بسم الله الرحمن الرحیم

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

(ماهـــــر)

مرکز ماهر

در راستای اقدام شماره ۲-۴ سند راهبردی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)، **مرکز ماهر** به عنوان CERT ملی کشور، در دهم اسفند سال ۱۳۸۷ با برگزاری اولین همایش خود اعلام موجودیت نمود.

راهبرد	شماره اقدام	اقدام	مجری	همکار
ایجاد و توسعه نظام های فرابخشی افتا	۲-۴	طرح ایجاد نظام پیش گیری، مقابله و امداد افتا، به منظور : ✓ جمع آوری مؤثر، پردازش و مدیریت یکپارچه اطلاعات مربوط به حملات، تهدیدها و آسیب پذیری ها ✓ اطلاع رسانی و ارائه هشدارهای امنیتی در سطح کشور ✓ کمک به رفع آسیب پذیری ها، تهدیدها و تأثیرات حملات	وزارت ارتباطات و فناوری اطلاعات	✓ وزارت کشور ✓ وزارت دفاع و پشتیبانی نیروهای مسلح ✓ وزارت علوم، تحقیقات و فناوری ✓ وزارت اطلاعات

اهداف مرکز ماهر

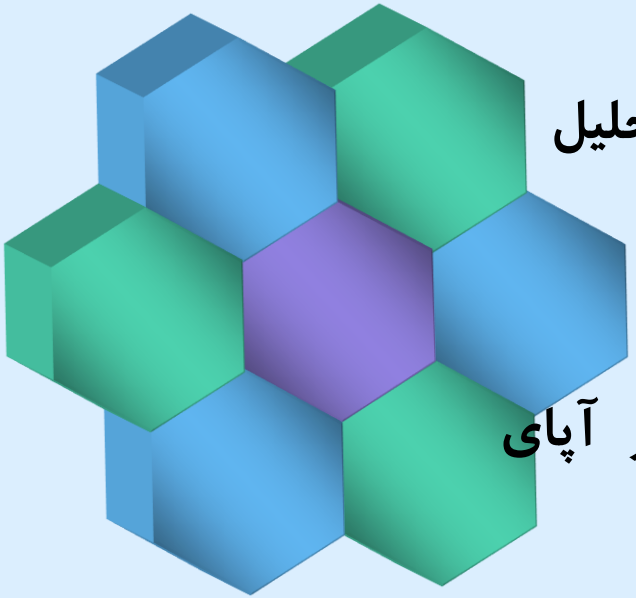
- ایجاد یک نقطه کانونی در سطح ملی برای انجام فعالیت های هماهنگ راهبری رخدادهای فضای تبادل داده
- ایجاد هماهنگی های لازم در راستای تجزیه و تحلیل رخدادها پاسخ گویی به رخدادها در فضای تبادل اطلاعات
- و وقایع امنیتی
- تعامل با سازمانها ، شرکت های دولتی ، بخش خصوصی وجامعه دانشگاهی
- افزایش سطح آگاهی وترویج استراتژی های کاهش دهنده مخاطرات از طریق اطلاع رسانی عمومی و آموزش
- کمک به شناسایی و رفع آسیب پذیری ها و تهدید ها وارائه خدمات امداد

اقدامات مرکز ماهر

اقدامات مرکز ماهر

- طراحی و ایجاد شبکه هانی نت ملی (شبکه کشف و جمع آوری بدافزار در سطح کشور)
- ایجاد تیم مدیریت و پاسخگویی به رخدادهای رایانه ای در مرکز ماهر
- راه اندازی آزمایشگاه تحلیل بدافزار و شناسایی تهدیدات سایبری و ارائه سرویس به تمامی سازمانها و دستگاه های اجرایی کشور
- رصد، پشتیبانی و مشاوره در حوزه افتای مرکز ماهـــر
- راه اندازی سامانه جامع تعاملی مرکز ماهر
- ایجاد تیم راه اندازی تیم های گوهر در سازمانها
- اقدام درخصوص راه اندازی C E R T صنعتی در منطقه جنوب کشور با محوریت استان فارس
- تدوین نظام ملی پیشگیری و مقابله با حوادث رایانه ای
- فرهنگ سازی، آموزش و اطلاع رسانی
- راه اندازی و به روز رسانی پرتال مرکز ماهر (w w w .C e r t c c .ir)

طراحی و ایجاد شبکه هانی نت ملی

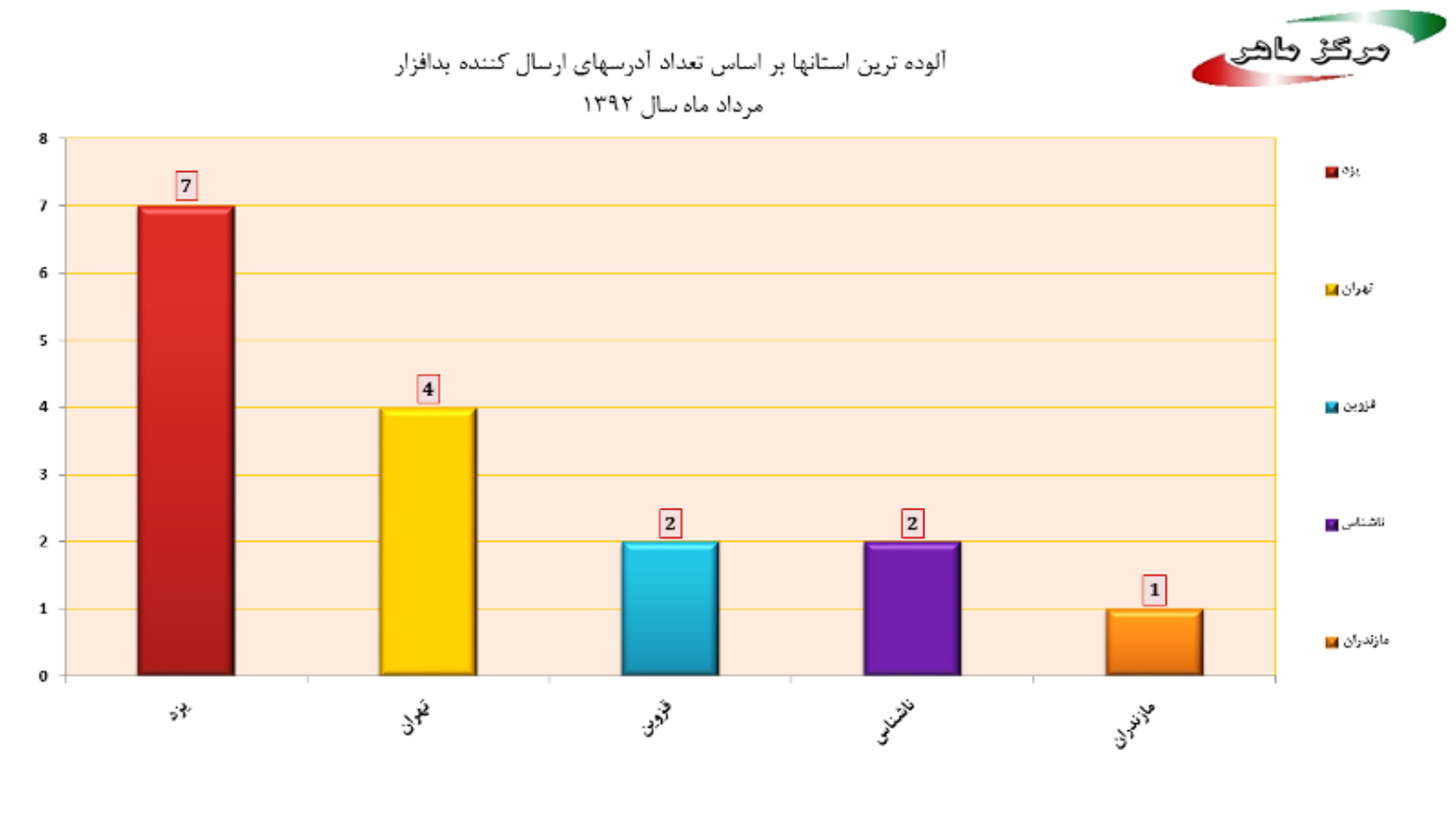


- اقدامات صورت گرفته در حوزه مدیریت و تجزیه و تحلیل بدافزارها در فضای آدرس های IP کشور:
  - ✓راه اندازی شبکه هانی نت با همکاری مراکز آپای دانشگاهی، با نصب ۱۹۶ هانی پات (۷۸۴ سنسور)
  - در ۳۱ استان کشور

طراحی و ایجاد شبکه هانی نت ملی

- آدرسهای آلوده :
  - شناسایی بیش از ۱۶۲۱۷ آدرس اینترنتی آلوده در سطح کشور در سال ۹۰
  - شناسایی بیش از ۱۲۶۰۶آدرس اینترنتی آلوده در سطح کشور در سال ۹۱
- بدافزار :
  - شناسایی بیش از ۱۵۴۷کد مخرب (ویروس ، تروجان و ...) در سال ۹۰
  - شناسایی بیش از ۲۶۴۵ کد مخرب (ویروس ، تروجان و ...) در سال ۹۱
- اعلان هشدار بطور مستمر به دارندگان این آدرس های اینترنتی آلوده
- مرجع اعلام استان های با بیشترین آلودگی در کشور به آدرس www.Certcc.ir
- راه اندازی سیستم هانی کلاینت و اسپم پات ، بات نت و DNS sinkhole ، تلسکوپ شبکه ای

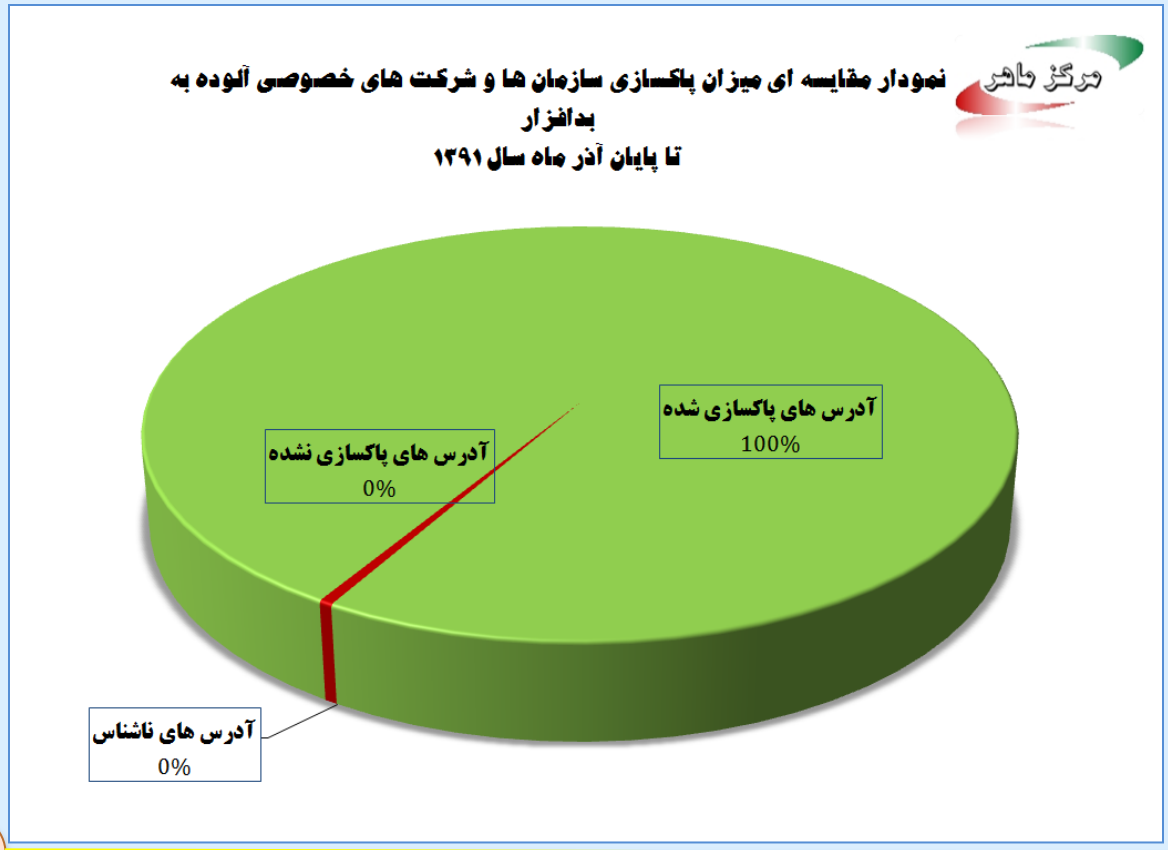
طراحی و ایجاد شبکه هانی نت ملی



طراحی و ایجاد شبکه هانی نت ملی

در راستای کاهش چشم گیر آدرسهای آلوده در سطح کشور با ارائه مداوم هشدارها جهت پاکسازی آدرسها شناسایی شده، مجموع آدرسهای شناسایی شده در آذر ماه ۹۰ از ۴۲۴ آدرس در سطح استانهای کشور به ۵۴ آدرس آلوده در آذر ماه ۹۱ کاهش یافته است.

این نمودار نشان دهنده پاکسازی آدرس های اعلان شده تا کنون بوده است.



روند پاکسازی آدرسهای آلوده اعلام شده به سازمانها از ابتدای سال ۹۱ تا مرداد ماه به ۹۶٪ ، شهریور ماه ۹۷٪، مهر ماه ۹۹٪ و آذر ماه ۱۰۰٪ ارتقا یافت.

- حمله سایبری استاکنت
- حمله سایبری دوکو
- حمله سایبری Wiper
- حمله سایبری شعله آتش (Flame)
- حمله سایبری Madi
- حمله سایبری Shamoon
- حمله سایبری Mini Flame
- حمله سایبری New Wiper

رصد، پشتیبانی و مشاوره در حوزه افتا

- شناسایی، تحلیل و ارائه راهکار بدافزارهای پرخطر با دامنه و وسعت آلودگی بالا (بیش از ۴۰ بدافزار پرخطر)
- تحلیل روند انتشار شبکه های بات بر اساس اطلاعات سنسورهای هانی نت ملی
- پایش آسیب پذیری ها و تهدیدات مربوط به برنامه های کاربردی، سیستم عامل، سرویس های شبکه، تجهیزات و نرم افزارهای پرتکرار و ارائه راهکار مقابله (تدوین بیش از ۱۰۰گزارش تحلیلی)
- بررسی پورتال های مهم کشور و شناسایی آسیب پذیریهای بیش از ۱۰پورتال مهم کشور و ارائه راهکار در جهت رفع آسیب پذیریهای مربوطه

شبکه تعاملی اطلاع رسانی مرکز ماهر

❑ راه اندازی شبکه تعاملی اطلاع رسانی مرکز ماهر :

مرکز ماهر به منظور اطلاع رسانی سریع و ایمن در زمان بروز رخداد در کوتاهترین زمان و حتی به دورترین مناطق کشور اقدام به راه اندازی یک سامانه تعاملی اطلاع رسانی نموده است.

- عضویت بیش از ۱۸۰۰ دستگاه دولتی، عمومی و نظارتی (تا کنون)
- ۱۰۰هشدار امنیتی حاوی جدیدترین آسیب پذیری ها و تهدیدات شناسایی شده و آماده باش ها در حوزه افتا
- تهیه ۲۴ بولتن خبری محرمانه در حوزه افتا

مدیریت و پاسخگویی به رخدادهای رایانه ای

- ایجاد تیم مدیریت و پاسخگویی به رخدادهای رایانه ای در مرکز ماهر

  - پاسخگویی به بیش از ۱۵۰۰ تماس در موارد مختلف، از جمله گزارش حملات مختلف همچون فیشینگ و یا راهکارهای پاکسازی بدافزارها

  - پاسخگویی به بیش از ۱۱۰۰ رخداد گزارش شده به مرکز در سال ۹۱

  - پاسخگویی به بیش از ۳۰ رخداد با حساسیت بالا در سال ۹۱

پرتال مرکز ماهر (www.Certcc.ir)

پرتال مرکز ماهر جهت دسترسی عموم مردم (کلیه سازمان ها و شرکت ها و کاربران خانگی) راه اندازی گردیده است با هدف ارائه آخرین اخبار و اطلاعات در حوزه امنیت فضای تبادل اطلاعات

- بیش از ۱۷۵۰ راهنمایی امنیتی
- ۹۷۰ خبر امنیتی
- ۹۰ گزارش تحلیلی
- ۱۰۰ مقاله در حوزه امنیت
- و ۱۴۰ گزارش فنی و راهکار پاکسازی بدافزار

سازمان فناوری اطلاعات ایران
مرکز ماهر
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای
وزارت ارتباطات و فناوری اطلاعات

www.Certcc.ir

04 آذر 1391 ساعت 21:12

اطلاعیه مرکز ماهر در خصوص بدافزار win32.narilam

پیرو اخبار منتشر شده اخیر در رابطه با شناسایی بدافزاری توسط شرکت سایمنتک تحت عنوان win32.narilam ، با هدف آسیب رسانی به پایگاههای داده سیستم های مالی در ایران، مرکز ماهر به اطلاع می رساند بر خلاف اخبار منتشر شده این بدافزار در سال 89 (2010) توسط مراکزوشرکتهای فعال در حوزه امنیت فناوری اطلاعات کشور ...

اخبار | هشدار امنیتی | حادثه امنیتی | آسیب پذیری | اصلاحیه امنیتی

- کشف بدافزار ... HTML جاوا را هدف قرار داده است
- صفحات ... CC ...
- به روز رسانی بزرگ ... میکند ... حملات ... سونگ
- انتشار HTTPS Everywhere برای اینترنت ...

صفحه اخبار | آرشیو اخبار

گزارشات تحلیلی

- وضعیت امنیت در ماه نوامبر 2012 به گزارش سایمانتک
- تهدیدات سه ماهه سوم سال 2012 به گزارش McAfee - قسمت دوم
- تهدیدات سه ماهه سوم سال 2012 به گزارش McAfee - قسمت اول
- بدافزارهای سه‌ماهه سوم 2012 به گزارش Kindsight – قسمت دوم
- بدافزارهای سه‌ماهه سوم 2012 به گزارش Kindsight – قسمت اول
- وضعیت امنیت در ماه اکتبر 2012 به گزارش سایمانتک
- وضعیت اینترنت در سه ماهه دوم 2012

تازه ها | دسته بندی موضوعی

مقالات

- برنامه‌نویسی امن با زبان جاوا - آشنایی
- چهار فاکتور برای جلوگیری از جاسوسی سایبری
- بهبود عملکرد BitLocker در ویندوز سرور 2012 و ویندوز 8– قسمت اول
- پشتیبان گیری از داده ها
- مدل ها و مکانیزم های کنترل دسترسی
- آیا سایت شما هدف حملات خودکار است؟
- آیا استفاده از جاوا خطرناک است؟

تازه ها | دسته بندی موضوعی

اخبار از سایتهای دیگر

- دفع حمله ویروس استاکس نت به تاسیسات زیربنایی هرمزگان
- جی‌میل بی‌دلیل قطع شد
- استفاده از آندروید به طور رسمی از سوی توکیا تکذیب شد
- کابوس استاکس نت پایان می یابد؟
- ویروس فلیم علیه فرانسه به کار گرفته می شود!

بیشتر...

معرفی ماهر

- اهداف و ماموریت
- ساختار
- نقشها و وظایف
- کمیته مشورتی
- دانلود بروشور
- تماس با ما

اطلاعات پورتال

- اخبار
- راهنماییهای امنیتی
- گزارشات تحلیلی
- مقالات
- امنیت در رایانه شما
- امنیت درگوشی های تلفن همراه
- همایشها
- بولتن خبری
- پرسش و پاسخ
- سایتهای مرتبط

خدمات

- گزارش حادثه
- گزارش آسیب پذیری
- مشاوره

مجموع بازدیدها : 7157107
تعداد بازدید امروز : 5195
تعداد بازدید دیروز : 9582
آخرین به روزرسانی : 09/10/1391 11:16

OIC-CERT
Computer Emergency Response Team

تهدیدات جاری

- شناسایی گونه جدیدی از بدافزار با قابلیت Wipe
- اطلاعیه مرکز ماهر در خصوص بدافزار win32.narilam

تازه ها | دسته بندی موضوعی

آزمایشگاه بدافزار ماهر

- گزارش استان های آلوده به بدافزار
- راهنمای پاکسازی بدافزار

امنیت در رایانه شما

- تاثیر بدافزارها بر روی رایانه و روش‌های مقابله با آن
- حفظ امنیت موبایل در سال 2012

تازه ها | دسته بندی موضوعی

... (Honey Pot)

- ...رفی حسگرها و سنسورهای ...ردآوری کننده بدافزارها
- مقالات مربوط به هانی پات

تازه ها

راهنمایی های امنیتی

- آسیب پذیری سرریز بافر در VLC Media Player
- به روز رسانی SUSE برای opera

تازه ها | دسته بندی موضوعی

همایشها

- همایش امنیت فضای تبادل اطلاعات
- دومین همایش منطقه ای امنیت فضای تبادل اطلاعات

تازه ها | دسته بندی موضوعی

172.16.105.208
سرعت شما هم اکنون
2815 KB/s
سرعت بارگذاری
866 KB/s
آزمون پیشرفته

راه اندازی تیم های گوهر دستگاهی

- همکاری در راه‌اندازی گروه واکنش هماهنگ رخداد رایانه ای (گوهر) شرکت ارتباطات زیرساخت
- اقدام در خصوص راه اندازی گروه واکنش هماهنگ رخداد رایانه ای (گوهر) در ستاد وزارت ارتباطات و فناوری اطلاعات
- تهیه طرح تفضیلی پیاده‌سازی گوهرهای استانی شامل استانهای بوشهر، قم، مازندران بعنوان پایلوت کشور
- اقدام در خصوص تهیه طرح تفضیلی راه‌اندازی گروه واکنش هماهنگ رخداد رایانه ای (گوهر) در ۴ دستگاه حیاتی کشورشامل وزارت راه و شهرسازی- وزارت علوم و تحقیقات فناوری- وزارت جهاد کشاورزی-سازمان انرژی اتمی
- راه‌اندازی گروه واکنش هماهنگ رخدادهای رایانه ای (گوهر) در منطقه جنوب کشور با محوریت استان فارس

تعاملات ملی و بین المللی مرکز ماهر

- چاپ ۱۳ عنوان کتاب و برگزاری ۶ همایش در حوزه افتا در سال ۹۰ و ۹۱
- تعامل با مراکز **CERT** کشورهای منطقه و مراکز **CERT** بین المللی در خصوص تبادل آخرین اطلاعات مربوط به تهدیدات سایبری
- عضویت در سازمان **OIC-CERT** (**CERT** کشورهای اسلامی)
- عضویت در سازمان **IMPACT** و تعامل در خصوص انتقال تجربیات و دانش فنی
- رفع تهدیدات با منشا داخلی پیرو درخواست مراکز **CERT** خارجی

CERT: Computer Emergency Response Team

OIC-Cert : Organization of Islamic Cooperation CERT

IMPACT : International Multilateral Partnership Against Cyber Threats

خدمات قابل ارائه

توسط

مـــرکـــز مـــاهـــــــر

خدمات قابل ارائه توسط مرکز ماهر

- توسعه سنسورهای شناسایی بدافزار در سازمانها (هانی پات، اسپم پات، هانی کلاینت و غیره) و ارائه گزارشات تحلیلی به سازمان ها
- بررسی نمونه فایل های مشکوک ارسالی از سوی سازمان ها و شرکت های مختلف و ارائه راهکار، ابزار پاکسازی و رفع آلودگی آنها
- تحلیل رخدادهای امنیت فضای تولید و تبادل اطلاعات در سازمانها از طریق اعزام تیم امداد
- مشاوره در خصوص رصد، پشتیبانی و مشاوره افتا بصورت تخصصی و دسترسی به تهدیدات، آسیب پذیری ها و راهکارهای امنیتی مرتبط با هر صنعت
- راه اندازی تیم های گوهر سازمانی
- برگزاری دوره های آموزشی تخصصی در حوزه امنیت فناوری اطلاعات

- روش های پیشگیری و مقابله با حملات هدفمند سایبری
- آشنایی با تحلیل بدافزار
- آشنایی با سرویس ها، خدمات و پیاده سازی مراکز گوهر
- مدیریت آسیب پذیری ها و رخدادهای رایانه ای سازمانی
- امنیت حسگرهای اطلاعاتی


اللهم صل علی محمد و آل محمد