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 دارائی‌های سازمان‌ها
- توانایی تحلیل و مدیریت ریسک
- توانایی تدوین خط‌مشی، فرایندها و راهنماهای امنیتی
- تسلط بر استانداردهای مدیریت امنیت اطلاعات و مدیریت فناوری اطالعات و تدوام کسب و کار و COBITو ITIL
- آشنایی با استانداردهای ارزیابی امنیتی
- آشنایی با مدل‌های بلوغ امنیت اطلاعات
- توانمندی‌های عمومی مشاوره

نحوه امتیازدهی در حوزه خدمات مدیریتی

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	
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
گواهیهای شرکت گواهیهای 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	
	دکترا	۶	
گواهیهای 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

رتبهبندی:

رتبهبندی: فرایندی است که برای یک نوع مقیاس‌گذاری جهت طبقه‌بندی شرکت‌های دارای پروانه فعالیت در حوزه خدمات مدیریتی افتا با گرایش «**مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات**» انجام می‌گیرد.

رتبه: طبقه امتیازی است بین اعداد ۱ الی ۳ که بر اساس شاخص‌های تعیین شده به شرکت‌های ارائه‌کننده خدمات «مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات» اختصاص داده می‌شود.

در حال حاضر فرایند رتبه‌بندی مخصوص شرکت‌های 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 معرفی‌شده 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 معرفی‌شده 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 معرفی‌شده 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 انطباق‌سنج 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 scopeامنیت 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 دارائی‌های 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 تداوم کسب و کار
- ❖ آشنایی با استانداردهای ارزیابی امنیتی
- ❖ آشنایی با مدل‌های بلوغ امنیت اطلاعات
- ❖ آشنایی با ISMS و استانداردهای سری ISO۲۷۰۰۰

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، پیاده‌سازی 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 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. 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 فارنزیک 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
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	
	دکترا	۶	
سوابق شرکت در آن حوزه	به ازای هرسال 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

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

اجزای اساسی در استراتژی امنیت سازمان‌ها محسوب می‌شود. این گرایش‌ها به منظور ایجاد یک ساختار سازمانی قوی برای شناسایی، پیشگیری، تشخیص، و پاسخ به حوادث امنیتی ایجاد شده‌اند. در این راستا شرکت‌های متنوعی وجود داشته که در حیطه پیاده‌سازی مرکز عملیات امنیت و تشکیل تیم پاسخ به رخداد، اقدام به ارائه خدمات می‌نمایند.

خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

- شرکت‌های ارائه دهنده‌ی خدمات زیر:

پیاده‌سازی مرکز عملیات امنیت

طراحی مرکز عملیات امنیت و پاسخ به رخداد

پیاده‌سازی مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

پیاده‌سازی مرکز مدیریت امداد و هماهنگی عملیات رخدادهای امنیتی

داشبوردسازی رخدادهای امنیتی

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

خودکارسازی فرآیندهایSOC

نصب و پشتیبانی SIEM

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

- توانایی برنامه‌ریزی توسعه و مدیریت رخداد
- تسلط بر انواع حملات شبکه بی‌سیم و باسیم
- آگاهی از مفاهیم فارنزیک سیستم و شبکه
- توانایی به‌روزرسانی و مدیریت رویه‌های مدیریت رخداد (با توسعه ابزارها و تکنیک‌ها)
- تسلط بر مفاهیم و معماری شبکه
- تسلط در زمینه امنیت شبکه، سیستم‌عامل، پایگاه داده و برنامه‌های کاربردی
- تسلط بر پیکربندی تجهیزات شبکه
- توانایی پیکربندی امن تجهیزات نرم‌افزاری و سخت‌افزاری
- آزمون و به روزرسانی رویه های مدیریت رخداد
- تهیه طرح تداوم کسب وکار
- تهیه طرح بازیابی از فاجعه
- نحوه شناسایی و اشراف بر داراییهای مطالعاتی
- مدیریت آسیب‌پذیریها و مخاطرات سایبری
- مدیریت دسترسی به منابع سازمان
- فرایند شکار تهدیدات (Threat Hunting)

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

معرفی گرایش پیاده‌سازی امنیت فیزیکی و محیط پیرامونی:

گرایش پیاده‌سازی امنیت فیزیکی و محیط پیرامونی به ایجاد سیاست‌ها و اقداماتی متناسب با حفاظت از جنبه‌های فیزیکی و محیطی سازمان می‌پردازد. این گرایش با هدف حفاظت از منابع، دارایی‌ها، و افراد در محیط فیزیکی سازمان ایجاد شده است. در این راستا شرکت‌های متنوعی وجود داشته که در به پیاده‌سازی امنیت فیزیکی و محیط پیرامونی ، اقدام به ارائه خدمات می‌نمایند.

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 :

1. **نظارت تصویری**
2. **تشخیص و اطفا حریق**
3. **کنترل دسترسی فیزیکی**
4. **تامین پایدار انرژی**

خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

- شرکت‌های ارائه دهنده‌ی خدمات و محصولات زیر:
  نصب و راه‌اندازی، پشتیبانی و تعمیرات دوربین‌های تحت شبکه IP دوربین‌ها
  نصب و راه‌اندازی، پشتیبانی و تعمیرات سیستم‌های اعلام و اطفاء حریق
  نصب و راه‌اندازی، پشتیبانی و تعمیرات گیت هوشمند و تجهیزات کنترل تردد
  نصب و راه‌اندازی، پشتیبانی و تعمیرات تأمین کننده‌ی برق (ژنراتور)
  نصب و راه‌اندازی، پشتیبانی و تعمیرات سنسورهای دما و رطوبت
  نصب و راه‌اندازی، پشتیبانی و تعمیرات سیستم‌های تهویه مطبوع(cooling)
  شرکت‌های فعال انطباق‌سنج در حوزه امنیت اطلاعات

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

- تسلط بر مکانیزم‌های فیزیکی کنترل دسترسی
- تسلط بر ایمن‌سازی محیطی برای حوزه فناوری اطلاعات
- تسلط بر مکانیزم‌ها و راه حل‌های امنیت محیط پیرامونی
- آشنایی با تجهیزات امنیت محیط پیرامونی
- تسلط بر راه‌حل‌های تامین مطمئن برق
- ارزیابی امنیت فیزیکی
- تسلط بر استانداردهای مرتبط با پیاده سازی و تامین امنیت فیزیکی و محیط پیرامونی

معرفی گرایش امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها:

گرایش امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها به ایجاد و اجرای سیاست‌ها، تدابیر و فناوری‌های امنیتی با هدف کاهش آسیب‌پذیری‌ها، حفاظت از اطلاعات و خدمات، و حفظ پایداری و عملکرد سیستم‌ها می‌پردازد. در این راستا شرکت‌های متنوعی وجود داشته که در به امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها، اقدام به ارائه خدمات می‌نمایند.

خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

- طراحی و اجرای کلیه اقدامات برای افزایش امنیت و مقاوم‌سازی شامل:
  پیکره‌بندی امن (اجرای تنظیمات امنیتی برای زیرساخت و سیستم‌ها)
- راه اندازی سیستمهای Firewall، UTM، WAF، IPS/IDS، DLP، AAA، PAM
- طراحی شبکه و زیرساخت، Zoneبندی‌ها و محل قرارگیری تجهیزات امنیتی در توپولوژی هم‌بندی به درستی و طبق معماری‌های رایج و استاندارد
- اعمال Based-line Policyها بر روی سرورها و دامین
- اعمال Firewall Rule
- نصب آنتی ویروسهای مناسب

- اعمال پروسه‌های Endpoint Protection
- اعمال صحیح پروسه Vulnerability Assessment
- جداسازی شبکه LAN از شبکه Internet
- رمزنگاری داده‌ها با هدف حفظ اطلاعات حساس حین انتقال و ذخیره‌سازی
- امن‌سازی و پشتیبانی شبکه‌های IOT و دیسپاچینگ
- انجام اقدامات پیشگیرانه امن‌سازی(Penetration Testing , Threat Hunting , Device Audit)

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

- تسلط بر مفاهیم و معماری شبکه
- تسلط بر راهبری و پیکربندی تجهیزات شبکه
- تسلط بر امن‌سازی و مقاوم‌سازی سیستم‌ها، سرورها و شبکه
- آشنایی با انواع پروتکل‌های امن و رمزنگاری
- تسلط بر راه‌حلهای مرتبط با تداوم کسب‌وکار در فناوری اطلاعات
- تسلط بر مجازی‌سازی و رایان ابری
- ارزیابی و مدیریت ریسک و آسیب‌پذیری‌ها
- آشنایی با انواع پروتکل‌های امن و رمزنگاری
- آگاهی از استانداردهای مدیریت فناوری اطلاعات و مدیریت امنیت فناوری اطلاعات

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

معرفی گرایش راهبری مرکز عملیات و تیم پاسخ به رخداد:

گرایش راهبری مرکز عملیات امنیت (SOC) و تیم پاســـخ به رخداد (CSIRT) به مدیریت و هدایت این دو اجزای مهم در زمینه امنیت اطلاعات و فناوری اطلاعات اشـاره دارد. این گرایش به تدبیرها و اسـتراتژی‌هایی متمرکز اسـت که بر اسـاس هوش تجاری، تصـمیم‌گیری موثر، و تدابیر بهینه در زمینه‌های SOC و IRT صورت می‌گیرد. در این را ستا شرکت‌های متنوعی وجود دا شته در گرایش راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد ، اقدام به ارائه خدمات می‌نمایند.خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

- مدیریت و راهبرد رخدادهای امنیتی
- پیاده‌سازی فرآیندهای پاسخ به رخدادهای امنیتی
- پیاده‌سازی استراتژی امنیتی
- ایجاد پروفایل و تعیین سطح بلوغ امنیتی
- تدوین برنامه عملیاتی امن‌سازی

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

- آشنایی با ابزارهای پای ترافیک و رکوردهای ثبت شده
- تسلط کافی بر انواع حمالت شبکه بیسیم و باسیم

- آشنایی با اقدامات فارنزیک سیستم و شبکه
- توانایی پشتیبانگیری و بازیابی دادهها
- توانایی بهروزرسانی و مدیریت رویههای مدیریت رخداد(راهبری رویهها)
- تسلط کافی بر مفاهیم و معماری شبکه
- تسلط کافی در زمینه امنیت شبکه، سیستمعامل، پایگاه داده و برنامههای 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 آسیبپذیریها و مخاطرات سایبری
- مدیریت دسترسی به منابع سازمان
- پیکربندی تجهیزات و سامانهها
- امنیت شبکه و سامانهها
- پایش و مدیریت لاگها
- تداوم و پایداری سرویسها
- اقدامات زمان بحران
- اقدامات پس از بحران

تذکر: متقاضی در هیچ یک از گرایشهای 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 میشود. در این نوع مسابقات، شرکتکنندگان با رقابت در مسائل و چالشهای مختلف امنیتی، مهارتها و تواناییهای خود را در زمینه کشف نقصهای امنیتی و مقابله با حملات سایبری به اثبات میکنند. در این راستا شرکتهای متنوعی وجود داشته در گرایش مسابقات کشف نقص امنیتی ، اقدام به ارائه خدمات مینمایند.خدمات ارائه شده این نوع شرکتها عبارت است از:

- شرکتهای برگزار کنندهی مسابقات کشف نقص امنیتی (در شبکه، سامانهها، سرویسها، نرمافزارها و...) و مسابقات تستهای نفوذ
- این شرکتها باید تمامی مهارتهای گرایش آزمون امنیتی سایبری و شبکه را دارا باشند.
- باگ باونتی
- 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 فارنزیک 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 مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌های صنعتی :

گرایش امن‌سازی و مقاوم‌سازی 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 مقاوم‌سازی 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
- ارایه 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
- ارایه سازوکارهای کنترل دسترسی و مدیریت کاربران در شبکه‌های صنعتی
- تدوین خط‌مشی‌ها، دستورالعمل‌ها، روش‌های اجرایی و مستندات امنیتی در شبکه‌های صنعتی
- ارایه راهکارهای مسیریابی امن در شبکه‌های صنعتی و امن‌سازی ارتباطات بیرونی شبکه سیستم‌های کنترلی
- تدوین توافق‌نامه‌های امنیتی شخص سوم در شبکه‌های صنعتی
- اجرای آزمون نفوذپذیری مختص به سیستم‌های کنترل صنعتی
- مدیریت وصله‌های امنیتی سیستم‌های کنترل صنعتی
- تدوین طرح‌های مقابله با بدافزار، تداوم کسب و کار و بازیابی از فاجعه در سیستم‌های کنترل صنعتی
- ارایه راه حل‌های امن‌سازی فیزیکی سیستم‌های کنترل صنعتی
- آموزش امنیتی مدیران، کارشناسان و کاربران شبکه‌های صنعتی
- پیکره‌بندی امن (اجرای تنظیمات امنیتی برای زیرساخت و سیستم‌ها) در حوزه صنعتی
- رمزنگاری داده‌ها با هدف حفظ اطلاعات حساس حین انتقال و ذخیره‌سازی در حوزه صنعتی
- امن‌سازی و پشتیبانی شبکه‌های PLC , DCS , SCADA , ISC , IIOT و دیسپاچینگ در حوزه صنعتی

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

- تسلط بر مفاهیم و معماری شبکه
- تسلط بر راهبری و پیکربندی تجهیزات شبکه
- تسلط بر امن‌سازی و مقاوم‌سازی سیستم‌ها، سرورها و شبکه
- آشنایی با انواع پروتکل‌های امن و رمزنگاری
- تسلط بر راه‌حل‌های مرتبط با تداوم کسب‌وکار در فناوری اطلاعات
- تسلط بر مجازی‌سازی و رایانش ابری
- بررسی و شناخت SIEM صنعتی و نحوه استفاده از آن در یک سیستم کنترل صنعتی
- ارزیابی و مدیریت ریسک و آسیب‌پذیری‌ها
- آشنایی با انواع پروتکل‌های 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 می‌باشد 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 فرآیند نصب، پیکربندی، و پشتیبانی از محصولات و سامانه‌های 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 شرکت‌های متنوعی وجود داشته گرایش نصب و پشتیبانی محصولات فتا، اقدام به ارائه خدمات می‌نمایند.خدمات ارائه شده این نوع شرکت‌ها عبارت است از:

- آموزش استفاده و چگونگی راهبری استفاده از محصول
- شرکت‌های فعال در زمینه‌ی فروش،موارد زیر:
- سخت‌افزار شبکه-(dispatching- UTM- access point-Router-storage-switch-server) ماژول شبکه
- نرم‌افزارهای کاربردی (سامانه‌های تحت وب)

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارت‌اند از:

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

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- شرکت هایی که تولیدکننده محصول بومی (داخلی) بوده و موفق به اخذ گواهی امنیتی محصول شده باشند. این شرکت ها لازم است نسبت به بارگذاری گواهی ارزیابی امنیتی محصول خود، در سامانه ارزیابی و صدور پروانه خدمات امنیتی اقدام نمایند.

۲- شرکت هایی که تولیدکننده محصول بومی (داخلی) هستند و هنوز موفق به اخذ گواهی امنیتی محصول خود نشده اند، در صورت طی مراحل ورود محصول به فرآیند ارزیابی فنی در یکی آزمایشگاه‌های مورد تایید سازمان فناوری اطلاعات ایران، لازم است نسبت به ارسال نامه کتبی به اداره‌کل توسعه صنعت افتا سازمان فناوری اطلاعات، جهت استعلام محصول خود اقدام نماید. در این راستا لازم است مراحل انعقاد قرارداد با آزمایشگاه، تحویل مستندات و نصب محصول در آزمایشگاه انجام شده باشد و آزمایشگاه در حال ارزیابی محصول باشد. لازم به ذکر است در صورت مثبت بودن نتیجه استعلام (وضعیت درحال ارزیابی، وضعیت اتمام ارزیابی یا وضعیت ارسال گزارش به افتا)، پاسخ کتبی دریافت شده از اداره‌کل توسعه صنعت افتا، به عنوان گواهی ارزیابی امنیتی محصول، در سامانه ارزیابی و صدور پروانه خدمات امنیتی قابل بارگذاری است.

۳- شرکت هایی که واردکننده محصولات وارداتی می-باشند و سابقه واردات محصولات (غیررادیویی، اکتیو و تحت شبکه اعم از سوئیچ شبکه، روتر، فایروال، سرور، ذخیره‌ساز، UTM، IDSو IPS) را از طریق سازمان تنظیم مقررات و ارتباطات رادیویی دارند، لازم است نسبت به ارسال نامه کتبی به اداره‌کل توسعه صنعت افتا سازمان فناوری اطلاعات، اقدام و پاسخ کتبی دریافت شده از اداره کل یاد شده را به عنوان گواهی ارزیابی امنیتی محصول، در سامانه ارزیابی و صدور پروانه خدمات امنیتی بارگذاری کنند.

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	
	دکترا	۶	
سوابق شرکت در آن حوزه	به ازای هرسال 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 دورهای 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 کمک‌آموزشی 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 ۸۰۰-۱۶ و SP NIST ۸۰۰-۵۰ و استانداردهای سری ISO ۲۷۰۰۰ و دیگر مستندات و استانداردهای مربوطه

داشتن مجوز استانداردی مبنی بر ارائه خدمات آموزش

نحوه امتیازدهی در حوزه خدمات آموزشی

شاخص	شرایط	امتیاز هر مورد	سقف امتیاز فرم
دورهای آموزشی برگزارشده 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	
	دکترا	۶	
سوابق شرکت/موسسه در آن حوزه	به ازای هرسال سابقه مرتبط	۱	۵
گواهیهای شرکت/موسسه	به ازای هر گواهی مرتبط	۳	۶
گواهیهای آموزشی مدرسین	به ازای هر گواهی افتا	۳	۳۰
فضای آموزشی	به ازای هر کلاس	۱۵	۶۰
تجهیزات	به ازای هر مورد	۵	۱۵
سابقه تدریس مرتبط مدرسان در ۵ سال اخیر (در سایر موسسات/شرکت آموزشی)	به ازای هر دوره	۵	۳۰

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) COBIT,ITIL,CIS استانداردهای, ,benchmark NIST SP ۸۰۰-۵۳ استاندارد , SANS-SEC ٥٦٦	✓ ندارد

۲		ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات	✓ دوره‌های NIST ✓ دوره‌های ENISA ✓ گواهینامه CISA ✓ گواهینامه CISSP ✓ دوره‌های SANS ✓ گواهینامه Security+ ✓ گواهینامه‌های سیسکو ✓ گواهینامه سرممیزی IATF ✓ گواهینامه سرممیزی NACI استاندارد ISO۱۹۰۱۱	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	✓ ندارد
۴	خدمات عملیاتی	آزمون و ارزیابی امنیتی	✓ OWASP ✓ CompTIA Security Plus	SANS-SEC ۵۰۴ SANS-SEC ۵۶۰, SANS-SEC ۵۴۲ Certified Ethical Hacker (CEH) SANS-SEC ۵۷۵	✓ لایسنس Nessus ✓ لایسنس Acunetix ✓ لایسنس XDR ✓ لایسنس PRTG ✓ و ...
۵		پیاده سازی مرکز عملیات امنیت و تیم پاسخ به رخداد	✓ Splunk ES ✓ Elastic XDR ✓ Memory Forensic ✓ Network Forensic ✓ تحلیلگر مرکز عملیات ✓ تیم قرمز(Offence) ✓ Network plus ✓ CompTIA Security Plus	SANS-SEC ۵۰۳ SANS-SEC ۵۱۱ Certified SOC Analyst (CSA)	✓ لایسنس Cobalt Strike ✓ لایسنس SPLUNK ✓ لایسنس NESSUS ✓ لایسنس WALLIX ✓ لایسنس Acunetix ✓ لایسنس XDR ✓ لایسنس مانیتورینگ شبکه نظیر PRTGوSOLAR ✓ لایسنس ISE ✓ لایسنس DLP Symantec ✓ لایسنس Email Secuirty ✓ Firewall

					intrusion detection systems ✓ security information and event management (SIEM) ✓ و...
۶		**پیاده سازی امنیت فیزیکی و محیط پیرامونی**	✓ گواهی آموزشی MCSE یا بالاتر ✓ گواهی آموزشی CCNA یا بالاتر ✓ گواهی آموزشی نصب و راه‌اندازی موارد زیر: دوربین تحت شبکه درهای اتومات و گیت‌های تردد سیستم‌های اعلام و اطفا حریق پاور ژنراتور سیستم‌های تهویه مطبوع نصب و طراحی شبکه سیستمهای UPS گواهی آموزشی نگهداری موارد زیر: دوربین تحت شبکه درهای اتومات و گیت‌های تردد سیستم‌های اعلام و اطفا حریق پاور ژنراتور سیستم‌های تهویه مطبوع	ISO/IEC TS ۲۲۲۳۷ ISO/IEC ۲۲۲۳۷Design Certification (DCDV) TECHNICAL SPECIFICATION, Information technology Data centre facilities and infrastructures NIST SP ۸۰۰-۱۸۰ آشنایی با نحوه نصب و راه اندازی دوربینهای CCTV	✓ تسترکابل شبکه ✓ دستگاه تست و آنالیز شبکه دستگاه لیبل زن
۷		**امن سازی و مقاوم سازی سامانه ها، زیر ساخت و سرویس ها**	✓ CompTIA Network plus ✓ CompTIA Security plus	NIST SP ۸۰۰-۵۳ SEC۵۲۲-API PCI-DSS ۲,۲ SANS-SEC ۵۰۵ SANS-SEC ۵۰۶ SANS ICS ,۴۱۰	Firewall ✓ UTM ✓ WAF ✓ IPS/IDS ✓ DLP ✓ AAA ✓ PAM ✓ antiviruse

۸		**راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد**	ISO۲۷۰۰۱ ✓ ISMS ✓ SOLAR ✓ PRTG ✓ مدیریت پروژه ✓ مدیریت استراتژیک ✓ دوره‌های مدیریتی ✓ CISSP ✓ CISM ✓ OWASP ✓ CompTIA Security Plus ✓	Certified SOC Analyst (CSA) CEH v۱۲ SANS-FOR ۵۰۸ SANS-FOR ۵۰۰ SANS-FOR ۵۰۹ SANS-SEC ۵۱۱ SANS-SEC ۵۵۵ SANS-FOR ۶۱۰	لایسنسnessus ✓ لایسنسprtg ✓ 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
۹		**مسابقات کشف نقص امنیتی**	انواع دوره‌های مدیریتی ✓ Power BI ✓ MSP ✓ Cisco ✓ Microsoft ✓ linux ✓ ISMS ✓ Tableu ✓ Mikrotic ✓ CompTIA Security Plus ✓	SANS-SEC ۵۰۴ SANS-SEC ۵۶۰ SANS-SEC ۵۴۲ CEH	لایسنس Nessus ✓ لایسنس Acunetix ✓ لایسنس XDR ✓ لایسنس PRTG ✓ و ...
۱۰		**امن سازی و مقاوم سازی سامانه ها، زیر ساخت و سرویس های صنعتی**	CompTIA Network plus ✓ CompTIA Security plus ✓	NIST SP ۸۰۰-۵۳ SEC۵۲۲-API PCI-DSS ۳,۲ SANS-SEC ۵۰۵ SANS-SEC ۵۰۶ SANS ICS ,۴۱۰	Firewall ✓ UTM ✓ WAF ✓ IPS/IDS ✓ DLP ✓ AAA ✓ PAM ✓

۱۱	خدمات فنی	نصب و پشتیبانی محصولات فتا	Linux ✓ Fortinet ✓ CISCO ✓ Huawei ✓ mikrotic ✓ Microsoft ✓ CompTIA Security Plus ✓ CompTIA Network Plus ✓ CCNA ✓	Systems Security Certified Practitioner (SSCP (CSCU) Certified Secure Computer User (+CySA) CompTIA Cybersecurity Analyst	✓ تست و آنالیز شبکه ✓ منبع تغذیه ✓ Fiber source and meter ✓ traffic generator
۲	خدمات آموزشی	آموزش امنیت فضای تولید و تبادل اطلاعات	✓ دوره‌هایNIST ✓ دوره‌هایENISA ✓ گواهینامهCISA ✓ گواهینامهCISSP ✓ دوره‌هایSANS ✓ گواهینامه+ Security	-	✓ 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