Cyber Security & Resilience Foundation

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 تعهدیدات با حصول اطمینان از راه حل های مناسب مناسب طراحی شده سازگار با استراتژی

Cyber Security & Resilience Foundation

درباره ی IT HOUSE

مؤسسه فناوری اطلاعات راهکار نوآوران فرتاک پس از 7 سال همکاری موفق و مستمر شرکت NIS CERT کانادا با سازمان های ایرانی، در سال 2011 میلادی به عنوان یکی از واحدهای کسب و کار استراتژیک (SBU) این شرکت، با نام تجاری NISICT پا به عرصه ی ظهور گذاشت. این مجموعه در طی 8 سال پس از همکاری موفق با بیش از 200 سازمان بر تر ایرانی، از ابتدای سال 2019 میلادی با توجه به راه اندازی مراکز تخصصی پیشرفته با همکاری شبکه ی گسترده ای از شرکای معتبر داخلی و بین المللی در طیف وسیعی از بهروش ها و استاندارد های بین المللی با هدف ارائه راهکار های جامع مدیریتی در حوزه ی فناوری اطلاعات، ماهیت تجاری خود (برند) را تغییر داده و از نشان تجاری IT HOUSE در حوزه ی محصولات و خدمات خود استفاده خواهد نمود. IT HOUSE با همکاری انحصاری مؤسساتی از جمله Quint (هلند)، NTT (ایرلند)، ACT POWER (مراکش) تحت اعتبار مراجع جهانی همچون انجمن جهانی tmforum آمریکا، PCI Council آمریکا، ISACA آمریکا، AXELOS انگلستان قادر به ارائه خدمات در تزار استاندارد های بین المللی به سازمان های ایرانی می باشد

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

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

- **مفاهیم پایه امنیت و تاب آوری سایبری**
  1- فضای سایبری
  2- امنیت سایبری
  3- تاب آوری سایبری
  4- امنیت و تاب آوری سایبری
  5- تهدید سایبری
  6- سناریوی تهدید
  7- آسیب پذیری
  8- حمله سایبری
  9- ریسک سایبری
  10- تاب آوری سایبری سازمان و نهاد
  11- اتوماسیون صنعتی
  12- سیستم های کنترل صنعتی
- **اجرای تاب آوری سایبری**
  13- چرخه تاب آوری سایبری
  14- چارچوب های اصلی در تاب آوری سایبری
  15- تاب آوری سایبری و ویژگی های مرتبط با سیستم ها
  16- رویکردهای بهبود تاب آوری در برابر تهدیدات سایبر
  17- فرایند بهبود تاب آوری سیستم ها
  18- اصول کلی و پایه تاب آوری سایبری
- **بررسی و توسعه تاب آوری سایبری**
  19- ابعاد و مولفه ها ارزیابی تاب آوری سایبری
  20- ارائه مدل مفهومی تاب آوری سایبری مبتنی بر مدل CERT
  21- آلزامات تاب آوری و شاخص های شناسایی و مدیریت دارایی و تجهیزات
  22- الزامات تاب آوری و شاخص های پیکره بندی و مدیریت تغییر
  23- الزامات تاب آوری و شاخص های نظارت و کنترل بر عملکرد
  24- الزامات تاب آوری و شاخص های ارزیابی و تحلیل آسیب پذیری ها
  25- الزامات تاب آوری و شاخص های ارزیابی و تحلیل رخداد ها و حوادث
- **سایبری**
  26- الزامات تاب آوری و شاخص های تداوم فعالیت ها و خدمات
  27- الزامات تاب آوری و اشخص های ارزیابی و تحلیل ریسک
  28- الزامات تاب آوری و شاخص های اریزابی و تحللی وابستگی و ارتباطات خارجی
- **خارجی**
  29- الزامات تاب آوری و شاخص های آموزش و آگاهی
  30- ازلامات تاب آوری و شاخص های آگاهی وضعیتی تاب آوری سایبری
  31- مدل ارزیابی تاب آوری سایبری سازمان
  32- مدل ارزیابی سطوح بلوغ تاب آوری سایبری سازمان

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.