

روش ارزیابی و آیین نامه اختصاصی

متقاضیان دریافت پروانه فعالیت در

حوزه خدمات افتا

خدمات مدیریتی

خدمات مدیریتی افتا، خدماتی از جنس طراحی‌های کلان و ساختاری، طرح‌ریزی، برنامه‌ریزی، بهبود و ساماندهی، سنجش و پیگیری مخاطرات ایمنی در سازمان‌ها و تدوین نظام‌ها و سیاست‌های امنیتی است. خدمات مدیریتی افتا شامل ۲ گرایش مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات و ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات می‌باشد.

معرفی گرایش مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات:

هر فرآیندی که بر محوریت تجارت می‌باشد، در معرض تهدیدات امنیتی و نقض حریم خصوصی قرار دارد. فناوری‌های پیشرفته، تا حدود زیادی قادر به مقابله با حملات امنیت سایبری هستند، اما این‌ها کافی نیست؛ سازمان‌ها باید اطمینان حاصل کنند که فرآیندهای تجاری، سیاست‌ها و رفتار نیروی کار نیز می‌تواند این خطرات را به حداقل رسانده و یا کاهش دهد. در این راستا شرکت‌های متنوعی وجود داشته که در حیطه مشاوره و استقرار استانداردهای امنیت اطلاعات، اقدام به ارائه خدمات می‌نمایند. خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

❖ شرکت‌های فعال طراحی فرآیندها در حوزه امنیت اطلاعات و ارتباطات

❖ شرکت‌های فعال مشاوره طراحی و استقرار استانداردهای:

ISMS

OWASP

NIST

SANS

ENISA

ISO۲۷۰۰۱

ITIL

PCI DSS

COBIT

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

❖ توانایی تعیین سطح امنیتی مناسب برای محافظت از سازوکار و دارایی‌های سازمان‌ها

❖ توانایی تحلیل و مدیریت ریسک

❖ توانایی تدوین خط‌مشی، فرایندها و راهنماهای امنیتی

❖ تسلط بر استانداردهای مدیریت امنیت اطلاعات و مدیریت فناوری اطلاعات و تدوین کسب و کار و COBIT و ITIL

❖ آشنایی با استانداردهای ارزیابی امنیتی

❖ آشنایی با مدل‌های بلوغ امنیت اطلاعات

❖ توانمندی‌های عمومی مشاوره

شاخص	شرایط	امتیاز هر مورد	سقف امتیاز فرم
قراردادهای مرتبط در ۵ سال اخیر	به ازای هر قرارداد (پایان یافته)	۸	بدون سقف
	به ازای هر قرارداد (در حال اجرا)	۴	سقف
قرارداد در سایر حوزههای خدمات افتا در ۵ سال اخیر	به ازای هر قرارداد (پایان یافته)	۲	۸
سوابق شرکت در آن حوزه	به ازای هر سال سابقه مرتبط	۱	۵
گواهیههای شرکت گواهیههای مرتبط مانند ۲۷۰۰۱، ۲۰۰۰۰، شورای انفورماتیک در گرایش مرتبط و...	به ازای هر گواهی مرتبط	۳	۶
مدرک تحصیلی کارشناسان	لیسانس	۳	۲۴
	فوقلیسانس	۴	
	دکتر	۶	
گواهیههای آموزشی کارکنان	به ازای هر گواهی مرتبط	۳	۲۴
	به ازای هر گواهی در سایر حوزهها	۱	
تعداد کارشناسان همکار	به ازای هر کارشناس	۳	۹

رتبه بندی:

رتبه بندی: فرایندی است که برای یک نوع مقیاس گذاری جهت طبقه بندی شرکت های دارای پروانه فعالیت در حوزه خدمات مدیریتی افتا با گرایش «مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات» انجام می گیرد.

رتبه: طبقه امتیازی است بین اعداد ۱ الی ۳ که بر اساس شاخص های تعیین شده به شرکت های ارائه کننده خدمات «مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات» اختصاص داده می شود.

در حال حاضر فرایند رتبه بندی مخصوص شرکت های متقاضی دریافت پروانه در حوزه «خدمات مدیریتی افتا» با گرایش «مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات» میباشد.

✓ حداقل الزامات کسب رتبه ۱:

- معرفی و تایید حداقل ۶ نفر از کارشناسان ارائه خدمت آن شرکت
- دارا بودن بیش از یک قرارداد مرتبط در ۵ سال اخیر منتهی به درخواست.
- کسب امتیاز ۷۰ به بالا
- در صورت نیاز، تایید کارشناسان معرفی شده در فرایندهای ارزیابی فنی تکمیلی (مانند مصاحبه حضوری).

✓ حداقل الزامات کسب رتبه ۲:

- معرفی و تایید حداقل ۴ نفر از کارشناسان ارائه خدمت آن شرکت
- دارا بودن حداقل یک قرارداد مرتبط در ۵ سال اخیر منتهی به درخواست.
- کسب امتیاز ۳۰ الی ۷۰
- در صورت نیاز، تایید کارشناسان معرفی شده در فرایندهای ارزیابی فنی تکمیلی (مانند مصاحبه حضوری).

✓ حداقل الزامات کسب رتبه ۳:

- معرفی و تایید حداقل ۳ نفر از کارشناسان ارائه خدمت آن شرکت
- تایید کارشناسان معرفی شده در فرایندهای ارزیابی فنی تکمیلی (مانند مصاحبه حضوری).

معرفی گرایش ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات:

معیارها و استانداردهای امنیت اطلاعات و ارتباطات از اهمیت بسیاری برخوردارند و در حفاظت اطلاعات حساس و جلوگیری از حملات سایبری نقش کلیدی دارند. امنیت اطلاعات به معنای تضمین حفاظت از سهولت دسترسی، صحت، محرمانگی، امنیت و کیفیت اطلاعات است. در این راستا، انطباق با استانداردها و معیارهای امنیت اطلاعات و ارتباطات به معنای تطابق سازمان با استانداردها و نگرشهای مشخصی است که برای تضمین امنیت اطلاعات اتخاذ می‌شود.

در این راستا شرکت‌های متنوعی وجود داشته که در حیطه ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات، اقدام به ارائه خدمات می‌نمایند.

خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

- ❖ شرکت‌های فعال ممیزی کننده در حوزه امنیت اطلاعات
- ❖ شرکت‌های فعال انطباق سنج در حوزه امنیت اطلاعات
- ❖ این شرکت‌ها باید دارای یکی از شرایط زیر باشد:
- دارای مجوز صدور گواهینامه از سازمان ملی استاندارد ایران به عنوان C.B در scope امنیت اطلاعات باشد.
- دارای نامه نمایندگی از یک C.B خارجی در حوزه ممیزی و صدور گواهینامه که خود آن از طرف یک سازمان A.B در scope امنیت اطلاعات تایید صلاحیت شده باشد.

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

- ❖ مطابقت با چک‌لیست الزامات ممیزی و صدور گواهینامه
- ❖ مطابقت با استانداردهای الزامات مراکز گواهی در حوزه سیستم‌های مدیریتی فتا و افتا
- ❖ توانایی توسعه و پشتیبانی از یک طرح امنیتی برای هر سیستم و دارایی‌های تحت کنترل سازمان
- ❖ توانایی تحلیل و مدیریت ریسک
- ❖ تسلط بر خط‌مشی، فرایندها و راهنماهای امنیتی
- ❖ تسلط بر استانداردهای مدیریت امنیت اطلاعات، مدیریت فناوری اطلاعات و تدوam کسب و کار
- ❖ آشنایی با استانداردهای ارزیابی امنیتی
- ❖ آشنایی با مدل‌های بلوغ امنیت اطلاعات
- ❖ آشنایی با ISMS و استانداردهای سری ISO ۲۷۰۰۰

خدمات عملیاتی

خدمات عملیاتی افتا، بیشتر بر مهارت‌های خاص و یا فنی پرسنل برای پیاده‌سازی و یا حصول اطمینان از عملکرد مناسب کنترل‌های پیاده‌سازی شده تاکید دارد. گرایش‌های این حوزه شامل آزمون و ارزیابی امنیتی، پیاده‌سازی مرکز عملیات امنیت و تیم پاسخ به رخداد،

پایه‌سازی امنیت فیزیک و محیط پیرامونی، امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها، امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌های صنعتی و مسابقات کشف نقص امنیتی.

معرفی گرایش آزمون و ارزیابی امنیتی:

به عنوان یک جنبه مهم در زمینه امنیت اطلاعات و فناوری اطلاعات مطرح است. این گرایش به تست و ارزیابی امنیت سیستم‌ها، شبکه‌ها، و برنامه‌های کاربردی با هدف شناسایی ضعف‌ها و نقاط آسیب‌پذیری و همچنین ارائه پیشنهادات برای بهبود امنیت می‌پردازد. در این راستا شرکت‌های متنوعی وجود داشته که در حیطه آزمون و ارزیابی امنیتی، اقدام به ارائه خدمات می‌نمایند.

لازم به ذکر است شرکت‌های متقاضی جهت ارائه خدمت در این گرایش میتوانند یک یا کلیه ی زیر گرایش های ذیل را جهت فعالیت انتخاب نمایند ، بدیهی است درج عنوان زیر گرایش انتخابی در پروانه فعالیت ، منوط به کسب امتیاز قبولی حداقل سه کارشناس از کارشناسان معرفی شده در زیر گرایش مذکور است.

عناوین زیر گرایش‌ها:

۱. شبکه های کامپیوتری و ارتباطات بی سیم
۲. برنامه های کاربردی و سامانه های مبتنی بر وب
۳. سامانه ها و تجهیزات کنترل صنعتی

خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

- ❖ شرکت‌هایی که در حوزه‌ی ارزیابی سطح امنیت شبکه یا تست نفوذ فعالیت می‌کنند.
- ❖ شرکت‌هایی که شناسایی نقاط ضعف و آسیب‌پذیر شبکه یک سازمان را با انجام ارزیابی‌های فنی انجام داده و اقدام اصلاحی پیشنهاد می‌دهند.
- ❖ شرکت‌هایی که آزمون‌های شناسایی بدافزار و اقدامات ضد بدافزار انجام می‌دهند.

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

- ❖ آگاهی، دانش و تسلط کافی بر سیستم‌عامل‌ها، شبکه و پروتکل‌های شبکه، پایگاه داده و برنامه‌های کاربردی
- ❖ آگاهی، دانش و تسلط کافی بر سرویس‌های شبکه
- ❖ آشنایی با بدافزارها، حملات و آسیب‌پذیری‌ها و توانایی ارائه راه‌حل برای کاهش اثر/جلوگیری از آن‌ها
- ❖ آگاهی از مفاهیم مهندسی معکوس
- ❖ توانایی تحلیل و کشف آسیب‌پذیری
- ❖ توانایی ارزیابی و مدیریت آسیب‌پذیری
- ❖ آگاهی از مفاهیم فارتزیک سیستم
- ❖ آشنایی و توانایی کار با ابزارهای آزمون
- ❖ آشنایی و تسلط بر انواع متدلوژی‌های آزمون
- ❖ آگاهی در مورد استانداردهای مدیریت امنیت اطلاعات

تذکر: متقاضی در هیچ یک از گرایش‌های آزمایشگاه دارای پروانه فعال نباشد.

نحوه امتیازدهی در حوزه عملیاتی

شاخص	شرایط	امتیاز هر مورد	سقف امتیاز فرم
------	-------	----------------	----------------

۳۰	۶	به ازای هر قرارداد (پایان یافته)	قراردادهای مرتبط در ۵ سال اخیر
	۳	به ازای هر قرارداد (در حال اجرا)	
۸	۲	به ازای هر قرارداد (پایان یافته)	قرارداد در سایر حوزههای افتا در ۵ سال اخیر
۲۴	۳	لیسانس	مدرک تحصیلی کارشناسان
	۴	فوقلیسانس	
	۶	دکتر	
۵	۱	به ازای هر سال سابقه مرتبط	سوابق شرکت در آن حوزه
۶	۳	به ازای هر گواهی مرتبط	گواهیهای شرکت
۲۴	۳	به ازای هر گواهی مرتبط	گواهیهای آموزشی کارکنان
	۱	به ازای هر گواهی در سایر حوزههای افتا	
۶	۲	استفاده از ابزار و یا نرمافزار مرتبط به (ازای هر مورد)	تجهیزات/ فضا
۱۸	۲	به ازای هر سال	سوابق مرتبط کارشناسان
۹	۳	به ازای هر کارشناس	تعداد کارشناسان همکار

معرفی گرایش پیادهسازی مرکز عملیات امنیت و تیم پاسخ به رخداد:

اجزای اساسی در استراتژی امنیت سازمانها محسوب می شود. این گرایشها به منظور ایجاد یک ساختار سازمانی قوی برای شناسایی، پیشگیری، تشخیص، و پاسخ به حوادث امنیتی ایجاد شده اند. در این راستا شرکت های متنوعی وجود داشته که در حیطه پیاده سازی مرکز عملیات امنیت و تشکیل تیم پاسخ به رخداد، اقدام به ارائه خدمات می نمایند.

خدمات ارائه شده این نوع شرکتها عبارت است از:

❖ شرکت های ارائه دهنده خدمات زیر:

پیاده سازی مرکز عملیات امنیت

طراحی مرکز عملیات امنیت و پاسخ به رخداد

پیاده سازی مرکز مدیریت امداد و هماهنگی عملیات رخداد های رایانه ای

پیاده سازی مرکز مدیریت امداد و هماهنگی عملیات رخداد های امنیتی

داشبورد سازی رخداد های امنیتی

پیاده سازی سامانه های SANSBOX، هانی پات، PAM، DAM، XDR، EDR، Full Packet Capture، AAA، DLP

خود کار سازی فرآیندهای SOC

نصب و پشتیبانی SIEM

مهارت ها و قابلیت های لازم برای ارائه این خدمات عبارت اند از:

❖ توانایی برنامه ریزی توسعه و مدیریت رخداد

❖ تسلط بر انواع حملات شبکه بی سیم و باسیم

- ❖ آگاهی از مفاهیم فارتزیک سیستم و شبکه
- ❖ توانایی به روزرسانی و مدیریت رویه های مدیریت رخداد (با توسعه ابزارها و تکنیک ها)
- ❖ تسلط بر مفاهیم و معماری شبکه
- ❖ تسلط در زمینه امنیت شبکه، سیستم عامل، پایگاه داده و برنامه های کاربردی
- ❖ تسلط بر پیکربندی تجهیزات شبکه
- ❖ توانایی پیکربندی امن تجهیزات نرم افزاری و سخت افزاری
- ❖ آزمون و به روزرسانی رویه های مدیریت رخداد
- ❖ تهیه طرح تداوم کسب و کار
- ❖ تهیه طرح بازیابی از فاجعه
- ❖ نحوه شناسایی و اشراف بر داراییهای مطالعاتی
- ❖ مدیریت آسیب پذیریها و مخاطرات سایبری
- ❖ مدیریت دسترسی به منابع سازمان
- ❖ فرایند شکار تهدیدات (Threat Hunting)

تذکر: متقاضی در هیچ یک از گرایش های آزمایشگاه دارای پروانه فعال نباشد.

معرفی گرایش پیاده سازی امنیت فیزیکی و محیط پیرامونی:

گرایش پیاده سازی امنیت فیزیکی و محیط پیرامونی به ایجاد سیاست ها و اقداماتی متناسب با حفاظت از جنبه های فیزیکی و محیطی سازمان می پردازد. این گرایش با هدف حفاظت از منابع، دارایی ها، و افراد در محیط فیزیکی سازمان ایجاد شده است. در این راستا شرکت های متنوعی وجود داشته که در به پیاده سازی امنیت فیزیکی و محیط پیرامونی، اقدام به ارائه خدمات می نمایند.

لازم به ذکر است شرکت های متقاضی جهت ارائه خدمت در این گرایش میتوانند یک یا کلیه ی زیر گرایش های ذیل را جهت فعالیت انتخاب نمایند، بدیهی است درج عنوان زیر گرایش انتخابی در پروانه فعالیت، منوط به کسب امتیاز قبولی حداقل سه کارشناس از کارشناسان معرفی شده در زیر گرایش مذکور است.

عناوین زیر گرایش ها :

۱. نظارت تصویری
۲. تشخیص و اطفاء حریق
۳. کنترل دسترسی فیزیکی
۴. تامین پایدار انرژی

خدمات ارائه شده این نوع شرکت ها عبارت است از:

- ❖ شرکت های ارائه دهنده ی خدمات و محصولات زیر:
- نصب و راه اندازی، پشتیبانی و تعمیرات دوربین های تحت شبکه IP دوربین ها
- نصب و راه اندازی، پشتیبانی و تعمیرات سیستم های اعلام و اطفاء حریق

نصب و راه اندازی، پشتیبانی و تعمیرات گیت هوشمند و تجهیزات کنترل تردد
نصب و راه اندازی، پشتیبانی و تعمیرات تأمین کننده ی برق (ژنراتور)
نصب و راه اندازی، پشتیبانی و تعمیرات سنسورهای دما و رطوبت
نصب و راه اندازی، پشتیبانی و تعمیرات سیستم های تهویه مطبوع (cooling)
شرکت های فعال انطباق سنج در حوزه امنیت اطلاعات

مهارت ها و قابلیت های لازم برای ارائه این خدمات عبارت اند از:

- ❖ تسلط بر مکانیزم های فیزیکی کنترل دسترسی
- ❖ تسلط بر ایمن سازی محیطی برای حوزه فناوری اطلاعات
- ❖ تسلط بر مکانیزم ها و راه حل های امنیت محیط پیرامونی
- ❖ آشنایی با تجهیزات امنیت محیط پیرامونی
- ❖ تسلط بر راه حل های تامین مطمئن برق
- ❖ ارزیابی امنیت فیزیکی
- ❖ تسلط بر استانداردهای مرتبط با پیاده سازی و تامین امنیت فیزیکی و محیط پیرامونی

معرفی گرایش امن سازی و مقاوم سازی سامانه ها، زیرساخت ها و سرویس ها:

گرایش امن سازی و مقاوم سازی سامانه ها، زیرساخت ها و سرویس ها به ایجاد و اجرای سیاست ها، تدابیر و فناوری های امنیتی با هدف کاهش آسیب پذیری ها، حفاظت از اطلاعات و خدمات، و حفظ پایداری و عملکرد سیستم ها می پردازد. در این راستا شرکت های متنوعی وجود داشته که در به امن سازی و مقاوم سازی سامانه ها، زیرساخت ها و سرویس ها، اقدام به ارائه خدمات می نمایند.

خدمات ارائه شده این نوع شرکت ها عبارت است از:

- ❖ طراحی و اجرای کلیه اقدامات برای افزایش امنیت و مقاوم سازی شامل:
پیکره بندی امن (اجرای تنظیمات امنیتی برای زیرساخت و سیستم ها)
- ❖ راه اندازی سیستم های PAM, AAA, DLP, IPS/IDS, WAF, UTM, Firewall
- ❖ طراحی شبکه و زیرساخت، Zone بندی ها و محل قرارگیری تجهیزات امنیتی در توپولوژی هم بندی به درستی و طبق معماری های رایج و استاندارد
- ❖ اعمال Based-line Policy ها بر روی سرورها و دامین
- ❖ اعمال Firewall Rule
- ❖ نصب آنتی ویروس های مناسب
- ❖ اعمال پروسه های Endpoint Protection
- ❖ اعمال صحیح پروسه Vulnerability Assessment
- ❖ جداسازی شبکه LAN از شبکه Internet
- ❖ رمزنگاری داده ها با هدف حفظ اطلاعات حساس حین انتقال و ذخیره سازی

- ❖ امن سازی و پشتیبانی شبکه های IOT و دیسپاچینگ
- ❖ انجام اقدامات پیشگیرانه امن سازی (Penetration Testing , Threat Hunting , Device Audit)

مهارت ها و قابلیت های لازم برای ارائه این خدمات عبارت اند از:

- ❖ تسلط بر مفاهیم و معماری شبکه
- ❖ تسلط بر راهبری و پیکربندی تجهیزات شبکه
- ❖ تسلط بر امن سازی و مقاوم سازی سیستم ها، سرورها و شبکه
- ❖ آشنایی با انواع پروتکل های امن و رمزنگاری
- ❖ تسلط بر راه حل های مرتبط با تداوم کسب و کار در فناوری اطلاعات
- ❖ تسلط بر مجازی سازی و رایان ابری
- ❖ ارزیابی و مدیریت ریسک و آسیب پذیری ها
- ❖ آشنایی با انواع پروتکل های امن و رمزنگاری
- ❖ آگاهی از استانداردهای مدیریت فناوری اطلاعات و مدیریت امنیت فناوری اطلاعات

تذکر: متقاضی در هیچ یک از گرایش های آزمایشگاه دارای پروانه فعال نباشد.

معرفی گرایش راهبری مرکز عملیات و تیم پاسخ به رخداد:

گرایش راهبری مرکز عملیات امنیت (SOC) و تیم پاسخ به رخداد (CSIRT) به مدیریت و هدایت این دو اجزای مهم در زمینه امنیت اطلاعات و فناوری اطلاعات اشاره دارد. این گرایش به تدبیرها و استراتژی هایی متمرکز است که بر اساس هوش تجاری، تصمیم گیری موثر، و تدابیر بهینه در زمینه های SOC و IRT صورت می گیرد. در این راستا شرکت های متنوعی وجود داشته در گرایش راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد ، اقدام به ارائه خدمات می نمایند. خدمات ارائه شده این نوع شرکت ها عبارت است از:

- ❖ مدیریت و راهبرد رخداد های امنیتی
- ❖ پیاده سازی فرآیندهای پاسخ به رخداد های امنیتی
- ❖ پیاده سازی استراتژی امنیتی
- ❖ ایجاد پروفایل و تعیین سطح بلوغ امنیتی
- ❖ تدوین برنامه عملیاتی امن سازی

مهارت ها و قابلیت های لازم برای ارائه این خدمات عبارت اند از:

- ❖ آشنایی با ابزارهای پای ترافیک و رکوردهای ثبت شده
- ❖ تسلط کافی بر انواع حملات شبکه بیسیم و باسیم
- ❖ آشنایی با اقدامات فارتزیک سیستم و شبکه
- ❖ توانایی پشتیبان گیری و بازیابی داده ها
- ❖ توانایی به روز رسانی و مدیریت رویه های مدیریت رخداد (راهبری رویه ها)
- ❖ تسلط کافی بر مفاهیم و معماری شبکه
- ❖ تسلط کافی در زمینه امنیت شبکه، سیستم عامل، پایگاه داده و برنامه های سیستمی

- ❖ تسلط فنی بر استفاده از تجهیزات شبکه
- ❖ تست نفوذ (Penetration Test)
- ❖ آشنایی با وظایف تیم قرمز (RedTeam)
- ❖ آشنایی با وظایف Blue team
- ❖ آشنایی با مباحث شکار تهدیدات (Threat Hunting)
- ❖ مدیریت آسیب پذیریها و مخاطرات سایبری
- ❖ مدیریت دسترسی به منابع سازمان
- ❖ پیکربندی تجهیزات و سامانه ها
- ❖ امنیت شبکه و سامانه ها
- ❖ پایش و مدیریت لاگها
- ❖ تداوم و پایداری سرویس ها
- ❖ اقدامات زمان بحران
- ❖ اقدامات پس از بحران

تذکر: متقاضی در هیچ یک از گرایش های آزمایشگاه دارای پروانه فعال نباشد.

معرفی گرایش مسابقات کشف نقص امنیتی:

گرایش مسابقات کشف نقص امنیتی (Security Capture The Flag - CTF) یک شاخه مهم در زمینه امنیت اطلاعات است که به صورت یک مسابقه یا چالش برگزار می شود. در این نوع مسابقات، شرکت کنندگان با رقابت در مسائل و چالش های مختلف امنیتی، مهارت ها و توانایی های خود را در زمینه کشف نقص های امنیتی و مقابله با حملات سایبری به اثبات می کنند. در این راستا شرکت های متنوعی وجود داشته در گرایش مسابقات کشف نقص امنیتی، اقدام به ارائه خدمات می نمایند. خدمات ارائه شده این نوع شرکت ها عبارت است از:

- ❖ شرکت های برگزار کننده ی مسابقات کشف نقص امنیتی (در شبکه، سامانه ها، سرویس ها، نرم افزارها و...) و مسابقات تست های نفوذ
- ❖ این شرکتها باید تمامی مهارتهای گرایش آزمون امنیتی سایبری و شبکه را دارا باشند.
- ❖ باگ باونتی
- ❖ شرکت هایی که در حوزه ی ارزیابی سطح امنیت شبکه یا تست نفوذ فعالیت می کنند.
- ❖ شرکت هایی که شناسایی نقاط ضعف و آسیب پذیر شبکه یک سازمان را با انجام ارزیابی های فنی انجام داده و اقدام اصلاحی پیشنهاد می دهند.
- ❖ شرکت هایی که آزمون های شناسایی بدافزار و اقدامات ضد بدافزار انجام می دهند.

مهارت ها و قابلیت های لازم برای ارائه این خدمات عبارت اند از:

- ❖ آگاهی، دانش و تسلط کافی بر سیستم عامل ها، شبکه و پروتکل های شبکه، پایگاه داده و برنامه های کاربردی
- ❖ آگاهی، دانش و تسلط کافی بر سرویس های شبکه
- ❖ آشنایی با بدافزارها، حملات و آسیب پذیری ها و توانایی ارائه راه حل برای کاهش اثر/جلوگیری از آنها

- ❖ آگاهی از مفاهیم مهندسی معکوس
- ❖ توانایی تحلیل و کشف آسیب پذیری
- ❖ توانایی ارزیابی و مدیریت آسیب پذیری
- ❖ آگاهی از مفاهیم فارتزیک سیستم
- ❖ آشنایی و توانایی کار با ابزارهای آزمون
- ❖ آشنایی و تسلط بر انواع متدلوژی‌های آزمون
- ❖ آگاهی در مورد استانداردهای مدیریت امنیت اطلاعات

تذکر: متقاضی در هیچ یک از گرایش‌های آزمایشگاه دارای پروانه فعال نباشد.

معرفی گرایش امن‌سازی و مقاومت‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌های صنعتی :

گرایش امن‌سازی و مقاومت‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌های صنعتی به مدیریت امنیتی در محیط‌های صنعتی متمرکز است. این گرایش بر افزایش امنیت سیستم‌ها، حفاظت از داده‌ها و فرآیندها، و ایجاد مقاومت در برابر حملات سایبری تأکید دارد. در این راستا شرکت‌های متنوعی وجود داشته در گرایش امنیت و مقاومت در سامانه‌ها، زیرساخت‌ها، و سرویس‌ها صنعتی، اقدام به ارائه خدمات می‌نمایند. خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

- ❖ طراحی و اجرای کلیه اقدامات برای افزایش امنیت و مقاومت‌سازی در حوزه‌ی صنعتی شامل:
- ❖ استحکام‌بخشی سیستم عامل‌ها و سرویس‌های شبکه صنعتی
- ❖ ارزیابی آسیب پذیری‌ها و مدیریت مخاطرات امنیتی شبکه‌ها و سیستم‌های کنترل صنعتی
- ❖ امن‌سازی سیستم‌ها و تجهیزات کنترلی و ارتباطی شبکه صنعتی
- ❖ ایمن‌سازی پایگاه‌های داده و محیط‌های ذخیره و پردازش اطلاعات سیستم‌های کنترل صنعتی
- ❖ ایمن‌سازی پروتکل‌های ارتباطی شبکه صنعتی
- ❖ ارائه راه حل‌های معماری امن شبکه‌های صنعتی
- ❖ تدوین نقشه راه امنیتی در زیرساخت‌های حیاتی کشور و شبکه‌های صنعتی
- ❖ امن‌سازی داده‌های انتقالی در سیستم‌های کنترل صنعتی
- ❖ ناحیه‌بندی امن و جداسازی منطقی و فیزیکی شبکه‌های کنترل صنعتی
- ❖ راه‌اندازی تجهیزات امنیتی در شبکه‌های صنعتی
- ❖ مشاوره، اجرا و ممیزی استانداردهای امنیتی سیستم‌های کنترل صنعتی
- ❖ راه‌اندازی مراکز گوهر و تیم‌های پاسخگویی به حوادث امنیتی در شبکه‌های صنعتی
- ❖ ارائه سازوکارهای کنترل دسترسی و مدیریت کاربران در شبکه‌های صنعتی
- ❖ تدوین خط‌مشی‌ها، دستورالعمل‌ها، روش‌های اجرایی و مستندات امنیتی در شبکه‌های صنعتی
- ❖ ارائه راهکارهای مسیریابی امن در شبکه‌های صنعتی و امن‌سازی ارتباطات بیرونی شبکه سیستم‌های کنترلی

- ❖ تدوین توافق نامه های امنیتی شخص سوم در شبکه های صنعتی
- ❖ اجرای آزمون نفوذپذیری مختص به سیستم های کنترل صنعتی
- ❖ مدیریت وصله های امنیتی سیستم های کنترل صنعتی
- ❖ تدوین طرح های مقابله با بدافزار، تداوم کسب و کار و بازیابی از فاجعه در سیستم های کنترل صنعتی
- ❖ ارائه راه حل های امن سازی فیزیکی سیستم های کنترل صنعتی
- ❖ آموزش امنیتی مدیران، کارشناسان و کاربران شبکه های صنعتی
- ❖ پیکربندی امن (اجرای تنظیمات امنیتی برای زیرساخت و سیستم ها) در حوزه صنعتی
- ❖ رمزنگاری داده ها با هدف حفظ اطلاعات حساس حین انتقال و ذخیره سازی در حوزه صنعتی
- ❖ امن سازی و پشتیبانی شبکه های IIOT , ISC , SCADA , DCS , PLC و دیسپاچینگ در حوزه صنعتی

مهارت ها و قابلیت های لازم برای ارائه این خدمات عبارت اند از:

- ❖ تسلط بر مفاهیم و معماری شبکه
- ❖ تسلط بر راهبری و پیکربندی تجهیزات شبکه
- ❖ تسلط بر امن سازی و مقاوم سازی سیستم ها، سرورها و شبکه
- ❖ آشنایی با انواع پروتکل های امن و رمزنگاری
- ❖ تسلط بر راه حل های مرتبط با تداوم کسب و کار در فناوری اطلاعات
- ❖ تسلط بر مجازی سازی و رایانش ابری
- ❖ بررسی و شناخت SIEM صنعتی و نحوه استفاده از آن در یک سیستم کنترل صنعتی
- ❖ ارزیابی و مدیریت ریسک و آسیب پذیری ها
- ❖ آشنایی با انواع پروتکل های امن و رمزنگاری
- ❖ آگاهی از استانداردهای مدیریت فناوری اطلاعات و مدیریت امنیت فناوری اطلاعات

خدمات فنی

خدمات فنی افتا، شامل پیکربندی امن و پشتیبانی امنیتی محصول فتا می باشد و متقاضیان در این حوزه میبایست برای محصول مورد نظر **گواهی ارزیابی امنیتی** دریافت کرده باشند. شایان ذکر است با توجه به درخواست متقاضی، عنوان محصول مورد تایید در پروانه فعالیت صادر شده در این گرایش ذکر میشود.

معرفی گرایش نصب و پشتیبانی محصولات فتا:

گرایش نصب و پشتیبانی محصولات فضای تولید و تبادل اطلاعات به مدیریت فرایند نصب، پیکربندی، و پشتیبانی از محصولات و سامانه های مرتبط با فضای تولید و تبادل اطلاعات اختصاص دارد. این گرایش تأکید بر ارائه خدمات پس از فروش، ایجاد فرآیندهای نصب و پیکربندی مؤثر، و ارتقاء پایداری و عملکرد محصولات دارد. در این راستا شرکت های متنوعی وجود داشته گرایش نصب و پشتیبانی محصولات فتا، اقدام به ارائه خدمات می نمایند. خدمات ارائه شده این نوع شرکت ها عبارت است از:

- ❖ آموزش استفاده و چگونگی راهبری استفاده از محصول
- ❖ شرکت های فعال در زمینه ی فروش، موارد زیر:
- ❖ سخت افزار شبکه (server-storage-switch-Router-access point-UTM-dispatching) مازول شبکه

❖ نرم افزارهای کاربردی (سامانه های تحت وب)

مهارت ها و قابلیت های لازم برای ارائه این خدمات عبارت اند از:

- ❖ تسلط فنی متقاضی بر پیکربندی امن محصول
- ❖ تسلط فنی متقاضی در پشتیبانی امن محصول
- ❖ تسلط فنی متقاضی بر روش های مختلف استفاده از محصول
- ❖ صلاحیت فرایندی و اعتباری پشتیبانی از محصول (تعامل متقاضی با شرکت تولیدکننده محصول)
- ❖ پیکربندی امن محصول
- ❖ پشتیبانی امن محصول
- ❖ روش های مختلف استفاده از محصول
- ❖ چگونگی و نحوه تعامل متقاضی با شرکت تولیدکننده محصول
- ❖ آشنایی با موافقت نامه سطح خدمات (SLA)

متقاضیان اخذ مجوز در گرایش « نصب و پشتیبانی محصولا فتا»، از ارزیابی فنی (مصاحبه و آزمون) معاف بوده و درخواست آنان پس از تکمیل مدارک در سامانه ارزیابی و صدور پروانه و ارزیابی اولیه توسط سازمان، مستقیماً جهت ارزیابی اعتباری به مرکز مدیریت راهبردی افتا ارسال شده و صدور مجوز، در صورت اخذ تاییدیه از مرکز یاد شده، انجام خواهد شد.

متقاضیان اخذ مجوز در گرایش « نصب و پشتیبانی محصولا فتا»، از ارزیابی فنی (مصاحبه و آزمون) معاف بوده و درخواست آنان پس از تکمیل مدارک در سامانه ارزیابی و صدور پروانه و ارزیابی اولیه توسط سازمان، مستقیماً جهت ارزیابی اعتباری به مرکز مدیریت راهبردی افتا ارسال شده و صدور مجوز، در صورت اخذ تاییدیه از مرکز یاد شده، انجام خواهد شد.

تذکر:

متقاضیان دریافت پروانه فعالیت در حوزه خدمات فنی در «گرایش نصب و پشتیبانی محصولات فتا»، در صورت دارا بودن یکی از شرایط ذیل، مشمول «تمدید» پروانه پیشین و یا «صدور» پروانه جدید در این گرایش می-باشند.

۱ - شرکتهای تولیدکننده محصول بومی (داخلی) هستند، می بایست ابتدا «گواهی امنیتی محصول» مورد نظر خود را اخذ کرده و پس از آن نسبت به ثبت درخواست مجوز فعالیت در حوزه خدمات نصب و پشتیبانی آن محصول اقدام نمایند..

تبصره: متقاضیانی که حداقل یک بار موفق به اخذ گواهی امنیتی محصول شده اند، در صورت انقضای گواهی امنیتی، در صورتی حائز شرایط دریافت مجوز فعالیت در گرایش نصب و پشتیبانی محصولات فتا می باشند که محصول مورد درخواست جهت نصب و پشتیبانی، در مرحله تمدید گواهی و در وضعیت ارزیابی در آزمایشگاه مورد تایید سازمان فناوری اطلاعات ایران باشد. این شرکتها لازم است جهت استعلام وضعیت محصول، ابتدا نسبت به ارسال نامه کتبی (مطابق نمونه نامه محصولات بومی) به اداره کل توسعه صنعت افتا سازمان فناوری اطلاعات اقدام نمایند و در صورت مثبت بودن نتیجه استعلام و تایید یکی از وضعیت های: درحال ارزیابی، اتمام ارزیابی و یا ارسال گزارش به افتا، در پاسخ کتبی دریافت شده از اداره کل توسعه صنعت افتا، پاسخ مذکور را به عنوان گواهی ارزیابی امنیتی محصول، در سامانه ارزیابی و صدور پروانه خدمات امنیتی بارگذاری نمایند.

• لازم به ذکر است انعقاد قرارداد با آزمایشگاه، تحویل مستندات و نصب محصول در آزمایشگاه، از الزامات شروع فرآیند ارزیابی

محصول در آزمایشگاه است و لذا شرکت های متقاضی تمدید گواهی امنیتی محصول، پس از طی مراحل یاد شده، میتوانند جهت استعلام وضعیت محصول خود، با اداره کل توسعه صنعت افتا سازمان فناوری اطلاعات مکاتبه نمایند.

۲- شرکت هایی که درخواست پروانه فعالیت در حوزه خدمات فنی امنیتی با گرایش نصب و پشتیبانی محصولات فتا، در زمینه فروش تجهیزات (غیررادیویی، اکتیو و تحت شبکه اعم از سوئیچ شبکه، روتر، سرور، ذخیره ساز) را دارند، می بایست نسبت به تکمیل مشخصات محصول وارداتی خود به شرح جدول مندرج در نمونه نامه ای که در اطلاعیه شماره ۲ پروتال امنیت به نشانی sec.ito.gov.ir اقدام نماید. نامه ارسال شده از سوی شرکت لازم است در سربرگ شرکت و با مهر و امضای مدیر عامل و یا یکی از افراد دارای حق امضا ارسال شده و حاوی شماره تماس و آدرس شرکت باشد، تصویر نامه مذکور را به عنوان تاییدیه امنیتی محصول در سامانه ارزیابی بارگذاری و اصل آن را هنگام دریافت پروانه به صورت فیزیکی همراه تعهدنامه تحویل نمایند.

۳- به محصولاتی که به سفارش یک مشتری دولتی و فقط برای استفاده آن مشتری تولید می شوند و قابل عرضه ی عام نیستند، اصطلاحاً ((محصول خاص منظوره)) اطلاق میشود. برای محصولاتی با این ماهیت، در قدم اول بهره بردار سامانه (مشتری دولتی) و در غیر این صورت پیمانکار، می بایست به منظور دریافت ((پروانه بهره برداری)) با مرکز مدیریت راهبردی افتا مکاتبه نمایند.

نحوه امتیازدهی در حوزه فنی

شاخص	شرایط	امتیاز هر مورد	سقف امتیاز فرم
قراردادهای مرتبط در ۵ سال اخیر	به ازای هر قرارداد (پایان یافته)	۶	۳۰
	به ازای هر قرارداد (در حال اجرا)	۳	
قرارداد در سایر حوزههای افتا در ۵ سال اخیر	به ازای هر قرارداد (پایان یافته)	۲	۸
مدرک تحصیلی کارشناسان	لیسانس	۳	۲۴
	فوقلیسانس	۴	
	دکتر	۶	
سوابق شرکت در آن حوزه	به ازای هر سال سابقه مرتبط	۱	۵
گواهیهای شرکت	به ازای هر گواهی مرتبط	۳	۶
گواهیهای آموزشی کارکنان	به ازای هر گواهی مرتبط	۳	۲۴
	به ازای هر گواهی در سایر حوزههای افتا	۱	
تجهیزات/ فضا	استفاده از ابزار و یا نرمافزار مرتبط به (ازای هر مورد)	۲	۶
سوابق مرتبط کارشناسان	به ازای هر سال	۲	۱۸
تعداد کارشناسان همکار	به ازای هر کارشناس	۳	۹

خدمات آموزشی

این حوزه خدمات شامل ارائه آموزش کلیه دوره‌های امنیتی در سطوح و موضوعات مختلف به متقاضیان است. تذکر: دامنه این حوزه مربوط به آموزش‌هایی می‌باشد که منجر به دریافت گواهینامه‌های ملی و بین‌المللی در زمینه دوره‌های آموزشی امنیت اطلاعات و ارتباطات گردد.

معرفی گرایش آموزش امنیت فضای تولید و تبادل اطلاعات:

گرایش آموزش در حوزه امنیت فضای تولید و تبادل اطلاعات به توسعه و ارتقاء دانش و مهارت‌های کارشناسان و فراهم کردن محیطی اطلاعاتی امن در سازمان‌ها متمرکز است. این گرایش به مواردی از جمله آموزش تیم‌های امنیت، ایجاد دوره‌های آموزشی تخصصی، ترویج فرهنگ امنیت اطلاعات، و ایجاد زیرساخت‌های آموزشی متناسب با نیازهای حوزه امنیتی پرداخته و در این زمینه به تربیت نیروهای متخصص و مسئولان امنیت کمک می‌کند. در این راستا شرکت‌های متنوعی وجود داشته گرایش آموزش افتا، اقدام به ارائه خدمات می‌نمایند.. خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

❖ برگزاری دوره‌های آموزشی در حوزه‌های فضای تولید یا تبادل اطلاعات مشتمل بر شبکه، IP، امنیت، سیستم‌های عامل،

دیتابیس و استانداردهای مرتبط

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

❖ آشنایی با مدیریت کیفیت خدمات آموزش

❖ آشنایی با مدیریت موثر آموزش

❖ آشنایی با الزامات استانداردهای آموزش و مدیریت امنیت

❖ توانایی ارائه محصولات کمک آموزشی و راه‌اندازی کارگاه آموزشی و برگزاری سمینارهای تخصصی

❖ تسلط فنی بر دوره‌های آموزشی از قبیل امنیت سیستم‌عامل، شبکه، پایگاه داده، برنامه‌های کاربردی،

❖ بدافزار، استانداردهای امنیتی

❖ آگاهی از مستندات SP NIST ۱۶-۸۰۰ و SP NIST ۵۰-۸۰۰ و استانداردهای سری ISO ۲۷۰۰۰ و دیگر مستندات و استانداردهای مربوطه

داشتن مجوز استاندارد مبنی بر ارائه خدمات آموزش

نحوه امتیازدهی در حوزه خدمات آموزشی

شاخص	شرایط	امتیاز هر مورد	سقف امتیاز فرم
دوره‌های آموزشی برگزار شده در شرکت/موسسه در حوزه افتا در ۵ سال اخیر	به ازای هر دوره پایانیافته	۶	۶۰
مدرک تحصیلی مدرسین	لیسانس	۳	۲۴
	فوق‌لیسانس	۴	
	دکتر	۶	
سوابق شرکت/موسسه در آن حوزه	به ازای هر سال سابقه مرتبط	۱	۵

۶	۳	به ازای هر گواهی مرتبط	گواهیهای شرکت/موسسه
۳۰	۳	به ازای هر گواهی افتا	گواهیهای آموزشی مدرسين
۶۰	۱۵	به ازای هر کلاس	فضای آموزشی
۱۵	۵	به ازای هر مورد	تجهيزات
۳۰	۵	به ازای هر دوره	سابقه تدریس مرتبط مدرسان در ۵ سال اخیر (در سایر موسسات/شرکت آموزشی)

معرفی تجهیزات و دوره‌های آموزشی کارشناسان مربوط به هر گرایش:

ردیف	نام حوزه	نام گرایش	دوره‌های عمومی	دوره‌های تخصصی	تجهیزات سخت افزاری و نرم افزاری
۱	خدمات مدیریتی	مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات	✓ دوره‌های NIST : CSF RMF SP ✓ دوره‌های ENISA ✓ گواهینامه CISA ✓ گواهینامه CISSP ✓ گواهینامه Security + ✓ دوره‌های آشنایی با مفاهیم: استانداردهای امنیت مدیریت فرآیند ✓ دوره‌های SANS: GSEC GCIH GCFA GWAPT GCIR GCIA GCED MGT۵۱۲ ✓ دوره‌های مدیریتی ✓ دوره‌های COBIT ✓ دوره ممیزی داخلی	CompTIA Security Plus (CSCU) Certified Secure Computer User Certified Information Security Manager (CISM) Information Security Management System (ISMS) (ISO ۲۷۰۰۱) Certified Information Systems Security Professional (CISSP) استانداردهای COBIT, ITIL, CIS , benchmark استاندارد ۵۳-۸۰۰ NIST SP ۵۶۶ SANS-SEC ,	✓ ندارد

✓ ندارد	Certified Information Systems Auditor (CISA) Information Security Management System (ISMS) (ISO۲۷۰۰۱), Certified Information Systems Security Professional (CISSP) استانداردهای COBIT, ITIL, CIS, benchmark استاندارد NIST SP ۸۰۰-۵۳	✓ دوره‌های NIST ✓ دوره‌های ENISA ✓ گواهینامه CISA ✓ گواهینامه CISSP ✓ دوره‌های SANS ✓ گواهینامه Security + ✓ گواهینامه‌های سیسکو ✓ گواهینامه سرمیزی IATF ✓ گواهینامه سرمیزی NACI استاندارد ISO۱۹۰۱۱	ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات	۲
✓ لایسنس Nessus ✓ لایسنس Acunetix ✓ لایسنس XDR ✓ لایسنس PRTG ✓ و ...	SANS-SEC ۵۰۴ SANS-SEC ۵۶۰, SANS-SEC ۵۴۲ Certified Ethical Hacker (CEH) SANS-SEC ۵۷۵	✓ OWASP ✓ CompTIA Security Plus	آزمون و ارزیابی امنیتی	۴
✓ لایسنس Cobalt Strike ✓ لایسنس SPLUNK ✓ لایسنس NESSUS ✓ لایسنس WALLIX ✓ لایسنس Acunetix ✓ لایسنس XDR ✓ لایسنس مانیتورینگ شبکه نظیر PRTG, SOLAR ✓ لایسنس ISE ✓ لایسنس DLP Symantec ✓ لایسنس Email Securty ✓ Firewall	SANS-SEC ۵۰۳ SANS-SEC ۵۱۱ Certified SOC Analyst (CSA)	✓ Splunk ES ✓ Elastic XDR ✓ Memory Forensic ✓ Network Forensic ✓ تحلیلگر مرکز عملیات ✓ تیم قرمز (Offence) ✓ Network plus ✓ CompTIA Security Plus	پایاده سازی مرکز عملیات امنیت و تیم پاسخ به رخداد	۵

intrusion detection systems ✓ security information and event management (SIEM) ✓ و ...					
✓ تست کابل شبکه ✓ دستگاه تست و آنالیز شبکه دستگاه لیبیل زن	ISO/IEC TS ۲۲۳۳۷ ISO/IEC ۲۲۳۳۷ Design Certification (DCDV) TECHNICAL SPECIFICATION, Information technology Data centre facilities and infrastructures NIST SP ۸۰۰-۱۸۰ آشنایی با نحوه نصب و راه اندازی دوربینهای CCTV	✓ گواهی آموزشی MCSE یا بالاتر ✓ گواهی آموزشی CCNA یا بالاتر ✓ گواهی آموزشی نصب و راه اندازی موارد زیر: دوربین تحت شبکه درهای اتومات و گیت های تردد سیستم های اعلام و اطفای حریق پاور ژنراتور سیستم های تهویه مطبوع نصب و طراحی شبکه سیستم های UPS گواهی آموزشی نگهداری موارد زیر: دوربین تحت شبکه درهای اتومات و گیت های تردد سیستم های اعلام و اطفای حریق پاور ژنراتور سیستم های تهویه مطبوع	پایه سازی امنیت فیزیکی و محیط پیرامونی		۶
Firewall ✓ UTM ✓ WAF ✓ IPS/IDS ✓ DLP ✓ AAA ✓ PAM ✓ antiviruse	NIST SP ۸۰۰-۵۳ SEC۵۲۲-API PCI-DSS ۲,۲ SANS-SEC ۵۰۵ SANS-SEC ۵۰۶ SANS ICS ,۴۱۰	CompTIA Network plus ✓ CompTIA Security plus ✓	امن سازی و مقاوم سازی سامانه ها، زیر ساخت و سرویس ها		۷

✓ لایسنس nessus ✓ لایسنس prtg ✓ سامانه درخت دانش ✓ سامانه مدیریت لایسنس ✓ سامانه تیکتینگ امنیت ✓ سامانه تحلیل شبکه های اجتماعی ✓ جهت آگاهی از وقوع حوادث امنیتی ✓ لایسنس سیستم مدیریت اطلاعات و - رویدادهای امنیتی نظیر Splunk	Certified SOC Analyst (CSA) CEH v۱۲ SANS-FOR ۵۰۸ SANS-FOR ۵۰۰ SANS-FOR ۵۰۹ SANS-SEC ۵۱۱ SANS-SEC ۵۵۵ SANS-FOR ۶۱۰	ISO۲۷۰۰۱ ✓ ISMS ✓ SOLAR ✓ PRTG ✓ ✓ مدیریت پروژه ✓ مدیریت استراتژیک ✓ دوره های مدیریتی ✓ CISSP ✓ CISM ✓ OWASP ✓ CompTIA Security Plus	راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد	۸
✓ لایسنس Nessus ✓ لایسنس Acunetix ✓ لایسنس XDR ✓ لایسنس PRTG - و ...	SANS-SEC ۵۰۴ SANS-SEC ۵۶۰ SANS-SEC ۵۴۲ CEH	✓ انواع دوره های مدیریتی ✓ Power BI ✓ MSP ✓ Cisco ✓ Microsoft ✓ linux ✓ ISMS ✓ Tableau ✓ Mikrotic ✓ CompTIA Security Plus	مسابقات کشف نقص امنیتی	۹
✓ Firewall ✓ UTM ✓ WAF ✓ IPS/IDS ✓ DLP ✓ AAA ✓ PAM	NIST SP ۸۰۰-۵۳ SEC۵۲۲-API PCI-DSS ۲,۲ SANS-SEC ۵۰۵ SANS-SEC ۵۰۶ SANS ICS ,۴۱۰	✓ CompTIA Network plus ✓ CompTIA Security plus	امن سازی و مقاوم سازی سامانه ها، زیر ساخت و سرویس های صنعتی	۱۰

✓ تست و آنالیز شبکه ✓ منبع تغذیه ✓ Fiber source and meter ✓ traffic generator	Systems Security Certified Practitioner (SSCP (CSCU) Certified Secure Computer User (+CySA) CompTIA Cybersecurity Analyst	Linux ✓ Fortinet ✓ CISCO ✓ Huawei ✓ mikrotic ✓ Microsoft ✓ CompTIA Security Plus ✓ CompTIA Network Plus ✓ CCNA ✓	نصب و پشتیبانی محصولات فتا	خدمات فنی	۱۱
✓ آزمایشگاه با تجهیزات شامل (سوئیچ، روتر، اکسس پوینت، فایروال، سرور، IPS/IDS، سیستم‌های مانیتورینگ و لاگ گیری، دستگاه‌ها و نرم‌افزارهای مجازی‌سازی، نرم‌افزارهای شبیه‌سازی شبکه، تجهیزات تست و تحلیل شبکه) ✓ کلاس ✓ سالن ✓ کامپیوتر ✓ ویدیو پروژکتور	-	✓ دوره‌های NIST ✓ دوره‌های ENISA ✓ گواهینامه CISA ✓ گواهینامه CISSP ✓ دوره‌های SANS ✓ گواهینامه Security +	آموزش امنیت فضای تولید و تبادل اطلاعات	خدمات آموزشی	۲