Cyber Security & Resilience Practitioner

مقدمه

مفهوم Cyber Security & Resilience مجموعه ای جامع از ابزارها و آموزش ها برای کمک به سازمان در دستیابی به بهترین عملکرد در حوزه ی امنیت سایبری است. این چارچوب کمک می کند تا سازمان بتواند از طریق استفاده از فرآیندها و استانداردهای موجود، انعطاف پذیری سایبری خود را ارتقا داده و بدون در نظر گرفتن نقش یا مسئولیت افراد از طریق بکار گیری بهترین مهارت ها و رفتارها در حوزه ی امنیت سایبری در سراسر سازمان فراتر از امنیت سایبری موثر و دستیابی به قابلیت انعطاف پذیری سایتی در سازمان اقدامات لازم مورد انجام قرار گیرد. بر این اساس می توان گفت مفهوم Cyber Security & Resilience به معنای تجهیز کارکنان با دانش و مهارت های لازم و ایجاد آگاهی، شفافیت و اطمینان از نحوه ی واکنش و بازیابی شرایط برای بهبود توانایی سازمان در تشخیص و مبارزه با تهدیدات امنیت سایبری می باشد:

انجام عملیات تشخیص و محافظت در مقابل حملات سایبری بر عهده سازمان نیست بلکه افراد سازمان هستند که مجری چنین فعالیتهایی خواهند بود. تجهیز افراد به نحوه کنش و واکنش در فضای سایبری امری الزامی جهت حفظ ارزشهای سازمان در داخل سازمان است

اهداف دوره

- خسارات ناشی از نقص امنیت سایبری را کاهش می دهد
- بهینه سازی بازیابی ناشی از نقض های امنیت سایبری
- اسان سازی پذیرش مفهوم Cyber resilience در فرآیندهای موجود سازمان
- پشتیبانی از بهترین روشهای طراحی استراتژی انعطاف پذیری سایبری در داخل سازمان
- ایجاد یک زبان مشترک برای پذیرش انعطاف پذیری سایبری در سراسر سازمان
- پشتیبانی موثر از هزینه ها با ایجاد امنیت در پروژه ها و برنامه های سازمان
- محافظت در برابر تهدیدات با حصول اطمینان از راه حل های مناسب مناسب طراحی شده سازگار با استراتژی

Cyber Security & Resilience Practioner

درباره ی IT HOUSE

تیم مدیریتی IT House از سال ۱۳۸۷ به صورت جدی به منظور ارائه‌ی خدمات مشاوره‌ای و آموزشی در حوزه‌ی چارچوب‌های مدیریتی فناوری اطلاعات پا به عرصه‌ی ظهور گذاشت. این گروه در ابتدا تحت نام‌های تجاری دیگری همچون NIS ICT شروع به فعالیت نموده که در سال ۱۳۹۸ به منظور ارائه‌ی خدمات جدید و متفاوت برند IT House را ایجاد نموده‌اند. IT House با اتکا به توانمندی نیروهای متخصص داخلی و همینطور حمایت شبکه‌ای گسترده از شرکای بین‌المللی، همچون گذشته آمادگی دارد سبد کاملی از خدمات مورد نیاز سازمان‌ها را در حوزه‌های استانداردها و چارچوب‌های مدیریت فناوری اطلاعات و امنیت اطلاعات، ارائه نماید. حوزه‌های اصلی فعالیت این شرکت چارچوب‌ها و استانداردها و بهروش‌های مدیریتی فناوری اطلاعات از جمله و نه محدود به موارد مندرج در دیاگرام‌های ذیل است که در هر یک از چارچوب‌های درج شده خدمات مرتبط با:

- آموزش
- مشاوره
- نرم‌افزار
- ممیزی و صدورگواهینامه
- ارزیابی

بسته به نوع محصول، ارائه می‌شود.

مخاطبان دوره

- مدیران امنیت اطلاعات
- مدیریان امنیت سایبری
- مدیران ریسک
- مدیران فناوری اطلاعات
- مدیران سیستم های و روش ها
- تحلیل گران کسب و کار

مدت زمان دوره

4 روز– حضوری (32 ساعت)
24 ساعت – آنلاین تعاملی

سرفصل های دوره

1- چارچوب مهندسی تاب آوری سایبری
2- اهداف تاب آوری سایبری
3- تکنیک ها و رویکردهای تاب آوری سایبری
4- اصول طراحی تاب آوری سایبری
5- رابطه بین ساختارهای تاب آوری سایبری
6- تاب آوری سایبری در چرخه حیات سیستم
7- مدیریت ریسک و تاب آوری سایبری
8- تاب آوری سایبری در عمل
9- انتخاب و اولویت بندی سازه های تاب آوی سایبری
10- روش دستیابی به اهداف و مقاصد تاب آوری سایبری
11- استراتژی مدیریت ریسک سایبری
12- انواع سیستم های سایبر پایه
13- تحلیل تهدید ها و ریسک های سایبری
14- مدل بلوغ سیستم ها در مواجهه ریسک
15- تجزیه و تحلیل سیستم های سایبری تاب آور
16- تعریف و تجزیه و تحلیل جایگزین های خاص
17- تدوین توصیه نامه های تاب آوری سایبری

پیش نیازهای دوره

تسلط بر مفاهیم RISK، امنیت و مدیریت و حاکمیت خدمات ضروری است

تعداد شرکت کنندگان

6 الی 18 نفر

درباره ی مدرک

به شرکت کنندگان در این دوره ی آموزشی گواهی حضور از سوی شرکت IT HOUSE اعطا خواهد شد.

تماس با IT HOUSE

آدرس:
تهران، سهروردی شمالی،کوچه تهمتن، پلاک 6 واحد 7
تلفن: + 98 (0) 21 88731466
فکس: + 98 (0) 21 86031447
وبسایت: www.it-house.me
ایمیل: info@it-house.me

iT House
Enabling Your Enterprise IT