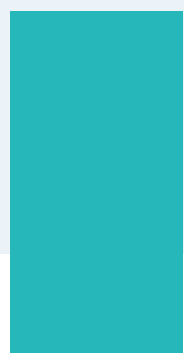
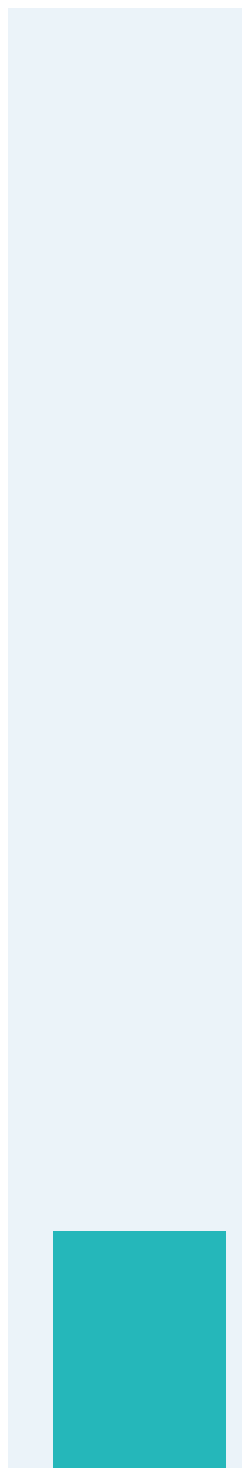




CYBERSECURITY SERVICES





راهکارهای جامع امنیت سایبری

شرکت مهندسی هیرساویژن با تکیه بر تجربه و تخصص خود در حوزه امنیت سایبری، به منظور ارتقای سطح خدمات به مشتریان، اقدام به بازنگری در نحوه ارائه خدمات امنیتی کرده است. این بازنگری شامل معرفی دو بسته مجزا از خدمات است که هر یک شامل ترکیبی از چند خدمت امنیتی است و در اختیار مشتریان قرار می‌گیرد.

هدف از این تغییر، تسهیل انتخاب و استفاده از خدمات امنیتی برای مشتریان است. هر یک از این خدمات ممکن است به تنهایی نتوانند تمام نیازهای امنیتی یک سازمان را به طور کامل پوشش دهند و به عنوان یک راهکار جامع عمل کنند. اما هنگامی که این خدمات به صورت ترکیبی و در قالب بسته‌های پیشنهادی ارائه شوند، کارایی و اثربخشی آنها به طور قابل توجهی افزایش می‌یابد. هر خدمت در جایگاه مناسب خود اجرا می‌شود و نقش حیاتی خود را در تأمین امنیت کلی سیستم ایفا می‌کند.

این هم‌افزایی میان خدمات، منجر به ایجاد راهکاری جامع و کارآمدتر می‌شود که تمامی جنبه‌های امنیت سایبری را پوشش می‌دهد. به عبارتی، هر بسته به گونه‌ای طراحی شده که بتواند طیف وسیعی از نیازهای امنیتی را پوشش داده و در کنار یکدیگر، سیستمی جامع و یکپارچه برای تضمین امنیت سایبری ارائه کنند.

مزایای این تغییر

- ✓ سفارشی‌سازی خدمات بر اساس نیاز مشتریان
- ✓ پاسخگویی به نیازهای امنیتی در حال تغییر
- ✓ افزایش کارآمدی و هم‌افزایی بین خدمات
- ✓ همکاری با کارشناسان امنیتی متخصص
- ✓ ارتقای بلوغ امنیتی و کاهش مخاطرات
- ✓ ارائه پاسخ جامع به نیازهای امنیتی
- ✓ بهینه‌سازی هزینه‌ها



ارائه خدمات امنیتی در قالب بسته‌های یکپارچه، مزایای بسیاری را برای سازمان‌ها به همراه دارد. این رویکرد با ایجاد هم‌افزایی بین خدمات مختلف، موجب بهبود امنیت کلی شده و بهره‌وری را افزایش می‌دهد. علاوه بر این، خرید این بسته‌ها نسبت به تهیه جداگانه هر خدمت، مقرون‌به‌صرفه‌تر است و در عین حال تمام مزایای لازم را برای امنیت فراهم می‌کند.

بسته‌های امنیتی، انعطاف‌پذیری بالایی دارند و می‌توانند با نیازهای خاص هر سازمان هماهنگ شوند. همچنین، ارتقای بلوغ امنیتی و کاهش ریسک‌ها از دیگر مزایای این بسته‌هاست. همکاری با یک شرکت امنیتی معتبر و با تجربه، فرصت دریافت مشاوره و پشتیبانی مداوم را فراهم می‌کند و به بهبود مستمر امنیت اطلاعات کمک می‌نماید.

به‌روزرسانی‌های منظم و انعطاف‌پذیری این بسته‌ها، تضمین می‌کند که سازمان‌ها همواره از جدیدترین تکنولوژی‌ها و راهکارهای امنیتی بهره‌مند می‌شوند.



خدمات

01 RED TEAM

03 HARDENING

05 PHISHING CAMPAIGN

07 VULNERABILITY ASSESSMENT

02 INCIDENT RESPONSE

04 FORENSIC

06 SECURITY AWARENESS TRAINING

08 PENETRATION TEST

09 COMPLIANCE CHECK

تیم قرمز (RED TEAM)

خدمات Red Team یک ارزیابی پیشرفته و جامع از امنیت سازمان است که توسط گروهی از متخصصان با تجربه انجام می‌شود. این تیم با شبیه‌سازی حملات پیچیده و واقعی، همانند یک مهاجم واقعی عمل کرده و زیرساخت‌ها، سیستم‌ها و فرایندهای امنیتی سازمان را از زوایای مختلف مورد بررسی قرار می‌دهد. هدف اصلی Red Team شناسایی نقاط ضعف پنهان و بهره‌برداری آن‌ها در امنیت سازمان است. این فرایند با استفاده از تکنیک‌های پیشرفته و جدید حملات سایبری، به سازمان کمک می‌کند تا پیش از وقوع حوادث امنیتی، آسیب‌پذیری‌های خود را برطرف کرده و سطح آمادگی در برابر تهدیدات را به‌طور چشمگیری افزایش دهد. همچنین، گزارش‌های دقیق و توصیه‌های کاربردی Red Team می‌تواند نقشه‌راهی برای بهبود مستمر امنیت در تمامی بخش‌های سازمان ارائه دهد.



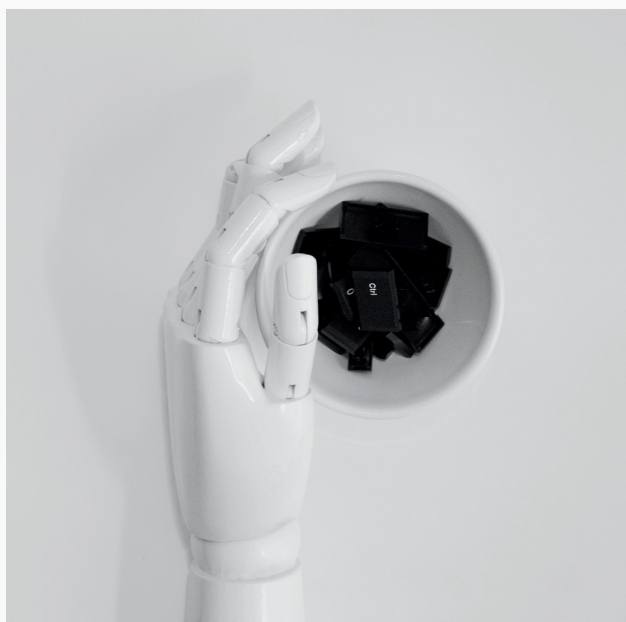
INCIDENT RESPONSE

خدمات Incident Response به سازمان‌ها کمک می‌کند تا در مواجهه با حوادث امنیتی، به سرعت و با دقت عمل کنند. تیم متخصص ما با استفاده از روش‌های پیشرفته شناسایی، تحلیل و مقابله با تهدیدات، فرایندهای کارآمدی برای مدیریت حوادث امنیتی ارائه می‌دهد.

این خدمات شامل شناسایی حملات، مهار تهدیدات، بازیابی اطلاعات و تحلیل ریشه‌ای حادثه است تا سازمان‌ها بتوانند از تکرار مجدد حملات جلوگیری کرده و سیستم‌های خود را به حالت پایدار برگردانند. با استفاده از این خدمات، سازمان‌ها نه تنها توانایی واکنش سریع به حوادث را افزایش می‌دهند، بلکه آمادگی بیشتری برای پیشگیری از تهدیدات آینده نیز به دست می‌آورند.

جرمیابی سایبری (FORENSIC)

جرمیابی سایبری پس از رخ دادن یک رویداد سایبری در سازمان اجرا می‌شود. این فرایند به منظور بازیابی اطلاعات و دستیابی به مدارک قابل ارائه در دادگاه انجام می‌شود. تکنیک‌ها و ابزارهای جرمیابی سایبری برای گردآوری و نگهداری مدارک جرائم سایبری استفاده می‌شوند. هدف اصلی این فرایند بررسی ساختار و جزئیات یک جرم سایبری و کشف زنجیره‌ای از مدارک برای پیدا کردن منشاء و چگونگی حملات است.



در جرمیابی سایبری، ابتدا یک متخصص جرمیابی سایبری اطلاعات را با حفظ یکپارچگی ساختار آن‌ها گردآوری می‌کند. سپس این اطلاعات توسط متخصصان تحلیل می‌شوند. جرمیابی سایبری تنها به کشف نحوه وقوع یک جرم سایبری محدود نیست؛ بلکه می‌تواند به منظور پیدا کردن شیوه و منشاء حملات سایبری و ساز و کار بدافزارها برای پیشگیری از حوادث سایبری در آینده یا حتی بازیابی داده‌های از دست رفته در یک سیستم عامل معیوب نیز به کار رود.

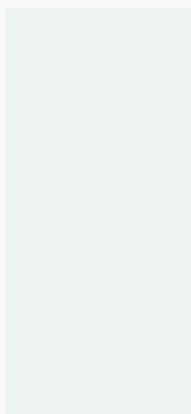
علاوه بر این، جرمیابی سایبری یکی از مؤلفه‌های مهم پاسخ به تهدیدات (Incident Response) در امنیت سایبری به شمار می‌آید. این فرایند می‌تواند با شناسایی روش‌ها و ابزارهای مورد استفاده هکرها به پیشگیری از حوادث سایبری کمک کرده و با بازیابی داده‌ها، خسارات چنین حوادثی را برای سازمان‌ها به حداقل برساند.

امن سازی (HARDENING)

امن سازی به مجموعه ای از تدابیر و اقدامات امنیتی گفته می شود که در نرم افزارها، سیستم عامل ها، و تجهیزات شبکه برای تقویت امنیت و محافظت در برابر حملات احتمالی به کار گرفته می شود. هدف اصلی این فرایند، کاهش نقاط ضعف امنیتی سیستم های کسب و کار است. متخصصان امنیت با استفاده از استانداردهای بین المللی مانند NIST، CIS، و STIG، اقدامات و روش هایی را در سیستم عامل ها و تجهیزات سازمانی (مانند Windows OS، Linux OS، و تجهیزات شبکه) اجرا می کنند تا آسیب پذیری سازمان در برابر رویدادهای امنیتی کاهش یابد.



هدف اصلی امن سازی، کاهش آسیب پذیری های سامانه ها، تجهیزات و شبکه سازمان است. این فرایند شامل شناسایی، اصلاح و بازرسی مداوم تهدیدات امنیتی است و با کاهش ریسک ها، سطح حمله به حداقل می رسد. امن سازی، بخشی حیاتی از استراتژی امنیت سایبری است که احتمال موفقیت حملات را به شدت کاهش می دهد. حتی با وجود بهترین تجهیزات، پیکربندی نادرست می تواند خطرات جدی ایجاد کند.



کمپین فیشینگ (PHISHING CAMPAIGN)

فیشینگ نوعی حمله با استفاده از مهندسی اجتماعی است که در آن هکرها افراد را فریب می‌دهند تا اطلاعات حساس مانند نام کاربری، رمز عبور و اطلاعات سازمانی را جمع‌آوری کنند. این حملات معمولاً از طریق ایمیل‌ها، تماس‌ها و پیامک‌های جعلی انجام می‌شوند. برگزاری کمپین فیشینگ در سازمان، کارکنان را به صورت هدفمند و کنترل شده مورد آزمون قرار می‌دهد تا از میزان بلوغ امنیتی آن‌ها مطلع شوید. پس از انجام این فرایند، گزارشی جهت ارائه دقیق شواهد جمع‌آوری شده تهیه می‌شود و جلسات آموزشی برای کارکنان و مدیران برگزار می‌شود.



PHISHING

به عنوان مثال، این حملات بدین صورت انجام می‌گیرند که در ایمیل‌ها، اشخاص را متقاعد می‌کنند تا اطلاعات شخصی خود را وارد یک وب‌سایت جعلی کنند یا فایل آلوده ضمیمه شده به ایمیل را در سیستم ذخیره و اجرا کنند. این کار باعث آلوده شدن سیستم، سرقت و سوء استفاده از اطلاعات سازمان می‌شود.

تست نفوذ (PENETRATION TEST)

تست نفوذپذیری، در واقع حملات شبیه‌سازی شده سایبری به ساختار سیستم‌های کسب‌وکار شما در شرایط کنترل شده است. هدف از این حملات شبیه‌سازی شده، پیدا کردن نقاط ضعف امنیتی سازمان و برطرف کردن آن‌هاست. در تست نفوذپذیری از همان تکنیک‌ها، ابزارها و فرایندهایی استفاده می‌شود که هکرها برای نفوذ به سامانه‌ها و سرویس‌های یک سازمان استفاده می‌کنند. به طور معمول، تمامی حملاتی که سازمان را تهدید می‌کنند، شبیه‌سازی می‌شوند تا حفره‌های امنیتی سازمان شناسایی و برطرف شوند. این فرایند به آزمونگران نفوذ اجازه می‌دهد که میزان تاب‌آوری سیستم‌عامل‌ها، نرم‌افزارها و تجهیزات شبکه را در مقابل یک ارزیابی امنیتی بسنجند و توصیه‌هایی برای تقویت ساختار سازمان در برابر آسیب‌پذیری‌های کشف شده ارائه دهند.



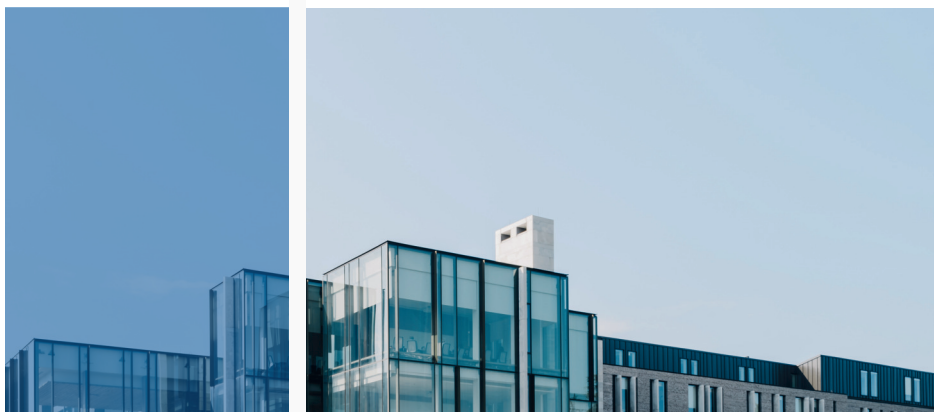
انواع تست نفوذ

تست نفوذ جعبه سفید (White Box Penetration Testing)

تست نفوذ جعبه سیاه (Black Box Penetration Testing)

تست نفوذ جعبه خاکستری (Gray Box Penetration Testing)

ارزیابی آسیب پذیری (VULNERABILITY ASSESSMENT)



ارزیابی آسیب پذیری فرایندی است که سازمان را از نظر وجود ضعف های احتمالی و موارد آسیب پذیر در تمامی سرویس ها، تجهیزات و سامانه ها ارزیابی می کند. این فرایند به سازمان امکان شناسایی و اصلاح آسیب پذیری های موجود را می دهد. پس از انجام ارزیابی، گزارشی شامل آسیب پذیری های شناسایی شده، چگونگی استفاده از آنها توسط هکر، سطح مخرب بودن و پیامدهای منفی در صورت عدم اصلاح، و روش های اصلاح آسیب پذیری تهیه می شود.

انجام ارزیابی آسیب پذیری به صورت دوره ای و منظم، می تواند سازمان را تا حد بسیار بالایی در مقابل تهدیدات سایبری، مقاوم کند.



انطباق سنجی فنی

(COMPLIANCE CHECK)

انطباق سنجی فرایند بررسی و تجزیه و تحلیل کنترل‌های اجرا شده روی تنظیمات تجهیزات و سرویس‌ها است. این فرایند برای بررسی اجرای صحیح الزامات امنیتی مطابق با استانداردهای بین‌المللی استفاده می‌شود. متخصصان امنیتی با استفاده از استانداردهای به‌روز، به بررسی تنظیمات پیکربندی شده در سازمان می‌پردازند و گزارشی از عدم انطباق‌های موجود تهیه می‌کنند.

از جمله استانداردهای مورد استفاده در این فرایند می‌توان به ITIL، DISA، COBIT، CIS، HIPAA، DSS، SDP و STIG اشاره کرد.



آگاهی رسانی امنیتی (SECURITY AWARENESS)

آگاهی رسانی امنیتی (Security Awareness) با هدف آموزش کارکنان و ارتقای سطح آگاهی امنیتی آن‌ها ارائه می‌شود. این دوره‌ها به گونه‌ای طراحی شده‌اند که مفاهیم کلیدی امنیت اطلاعات، از جمله شناسایی تهدیدات، رفتارهای امن در فضای دیجیتال، و مقابله با حملات فیشینگ و مهندسی اجتماعی، به کارکنان آموزش داده شوند.

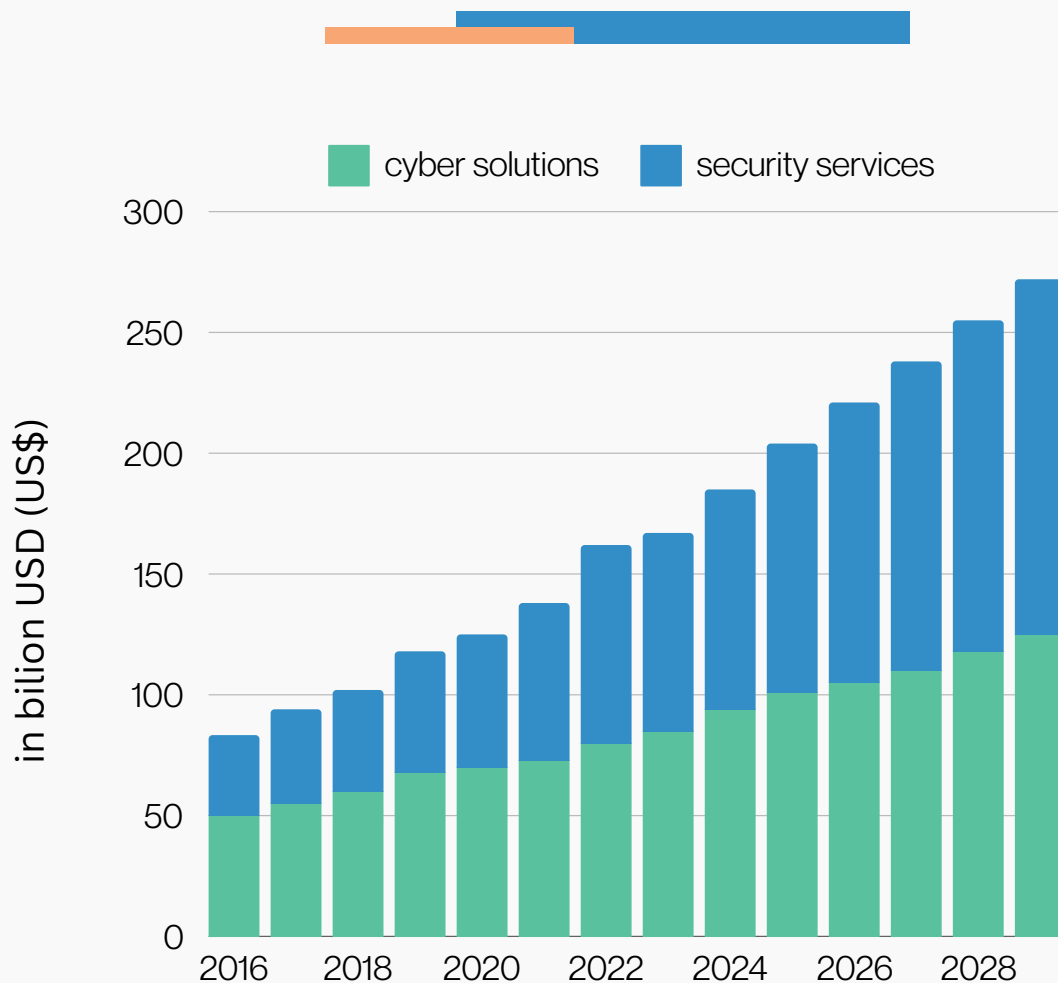


این دوره‌ها به‌طور منظم برگزار می‌شوند و شامل آزمون‌های ارزیابی، سناریوهای واقعی و محتوای تعاملی هستند تا کارکنان را برای شناسایی و واکنش به تهدیدات روزمره آماده کنند. در نهایت، Security Awareness به سازمان‌ها کمک می‌کند تا سطح کلی آگاهی امنیتی خود را افزایش دهند و فرهنگ امنیتی قوی‌تری در محیط کار ایجاد کنند، که در نتیجه، امنیت کلی سازمان بهبود یافته و از وقوع بسیاری از حوادث قابل پیشگیری جلوگیری شود.

خدمات بسته‌های نقره‌ای و طلایی

Gold	Silver	خدمت
✓	✗	تیم قرمز (Red team)
✓	✓	آزمون نفوذ (Penetration Test)
✓	✗	پاسخگویی به حوادث امنیتی (Incident Response)
✓	✓	ارزیابی آسیب‌پذیری (Vulnerability Assessment)
✓	✓	آموزش و آگاهی‌رسانی امنیتی (Security Awareness Training)
✓	✓	کمپین جعل ایمیل (Phishing Campaigns)
✓	✗	جرم‌یابی سایبری (Digital Forensics)
✓	✓	انطباق‌سنجی (Compliance check)
✓	✗	امن‌سازی (Hardening)

CYBERSECURITY INVESTMENT



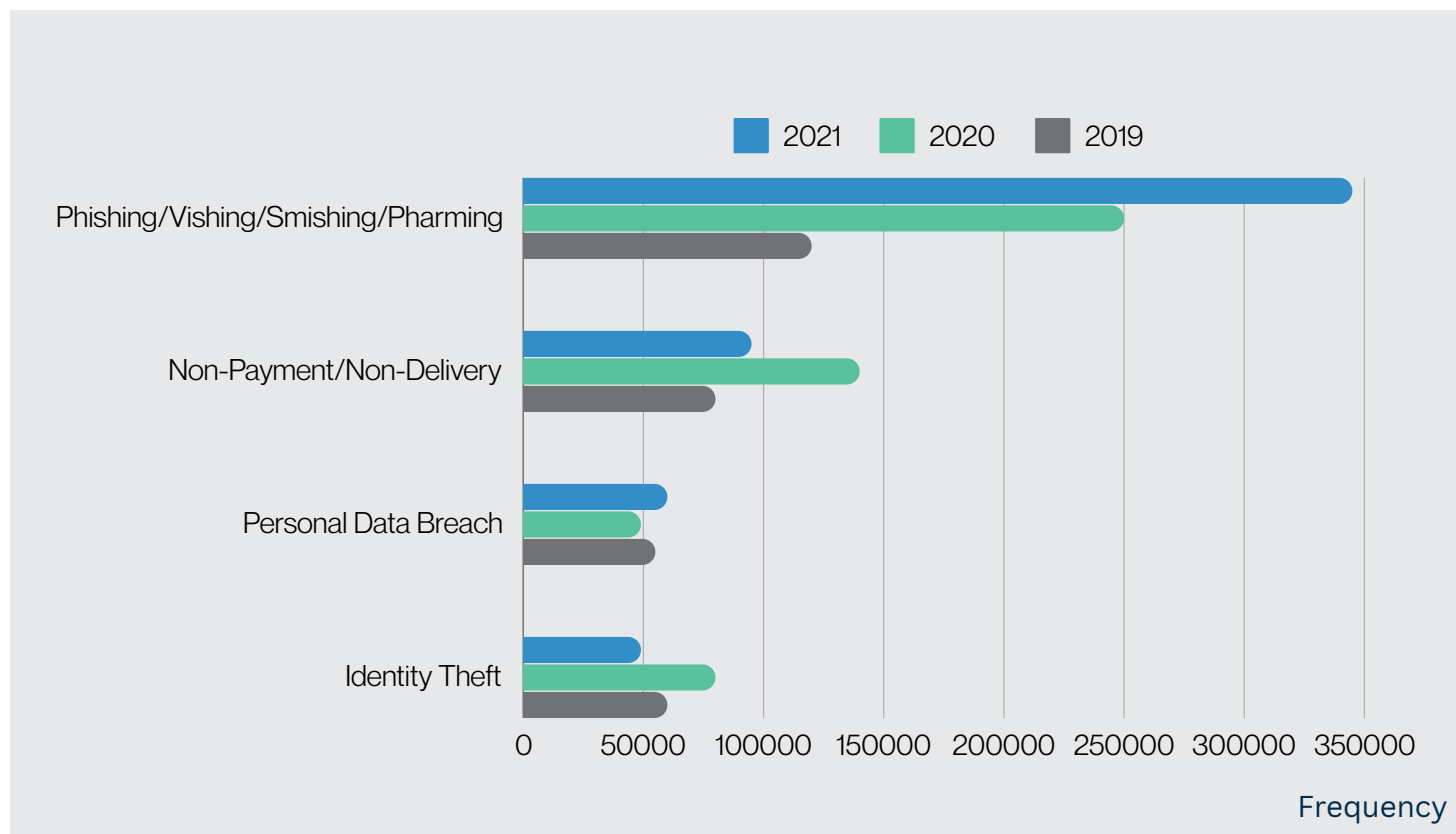
Remediate gaps within your existing tech stack

Automate risk discovery and assessment processes

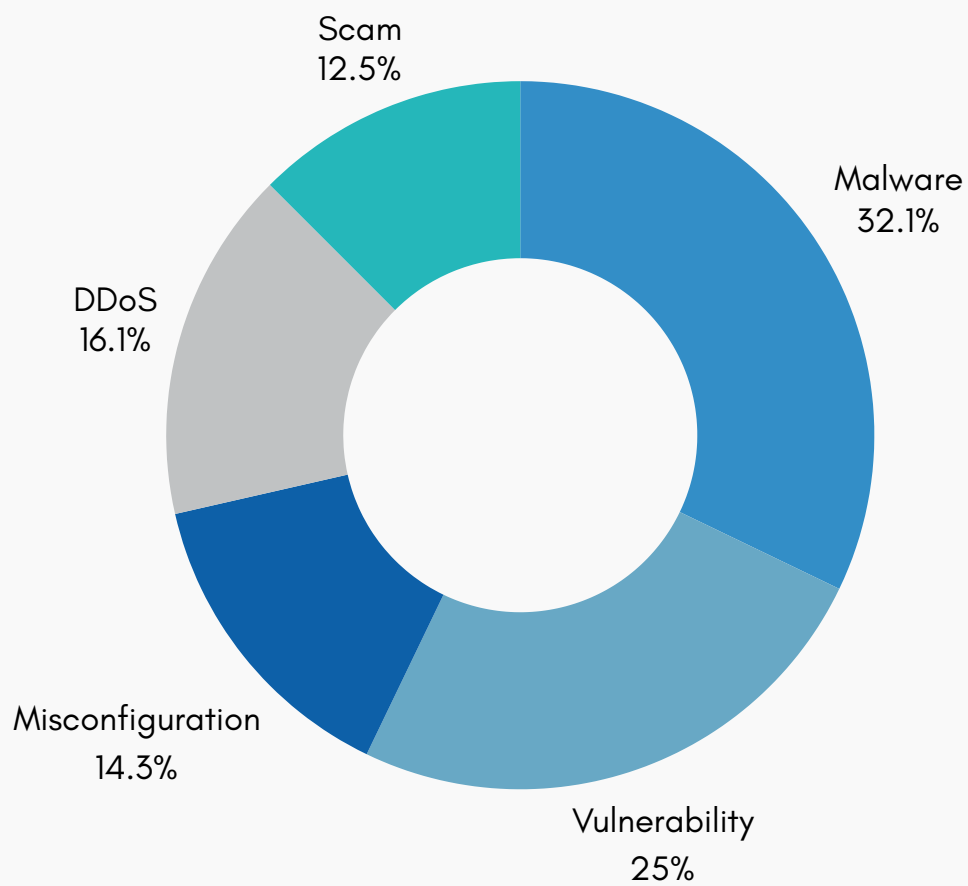
Make strategic, data-driven decisions

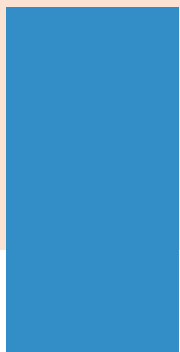
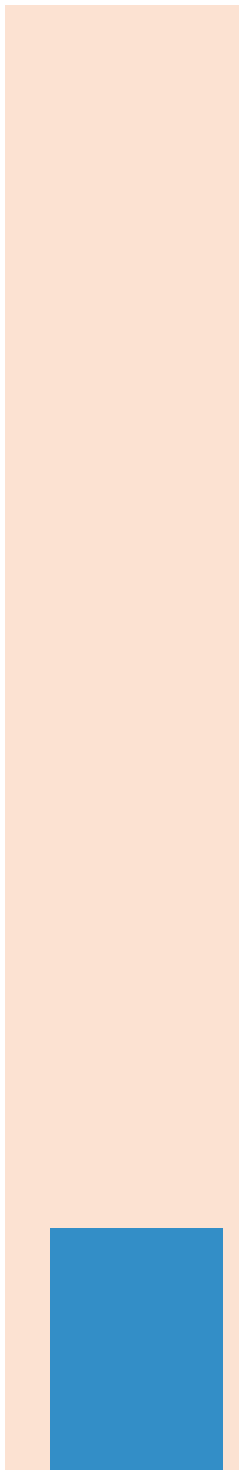


A COMPARISON OF THE TOP 5 CRIME TYPES (2019-2021)



TOP 5 ATTACKS 2023





HIRSAVISION

At the heart of Hirsavision's mission lies one goal: to deliver world-class cybersecurity services that shield organizations from today's evolving threats. With over a decade of expertise in cyber defense, we empower businesses to stay ahead of cybercriminals and secure their most vital assets. From advanced threat detection to comprehensive network protection, we tailor our services to meet the unique security needs of industries such as telecom, banking, energy, and beyond. Your security is our priority.

Address

unitB4 .4th Floor, No.26,East Daneshvar St,
North Shirazi St, Molla Sadra St, Tehran.

Phone & fax

+98 21 88 61 81 41-2

Website

hirsavision.co

Mail

info@Hirsavision.co



Website



Linkedin