۰
+۹۸ ۲۱ ۸۸۹۳۷۶۵۸
www.rcii.ir