شرکت فنی مهندسی

نوآوران افراتک هوشمند

قواعد بازی را تعیین کنید...

تامین تجهیزات و لایسنس‌ها

ارائه راهکار، اجرا و پشتیبانی

تعمیرات تخصصی

آموزش

AFRATEC

afratec.ir

شرکت فنی مهندسی نوآوران افراتک هوشمند

مجوزها و گواهینامه‌ها

- مجوز فعالیت از نظام صنفی رایانه‌ای استان تهران
- گواهینامه صلاحیت خدمات انفورماتیک
- گواهی «امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها» (افتا)
- گواهی «نصب و پشتیبانی محصولات فتا» (افتا)
- گواهی «آموزش امنیت فضای تولید و تبادل اطلاعات» (افتا)
- گواهینامه صلاحیت ارائه خدمات در حوزه پدافند سایبری
- عضویت انجمن انفورماتیک ایران

گواهینامه‌های بین‌المللی کارشناسان فنی افراتک

- **CISSP** (Certified Information Systems Security Professional)
- **CCNP Routing and Switching** (Cisco Certified Network Professional Routing and Switching)
- **Cisco Certified Internetwork Expert Written**
- **MCSE** (Microsoft Certified Systems Engineer)
- **Business Continuity Management System - Auditor/Lead Auditor** (ISO/IEC 22301)
- **Information Security Management System (ISMS) Auditor/Lead Auditor** (ISO/IEC 27001:2013)
- **ITIL Foundation Certificate in IT Service Management**
- **FCNSA V4.x** (Fortinet Certified Network Security Administrator)
- **FCNSP V4.x** (Fortinet Certified Network Security Professional)
- **ICSI | CNSS Cerified Network Security Specialist**
- **MCSA** (Microsoft Certified Systems Administrator)
- **CCNA** (Cisco Certified Network Associate)
- **MCTS** (Microsoft Certified Technology Specialist)
- **Cisco Certified Specialist - Enterprise Core**
- **Cisco Certified Networking Professional -Enterprise**
- **Cisco Certified Specialist - Enterprise Advanced Infrastructure Implementation** (CCS-EAII)
- **NSE1 & NSE2 Network Security Associate** (Fortinet)
- **Kaspersky Threat Intelligence** (Certified Professional)

معرفی شرکت

امروزه با پیشرفت‌های فناوری اطلاعات و ظهور نیازمندی‌های خاص این عصر، اتکای بخش دولتی و خصوصی کشور به فضای تبادل اطلاعات در حال افزایش است. از طرفی پیچیدگی روزافزون فناوری اطلاعات، سازمان‌ها را با مجموعه‌ای از چالش‌ها و تهدیداتی مواجه کرده است که بعضاً با توجه به مقتضیات کشور (همچون تحریم‌های همه‌جانبه)، دغدغه‌های جدیدی را نیز با ماهیت و کیفیت متفاوت مطرح نموده است. برطرف‌سازی این مخاطرات و گام برداشتن در راستای تامین خدمات امن و یکپارچه در سطح خدمات حساس و حیاتی، نه تنها نیازمند اشراف به تهدیدات روزافزون، بلکه مستلزم آشنایی با چالش‌های بخش دولتی و خصوصی کشور است.

«**شرکت فنی-مهندسی نوآوران افراتک هوشمند**» با هدف همیاری سازمان‌ها و کسب‌وکارهای متکی بر خدمات فناوری اطلاعات و با عنایت به مقتضیات و نیازمندی‌های کنونی کشور از سال ۱۳۹۳ فعالیت خود را در زمینه پشتیبانی خدمات زیرساختی و امنیت اطلاعات و سرویس‌های حساس سازمان‌ها و شرکت‌ها در دو حوزه اصلی ارائه خدمات فناوری اطلاعات و همچنین تامین تجهیزات و لایسنس‌های آن‌ها در این حوزه آغاز نموده است. همچنین **شرکت افراتک** از سال ۱۳۹۸ خدمات خود را در زمینه انتقال دانش و ارتقای فرهنگ امنیت اطلاعات توسعه داده است.

شرکت «**افراتک**» طی سنوات خدمت خود در عرصه تأمین زیرساخت‌ها و ارائه راهکارهای فناوری اطلاعات توانسته ضمن توسعه خدمات خود، اعتماد بخش خصوصی و دولتی را کسب نموده و مفتخر است که در فهرست تأمین‌کنندگان شماری از ادارات و سازمان‌های دولتی قرار گرفته است. همچنین با عنایت به سابقه فعالیت و دانش عمیق در تأمین تجهیزات امنیتی و ارتباطی فناوری اطلاعات، این مجموعه توانسته است با چندین شرکت خدماتی همکار، ارتباطات سازنده‌ای برای تبادل تجارب و هم‌افزایی ایجاد کند.

شرکت افراتک آماده است تا به پشتوانه دانش تخصصی و تجربه چندین ساله کارشناسان فنی و متخصصین در محیط‌های عملیاتی حساس خدمت‌رسانی نماید. همچنین این شرکت با بهره‌گیری از ارتباطات قوی با شرکای تجاری بین‌المللی در زمینه تأمین تجهیزات معتبر خارجی، خدماتی قابل اطمینان و متناسب با نیاز سازمان‌ها و شرکت‌ها را ارائه می‌نماید.

خدمات افراتک

تامین تجهیزات و لایسنس‌ها

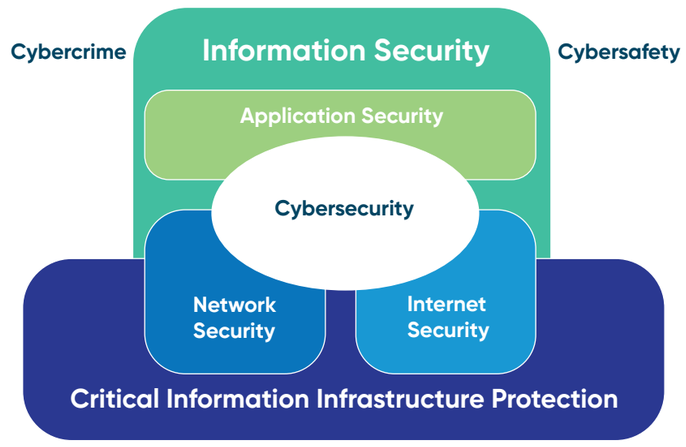
شرکت افراتک آمادگی خود را درجهت تأمین و ارائه تجهیزات و لایسنس‌های ذیل اعلام می‌دارد:

حوزه		نام تجهیزات
محصولات حوزه شبکه	شبکه	Cisco
		MikroTik
	ذخیره‌سازی	HPE
		EMC
		QNAP
	پردازش	HPE
		EMC
	Load Balancer توزیع‌کننده بار	F5 LTM
		FortiADC
امنیت	WAF (دیواره آتش لایه کاربردی)	FortiWeb
		F5 ASM
		Imperva WAF

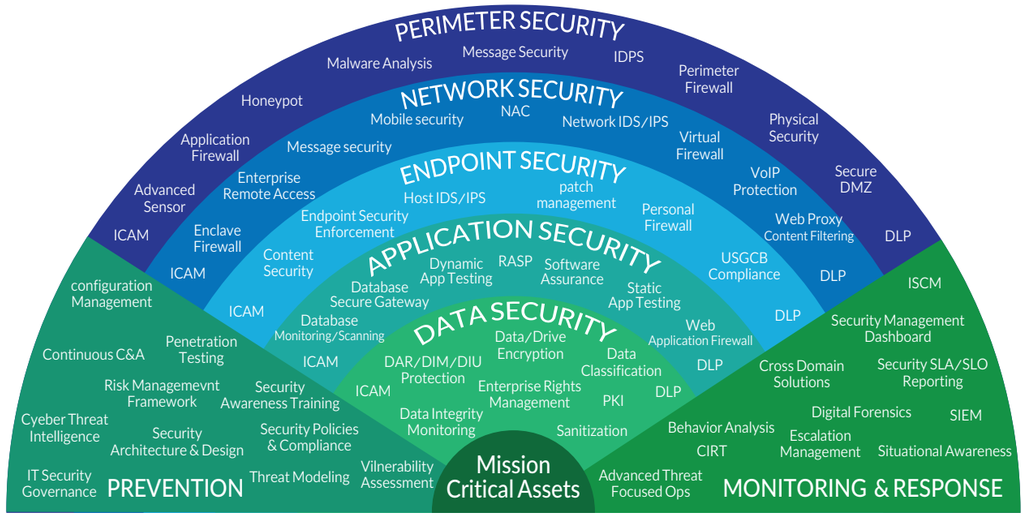
حوزه		نام تجهیزات
امنیت	Firewall (دیواره‌ی آتش)	FortiGate NGFW
		Cisco ASA
		Juniper NGFW
		Palo Alto
	Endpoint Protection DLP File Integrity Monitor	Symantec
		Kaspersky
		ESET
		BitDefender
		TripWire FIM
	Vulnerability Assessment & Penetration Test (ارزیابی امنیتی و آزمون نفوذ)	Nessus Professional
		Tenable.io
		Standard Acunetix
		Premium Acunetix
		Acunetix 360
		Burp Suite
		Core Impact
		Metasploit
		Fortify
	Mail Secuirty (امنیت سرویس ایمیل)	FortiMail
		Cisco ESA
	SIEM	Micro Focus ArcSight
		IBM Security Qradar
		Splunk Enterprise Security (ES)
		FortiSIEM
	Identity and Access Management	FortiAuthenticator
		FortiToken
		FortiNAC
		CyberArk
	Industrial Security	Kaspersky Industrial Cyber Security

خدمات ارائه راهکار، اجرا و پشتیبانی

طبـق اسـتانداردها و چارچوب‌ها، امنیـت فضای تبادل اطلاعات می‌تواند متناسـب با دغدغه‌هـا، با امنیت در حیطه‌های متفاوتی دنبال شود؛ این حیطه‌ها نظیر امنیت داده، امنیت برنامه کاربردی، امنیت سایبری، امنیت شـبکه، امنیـت اینترنـت و حفاظت از زیرسـاخت اطلاعـات حیاتی، مکمـل یکدیگرند و می‌تواننـد با یکدیگر همپوشانی داشته باشند. اغلب اوقات تأمین امنیت در سازمان‌ها نیازمند توجه به چندین حیطه از حوزه‌های امنیت فضای تبادل اطلاعات اسـت. با علم به اینکه توجه به یک حیطه برای حفظ امنیت کسـب‌وکار و مدیریت ریسـک‌های آن کافی نیسـت، ضروری است متناسـب با نوع مأموریت یا کسـب و کار و همچنین زمینه و نوع حساسـیت سـرویس‌ها و دارایی‌های حیاتی سـازمان، ارتقای امنیت در چندین لایه دنبال شـود. امروزه این رویکرد در دنیای امنیت با عناوینی همچون «دفاع چند-لایه» شناخته می‌شود.



حیطه‌های مختلف امنیت و ارتباط بین آن‌ها



مکانیزم‌های دفاع چندلایه

ایده اصلی مکانیزم دفاع چند-لایه (همانطور که در نمودار فوق مشـاهده می شود)، محافظت از یک سیستم با چندین روش متفاوت و مسـتقل از هم در برابر حملات گوناگون است. دشوار ساختن راه نفوذ نفوذگرها و کاهش مخاطرات داخلی سـازمان از طریق ایجاد کنترل‌های متعدد یکی از شناخته‌شـده‌ترین بهروش‌ها برای حفاظت از دارایی‌های حساس سازمان‌ها است.

شـرکت افراتک با بهره‌گیـری از تجربیات پروژه‌های متعـدد و بهروش‌های مطرح امنیتـی در خصوص دفاع چند-لایه، راهکاری‌های متعددی برای باز طراحی مکانیزم‌های امنیتی سـازمان‌ها ارائه می‌نماید. به طور کلی خدمات افراتک در زمینه‌ی «ارائه راهکار، اجرا و پشتیبانی» شامل حوزه‌های زیر می‌شود:

در ادامه هر یک از این حوزه‌ها به تفصیل شرح داده خواهد شد.

خدمات امنیت پایانه‌ها و داده‌های فناوری اطلاعات

در دو دهه گذشته، حفاظت از سیستم‌عامل بیش از پیش به یکی از اساسی‌ترین لایه‌های دفاعی سامانه‌های اطلاعاتی بدل شـــده است. ثابت شده است که حفاظت از سیستم‌عاملِ سرورها، ضرورتی فراتر از حفاظت در برابر انواع بدافزارها است و می‌تواند نقش یک کنترل تشخیصی و تکمیلی را نیز داشته باشد؛ از جمله‌ی این کنترل‌ها می‌توان به امن‌ســازی سرورها و ســرویس‌ها (Hardening)، کنترل تغییرات ناخواسته در سرور، گردآوری اطلاعات هوش تهدید و ارسال انواع لاگ از وقایع روی سامانه‌ها اشاره نمود.

می‌دانیم که حفاظت از گردش اطلاعات در ســطح پایانه‌های کاربری (تأمین امنیت پایانه‌های کاری) اهمیت دو چندانی دارد. امنیت پایانه‌های کاری به دو دلیل حائز اهمیت فراوانی است؛ اول، این پایانه‌ها به عنوان ابزار پردازشـــی اطلاعات سازمان کاربری دارند؛ دوم، این پایانه‌ها ابزار کاریِ کاربران ناآگاه، ناراضی و بعضا نفوذی هستند و هر کدام از این کاربران برحسب وظایف خود در سطوح متفاوتی به اطلاعات سازمان دسترسی دارند. بعد از شـــیوع بدافزارهایی در ســطح محیط‌های عملیاتی (همچون Stuxnet، در دهـــه اول ۲۰۰۰)، و موارد متعددی از افشای اطلاعات مشتریان کسب‌وکاری، (علاوه بر کنترل‌های مربوط به حوزه فناوری اطلاعات) امنیت در ســطح پایانه‌ها به سمت حفاظت از سیستم‌های اطلاعاتی خاص‌منظوره‌ی خدمات بانکی و همچنین بسترهای کنترل صنعتی (ICS) در زیرساخت‌های حیاتی سوق پیدا کرده است.

با عنایت به تحول به وجود آمده در این حوزه و اهمیت توجه تخصصی‌تر به حوزهٔ حفاظت از پایانه‌های اطلاعاتی و عملیاتی، **شرکت افراتک** خدمات خود را برای این حوزه متناسب با نیازمندی‌های داخلی و جهانی توسعه داده است:

- مشاوره، پیاده‌سازی و توسعه راهکارهای جامع امنیت پایانه‌ها و سرورها برای شبکه‌های سازمانی و پایانه‌های عملیاتی زیرساخت‌های حیاتی
- مشاوره و پیاده‌سازی Endpoint Security و آنتی ویروس متمرکز در سطح سازمان‌ها با اتکا به برندهای معتبری همچون Bitdefender، ESET، Kaspersky و همچنین محصولات بومی نظیر پادویش.
- مشاوره، پیاده‌سازی و بهینه‌سازیِ ساز و کارهای کنترل گردش اطلاعات (مبتنی بر DLP) در سازمان
- مشـــاوره و اجـــرا در خصوص امن‌ســـازی ســـرویس‌ها و سیســـتم‌های متعـــارف و همچنین امنیت زیرساخت‌های مجازی‌سازی

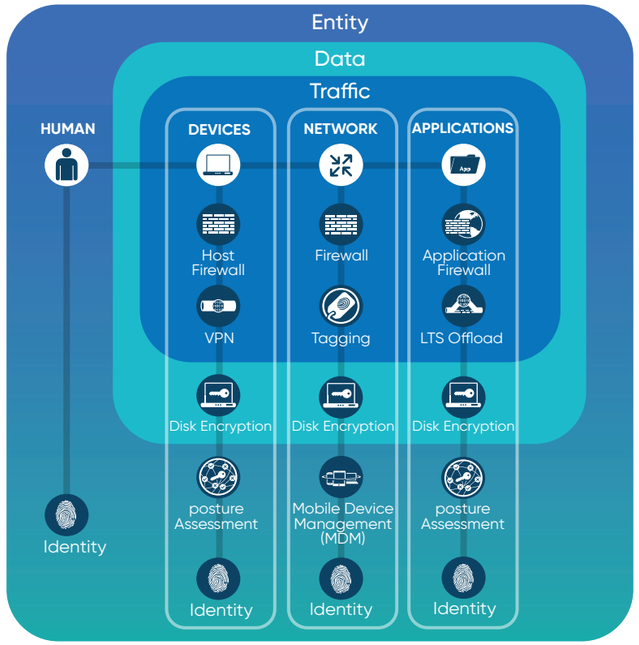
خدمات امنیت شبکه

الف. ارائه راهکارهای معماری امن شبکه (Secure Network Architecture)

بسیاری از حملات و نفوذها به شبکه یک سازمان، به دلیل ساختار و توپولوژی شبکه ناامن یا نامتناسب با مأموریت و نیازمندی‌های آن سازمان رخ می‌دهد. علاوه بر این، استقرار توپولوژی (همبندی) نامتناسب تجهیزات و همچنین تنوع سرویس‌های فناوری اطلاعات، می‌تواند به بستری برای نفوذ به شبکه یا دسترسی غیرمجاز در شبکه بدل شود. بنابراین ضروری است معماری شبکه هر سازمان متناسب با مأموریت سازمان، جنس خدمات و تنوع دسترسی های داخلی و بیرونی بر روی شبکه آن سازمان طراحی و پیاده سازی شود.

ب. پیاده‌سازی، بهینه‌سازی و پشتیبانی تجهیزات امنیت شبکه

تجهیزات امنیتی متعددی برای امن‌سازی شبکه و زیرساخت فناوری اطلاعات وجود دارد که از مهم‌ترینروان به فایروال‌های شبکه، فایروال‌های برنامه کاربردی تحت وب (WAF) و سیستم‌های تشخیص نفوذ (IDS) اشاره کرد.



دفاع چند لایه با رویکرد طراحی بی‌اعتماد (ZTA) در داخل سازمان

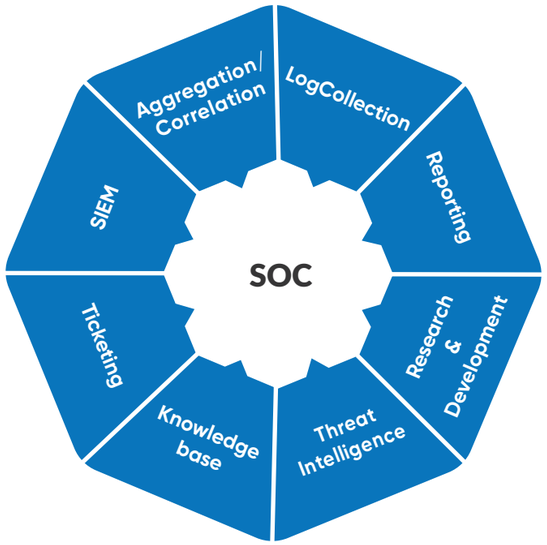
شرکت افراتک در زمینه امنیت شبکه، خدمات ذیل را ارائه می‌نماید:

- مشاوره، طراحی و پیاده‌سازی معماری امن شبکه متناسب با کاربرد شبکه
- مشاوره، اصلاح معماری شبکه و بهینه‌سازی تجهیزات امنیتی پیاده‌سازی شده در شبکه
- پیاده‌سازی و بهینه‌سازی فایروال‌های برنامه کاربردی تحت وب (WAF)
- پیاده‌سازی و بهینه‌سازی سیستم‌های تشخیص و جلوگیری از نفوذ(IPS/IDS)
- تعمیرات سخت‌افزاری و پشتیبانی نرم‌افزاری تجهیزات امنیت شبکه

خدمات زیرساخت پایش و نظارت امنیتی

تنوع و پیچیدگی روزافزون تهدیدات در کنار افزایش تعدد سرویس‌های فناوری اطلاعات در سازمان‌ها موجب شده است که توجه به حجم عظیمی از لاگ‌ها و رویدادهای امنیتی که روزانه تولید می‌شوند، اهمیتی دو چندان پیدا کند.

برای کشف و شناسایی حملات سایبری ضروری است این رویدادهای امنیتی به طور مستمر مورد پایش و نظارت قرار گیرند. یکی از بنیادی‌ترین اقدامات در راستای پایش و نظارتِ حملات امنیت سایبری در سازمان‌های مهم یا زیرساخت‌های حیاتی، پیاده‌سازی مرکز عملیات امنیت (Security Operation Center) است. مرکز عملیات امنیت، مجموعه‌ای از پلتفرم‌ها، افراد، فرایندها و ابزارهاست که وظیفه نظارت بر وقایع و حوادث تهدید کننده امنیت اطلاعات را برعهده دارد. هدف از ایجاد مرکز عملیات امنیت، شناسایی تهدیدات بالقوه یا جاری امنیتی و تحلیل و آنالیز این وقایع امنیتی در راستای اجرای اقدامات امنیتی مناسب برای بهبود سطح امنیت است.

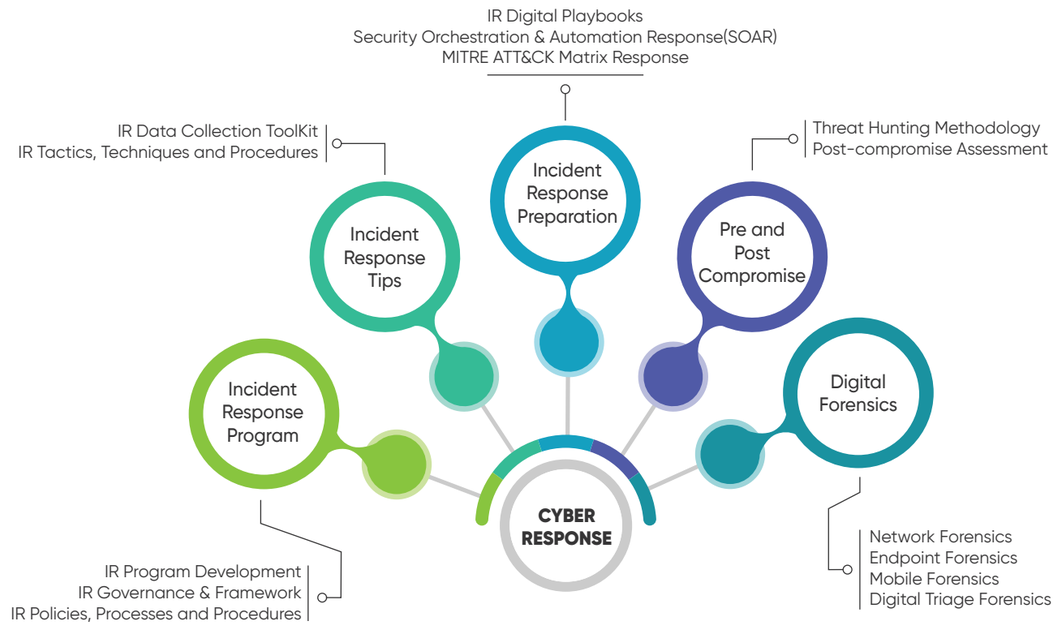


شرکت افراتک، خدمات خود را در حوزه پایش و نظارت امنیتی، در قالب عناوین ذیل ارائه می‌نماید:

- مشاوره و طراحی فنی مرکز عملیات امنیت (SOC)
- راه‌اندازی اولیه و پیکربندی مرکز عملیات امنیت (SOC) و ارائه آموزش‌های مرتبط با آن
- خدمات بهینه‌سازی پیکربندی و پیکربندی‌های پیشرفته SIEM
- مشاوره و طراحی زیرساخت فیزیکی SOC

خدمات کشف و استخراج ادله دیجیتال و تحلیل جرائم رایانه‌ای
(Digital evidence and computer crime)

در یک سازمان، در صورت بروز خدشه در خدمات و اطلاعات در نتیجه‌ی وقوع رخدادهای امنیتی چه باید کرد؟ امروزه، با توجه به افزایش رخدادهای امنیتی منجر به خسارت یا نیازمند پیگیری حقوقی در کسب‌وکارهای الکترونیکی، ضرورت ارائه شواهدی از عوامل عمدی و سهوِی منجر به زیان‌های کسب‌وکاری بیش از پیش احساس می‌شود. این مساله سازمان‌ها را بر آن داشته که به دنبال راهکاری باشند تا بتوانند در قالب ساختارهای متعارف، علل وقوع حوادث امنیتی منجر به خسارت در سازمان را استخراج کنند. این روال‌ها در نهادهای ضابط قوانین فضای تبادل اطلاعات و همچنین بخش‌های اطلاعاتی و نظامی، در چارچوب‌های ساختاریافته‌ای وجود دارد؛ با این وجود بنگاه‌های تجاری ترجیح می‌دهند حتی در شرایطی که جرم رایانه‌ای مدعی‌العموم ندارد، بتوانند علت و عوامل ریشه‌ای آن را با کمترین هزینه کشف نمایند.



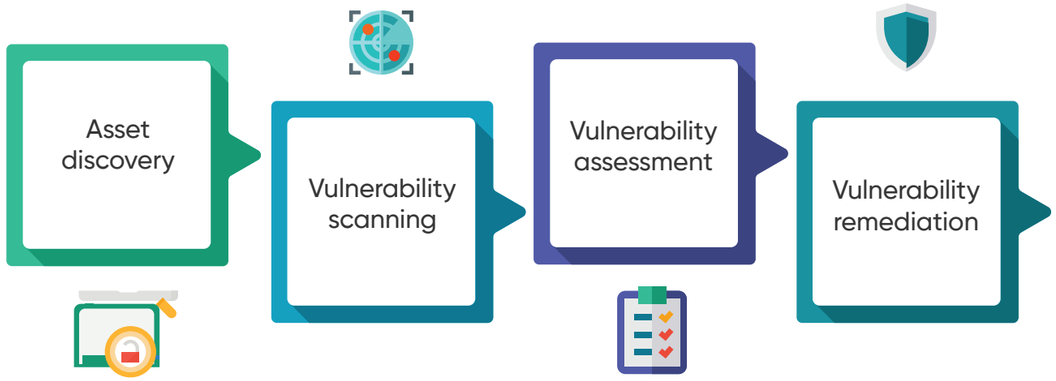
در ساختار عمومیِ کشف و رسیدگی جرائم رایانه‌ای تجاری (که به صورت معمول توسط نهادهای حاکمیتی دنبال می‌شود) تحقیق و تحلیل حادثه با ارائه گزارشی از «یافته‌ها» تمام می‌شود. همچنین اگر لازم باشد تا زمان طی شدن روال رسیدگی به حادثه، سیستم‌های اطلاعاتی کسب‌وکار توسط ضابط قانونی توقیف باشد کسب و کار بیشتر متضرر خواهد شد. بنابراین، لازم است که بنگاه‌های تجاری در کنار دنبال کردن روال‌های بازآوری سریع سیستم‌های اطلاعاتی و خدمات کسب‌وکار، به طریقی قابل اطمینان، شواهد حادثه را ضبط و حفظ کنند. بدین ترتیب سازمان‌ها می‌توانند در زمان مناسب آن را از جنبه حقوقی پیگیری کنند و خسارت وارد شده را ازطریق احکام حقوقی یا بیمه امنیت فضای تبادل اطلاعات جبران کنند.

لذا ضروری است که مالکان کسب‌وکارهای حساس و کلیدی، فرایند مدیریت حوادث امنیتی خود را به مهارت‌ها، روال‌ها و ابزار استخراج و کشف ادله دیجیتالیِ مرتبط با رخداد حادثه و جرائم رایانه‌ای مجهز کنند. **شرکت افراتک** خدمات خود را در حوزه کشف و استخراج ادله دیجیتال و تحلیل جرائم رایانه‌ای، در قالب عناوین ذیل ارائه می‌نماید:

- مشاوره و راه‌اندازی ابزار تحلیل، کشف و استخراج ادله دیجیتالِ مرتبط با رخدادهای امنیتی و جرائم رایانه‌ای و ارائه آموزش‌های مرتبط با آن
- مساعدت در تحقیق، تحلیل و ضبط ادله دیجیتال رخدادهای امنیتی بر حسب مورد یا در قالب قراردادهای بلندمدت

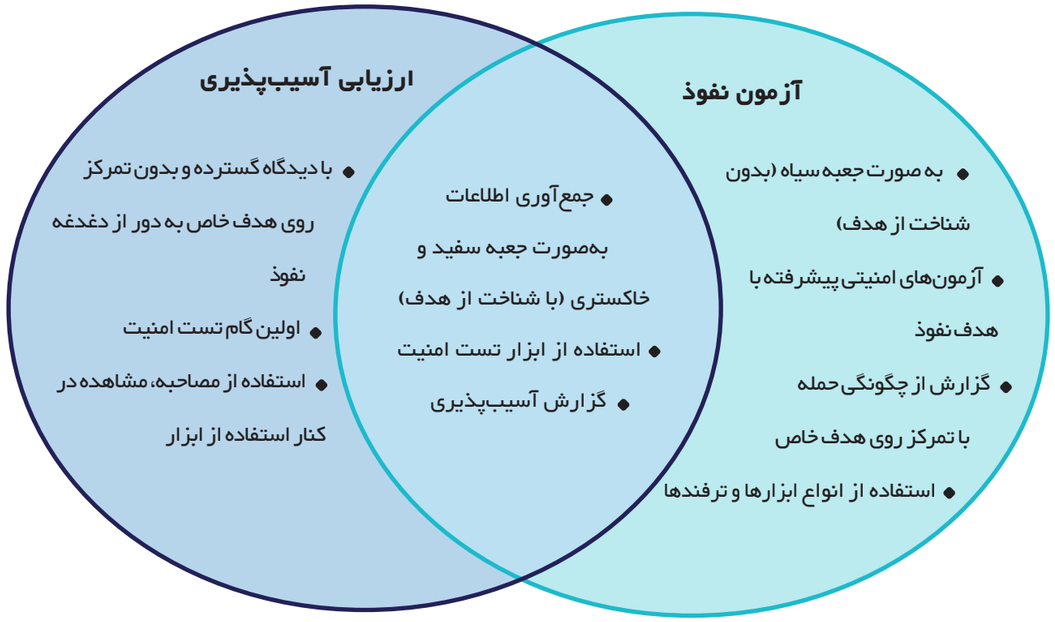
خدمات ارزیابی امنیتی وآزمون نفوذ
(Security Assessment & Penetration Test)

وقوع خطای انســانی در فرایندها و نقائص نرم‌افزاری بسیار محتمل است و طبق مطالعه‌ای که توسط موسسه غیرانتفاعی CompTIA انجام شده است خطای انســانی دلیل اصلیِ ۵۲% از حوادث امنیتی در سازمان‌ها را شــامل می‌شــود. بنابراین اطمینان از امنیت حاصل نخواهد شد مگر این که علاوه بر اتکا به ابزارهای کنترلی قابل اطمینان و اقدامات عملیاتی تعریف شــده بــرای مواجهه با حملات، ســازمان‌ها برنامه‌هایی مرتب برای بررســی احتمال وجود این نقائص داشــته باشــند. در واقع در کنار برنامه‌های ممیــزی داخلی، بهره‌گیری از ابزارهای پویش آسیب‌پذیری به کارکنان فناوری اطلاعات کمک می‌کند تا نقائص نرم‌افزاری جاری در سازمان را به صورت دقیق و مرتب شناسایی کرده و مراتب پیگیری برای برطرف سازی آن‌ها را دنبال کنند.



«آزمون نفوذ»، خدماتی قاعده‌مند برای ارزیابی امنیت زیرســاخت فناوری اطلاعات، سامانه‌ها، اپلیکیشن‌های موبایل و نرم‌افزارها در زمان سرویس‌دهی روزمره است و سعی می‌کند نقاط ضعف مرتبط با عملکرد سیستم را از دیدگاه یک نفوذگر کشــف کند. منشــأ این نقاط ضعف می‌تواند یک آسیب‌پذیری در بستر نرم‌افزاری، پیکربندی نامناســب نرم‌افزار یا سیستم‌عامل، پیکربندی نامناسب یا آسیب‌پذیری در تجهیزات شبکه مرتبط با سرویس و یا حتی رفتار ناامن کاربران در انجام امور روزمره و یا در مواجهه با شرایط خاص باشد.

در واقع آزمون نفوذ حمله‌ای را به واســطه یک نفوذگر شبیه‌ســازی می‌کند و از این طریق سعی می‌کند نقاط ضعف فنی و فرایندی عناصر یک ســرویس‌دهنده در سازمان را کشف نماید. علاوه بر این، اعتبارسنجی تأثیر مکانیزم‌های دفاعیِ موجو بررســی میزان آگاهی و التزام عملی کاربران نسبت به سیاست‌های امنیتی جاری، از دیگر دستاوردهای اجرای آزمون نفوذ در یک سازمان است.



شرکت افراتک خدمات آزمون نفوذ و استقرار فرایند مدیریت آسیب‌پذیری در یک سازمان را در قالب عناوین ذیل ارائه می‌کند:

- مشاوره و راه‌اندازی زیرساخت‌های ارزیابی امنیتیِ متناسب با مأموریت سازمان
- مشاوره، استقرار و بهینه‌سازی فرایندهای مرتبط با ارزیابی امنیتی در سازمان
- مشاوره و اجرای خدمات آزمون نفوذ
- مشاوره در برطرف‌سازی مخاطرات و آسیب‌پذیری‌های امنیتی

مشاوره و مدیریت امنیت اطلاعات

امنیت اطلاعات به عنوان یک شاخص کیفی در یک سازمان، مستلزم استقرار کنترل‌های محدودکننده، هزینه‌بر و تا حدی دشوارکننده انجام امور است؛ لذا تحقق و تداوم آن در گرو تصمیم‌ها و پیگیری‌های مدیریت سازمان در قبال اقدامات امنیت اطلاعات است. در نبود این پیگیری مداوم، نمی‌توان انتظار داشت که تمامی کارکنان، به طور یکپارچه و اثربخش، در چارچوب‌های امنیتی سازمان انجام وظیفه کنند.

از یک طرف بعید است که مدیران ارشد سازمان دغدغه‌های امنیتی نداشته باشند و از طرف دیگر، این مدیران نگران هزینه‌ها و چالش‌های ناشی از چارچوب‌های محدودکننده هستند؛ بنابراین مدیران به دنبال یک رویکرد بهینه هستند تا اقدامات امنیت اطلاعات را به اندازه کافی، مؤثر و مقرون‌به‌صرفه پیاده‌سازی و هدایت نمایند.

همه این اقدامات زمانی می‌تواند هدفمند، کافی و مقرون‌به‌صرفه باشد که سازمان بتواند متناسب با میزان مخاطره‌های امنیتی جاری، کیفیت و کمیت این اقدامات را اولیت‌بندی، برنامه‌ریزی و اجرا نماید. در نتیجه وجود یک فرایند مدیریت مخاطرات امنیتی متمرکز در سازمان می‌تواند به مدیران سازمان در مورد درستی و کفایت اقدامات امنیتی اطمینان خاطر دهد. بدین ترتیب مدیران ارشد با اطمینان خاطر بیشتری از اقدامات حمایت می‌کنند و می‌توانند روی یکپارچگی آنها نظارت و پیگیری بیشتری داشته باشند.

در برخی سازمان‌ها (در راستای مدیریت جامع اقدامات امنیت اطلاعات توسط مدیر ارشد و ارتقا و بهبود همواره امنیت اطلاعات متناسب با تغییرات در مخاطرات امنیتی) مدیران سازمان به دنبال استقرار سیستم مدیریت امنیت اطلاعات (ISMS) هستند. برخی سازمان‌ها نیز از سوی نهادهای حاکمیتی و مقررات صنفی ملزم شده‌اند که یک یا چند استاندارد امنیتی مانند استاندارد ISMS (ISO/IEC 27001) را در سازمان مستقر کنند. استقرار ISMS در سازمان، به مدیر سازمان کمک می‌کند تا ضمن پیاده‌سازی الزامات ISO/IEC 27001 و اخذ گواهینامه اعتبار ISMS، اطمینان حاصل کند که سایر الزامات حاکمیتی، مقررات صنفی و قراردادی مرتبط یا نامرتبط با امنیت اطلاعات در نظر گرفته شده است.

نقش کلیدی حمایت و رهبری مدیریت ارشد در استقرار و نگهداشت ISMS

شرکت افراتک در راستای ارتقای مدیریت امنیت اطلاعات در سازمان‌ها، خدماتی را در هر یک از حوزه‌های مطرح شده در فهرست ذیل ارائه می‌دهد:

- **مشاوره و ارائه راهکار برای استقرار سیستم مدیریت امنیت اطلاعات (ISMS) و اخذ گواهینامه استانداردهای بین‌المللی**
- **مشاوره در تدوین چارچوب مدیریت و ارزیابی مخاطرات امنیت اطلاعات**
- **مشاوره و ارائه راهکاردرجهت پیاده‌سازی الزامات شاپرک (مبتنی بر استاندارد PCI DSS) در شبکه پرداخت کشور**
- **مشاوره و ارائه راهکار درجهت پیاده‌سازی الزامات بالادستی در حوزه امنیت اطلاعات**

خدمات تخصصی تعمیرات تجهیزات

شرکت افراتک از سال‌ها تجربه راه‌اندازی، پیکربندی و راهبری تجهیزات ارتباطی شبکه و امنیت شبکه بخصوص محصولات شرکت‌های Juniper، HPE، F5، Cisco، Fortinet و ... برخوردار است. **شرکت افراتک** مفتخر است که توانسته با استعانت از این تجارب در کنار دانش و مهارت رفع ایرادات نرم‌افزاری و سخت‌افزاری، مجموعه‌ای از خدمات بی‌همتا و پرتقاضا را در خصوص تعمیرات و نگهداری تجهیزات ارتباطی ارائه دهد.

شرکت افراتک در زمینه تعمیرات تخصصی تجهیزات شبکه و امنیت شبکه خدمات ذیل را ارائه می‌دهد:

- مرتفع نمودن مشکلات مربوط به Raid Controller و پارتیشن‌بندی تجهیزات
- مرتفع نمودن مشکلات مربوط به فرایند Boot تجهیزات
- مرتفع نمودن مشکلات سخت‌افزاری اعم از برق‌رسانی منبع تغذیه (Power Supply)، برد اصلی تجهیزات و غیره
- رفع ایرادات نرم‌افزاری و ثابت‌افزارهای تجهیزات

خدمات آموزش

با عنایت به کمبود شـــدید نیروی متخصص در حوزه امنیت اطلاعات و نیاز مبرم سازمان‌ها، نهادها و شرکت‌ها بـــه نیروهای توانمند امنیت اطلاعات، **شـــرکت افراتک** با آگاهی از نیازمندی‌های کنونی کشـــور و بهره‌گیری از اساتید توانمند و صاحب‌نام در زمینه‌های مختلف امنیت اطلاعات، اقدام به ارائه خدمات آموزش، مشخصاً در حوزه امنیت اطلاعات نموده اســـت. این مجموعه آمادگی دارد دوره‌های آموزشی خود را به دو صورت حضوری و آنلاین ارائه نماید. همچنین مجموعه افراتک آمادگی خود را در جهت برگزاری دوره‌های آموزشـــی بر حسب نیاز ســـازمان‌ها و متناسب با سطوح مدیران عالی، مدیران فنی، کارمندان و کارشناسان فناوری، در درون آن سازمان‌ها اعلام می‌نماید.

دوره‌های آگاهی‌رسانی امنیتی

در ســـال‌های اخیـــر، تقریبـــاً از هر ۴ دفعه ای که نشـــت اطلاعات (Data Breach) در ســـازمانی رخ داده اســـت، در ۳ دفعه از آن، کارکنان سازمان به‌طور مستقیم یا غیرمستقیم دخیل بوده‌اند.

بهروش‌های امنیتی و اســـتانداردهای امنیتـــی نظیر ISMS، آموزش حـــوزه امنیت اطلاعـــات را برای همـــه کارکنان ســـازمان‌ها توصیه کرده‌اند.

دوره «آگاهی‌رسانی امنیتی» متناسب با مأموریت سازمان‌ها و نقش کارکنان تدوین و ارائه می‌شود.

دوره‌های عمومی امنیت اطلاعات

دوره‌های پایه امنیت اطلاعات

مانند دورهٔ SANS SEC301، CEH، Security+ و دوره‌های آشنایی با مقدمات و الزامات استقرار ISMS، و دوره‌های خاص امنیت برای بخش‌های مختلف؛

دوره‌های امنیت در زیرساخت‌های فناوری اطلاعات

مانـــند امن‌ســـازی سیســـتم‌عامل، امنیـــت زیرســـاخت مجازی‌ســـازی، CCNA Security؛

دوره‌های مهارتی امنیت اطلاعات

کارگاه‌هایی متناســـب با نیاز روز و تجارب کســـب شده جهت آموزش مهارت‌های کار با ابزار و تکنیک‌های امنیتی

دوره‌های مهارت فنی

مانـــند دوره‌های تخصصی تجهیـــزات Fortinet (NSE)، آمـــوزش فایروال Palo Alto و آمـــوزش راهبری مدیریـــت راهکار حفاظـــت و ضدبدافزار Kaspersky؛

کارگاه‌های کاربردی

آموزش مهارت‌هـــا و تجارب پیکربندی و رفع اشـــکال تجهیـــزات امنیتی (متناسب با نیاز سازمان‌ها)؛

مهارت‌های ارزیابی امنیتی

کارگاه آمـــوزش راهبری و ارزیابی به وســـیله ابزارهـــای ارزیابی همچون Nessus Professional و Acunetix؛

دوره‌های مهارتی فرایندی

این دوره‌ها برای کارشناسان حوزه امنیت اطلاعات و در حیطه دانش اجرای فرایندهـــا و اقدامات امنیت برگزار می‌شـــود؛ دوره‌های مرتبط با مدیریت حوادث امنیتی، کشف و پیگیری جرائم رایانه‌ای، مقابله با حملات مهندسی اجتماعی، تهدیدات درون‌ســـازمانی و تهدیدات سایبری از قبیل دوره‌های رسمی SANS SEC503، SANS SEC460 و SANS SEC542؛

دوره‌های ویژه

ایـــن دوره‌ها حول موضوعات خاص امنیت اطلاعات و فضای ســـایبری ارائه می‌شـــود؛ مانند دوره‌هـــای امنیت سیســـتم‌های کنترل صنعتـــی (ICS) و دوره‌های امنیت شبکه بانکی و پرداخت مانند PCI DSS و PCI PA-DSS؛

دوره‌های پیشرفته امنیت اطلاعات

- ارتقا سطح دانش تخصصی کارشناسان متخصص و مجرب در حوزه امنیت اطلاعات
- آمادگی برای آزمون‌های بین‌المللی

ارتقا دانش در زمینه مدیریت امنیت اطلاعات

برای کارشناســـان و مدیران فناوری اطلاعات، مدیـــران امنیت اطلاعات و همچنین ســـازمان‌هایی که اســـتقرار سیســـتم مدیریـــت امنیت اطلاعات (ISMS) را در برنامـــه دارند، دوره‌های کاربردی مدون و سفارشـــی ارائه می‌شود. دوره‌های مرتبط با اســـتقرار ISMS، دوره‌های مدیریت مخاطرات امنیتی، دوره‌های مرتبـــط با الگوها و چارچوب‌های فناوری اطلاعات همچون ITIL، CoBIT و DevSecOps نمونه‌ای از این دوره‌ها هستند؛

آمادگی برای آزمون‌های بین‌المللی

این دوره‌ها به صورت مشخص در راستای آمادگی متخصصین امنیت برای شـــرکت در دوره‌های جامع و معتبر امنیت ماننـــد CISM، CISSP و SSCP طراحی و ارائه می‌شود؛

ارائه بستر آزمون

همچنین نظر به اینکه به دلیل محدودیت‌های ناشـــی از تحریم‌های همه‌جانبه در حوزه‌های مختلف، هموطنان عزیزمان از شـــرکت در برخی از دوره‌ها و آزمون‌های بین‌المللی مرتبط به مهارت‌های فناوری اطلاعات محروم هستند، **شرکت افراتک** مفتخر است که توانسته بستری را فراهم سازد که هموطنان عزیزمان بتوانند بدون حضور در ســـایر کشـــورها، در آزمون‌های بین‌المللی خاص، همچون آزمون‌های تخصصـــی Fortinet NSE و Ciscoو غیره شرکت نمایند.

در کنار شما هستیم...

AFRATEC
afratec.ir
شرکت فنی مهندسی نوآوران افراتک هوشمند

به ما اعتماد کرده‌اند...

- سداد SADAD پرداخت الکترونیک سداد
- digikala
- شرکت تجارت الکترونیک پارسیان
- ملی کارت
- مرکز آمار ایران
- جمهوری اسلامی ایران وزارت بهداشت، درمان و آموزش پزشکی
- بانک خاورمیانه
- قوامین
- بانک توسعه تعاون
- قوه قضاییه جمهوری اسلامی ایران
- دانشگاه صنعتی شریف
- شرکت مجتمع گاز پارس جنوبی
- بانک سینا
- شرکت مخابرات استان یزد
- های وب HiWEB
- pars online
- های اول
- سازمان نقشه برداری کشور
- دانشگاه علوم پزشکی و خدمات بهداشتی درمانی تهران
- دانشگاه علوم پزشکی و خدمات بهداشتی درمانی شهرکرد
- برق منطقه ای فارس
- شرکت گاز استان آذربایجان شرقی
- دانشگاه فردوسی مشهد
- سازمان بهزیستی کشور اداره کل بهزیستی خراسان شمالی
- شرکت بهسازان ملت بانکداری نوین
- جمهوری اسلامی ایران وزارت ورزش و جوانان اداره کل ورزش و جوانان خراسان جنوبی
- منطقه ویژه اقتصادی ماهشهر
- شرکت سهامی آب منطقه‌ای ایلام
- (بانک ملی ایران) اداره امور شعب استان یزد
- موزه تاریخ طبیعی دانشگاه فردوسی مشهد

AFRATEC

afratec.ir

شرکت فنی مهندسی نوآوران افراتک هوشمند

ارتباط با ما

(۰۲۱) ۸۶۷۶۵۰۰۰

info@afratec.ir

www.afratec.ir

خیابان شـهید مطهری، خیابـان میرعماد،
روبروی سفارت هند، پلاک ۳۳، طبقه سوم

aparat.com/afratec

linkedin.com/afratec

youtube.com/afratec

instagram.com/afratec.ir