دوره آموزشی راه‌اندازی گوهر سازمانی

APA- IUTcert 602

گروه واکنش هماهنگ رخداد رایانه‌ای (گوهر) نام دیگر گروه‌های CSIRT) Computer Security Incident Response Team)بوده و به گروهی اطلاق می‌گردد که در یک سازمان وظیفه **جلوگیری**، **رسیدگی** و **مقابله** با کلیه حوادث امنیتی صورت گرفته در فضای تولید و تبادل اطلاعات را برعهده دارد. در این دوره کوتاه مدت مدیریتی، به معرفی گوهرهای سازمانی پرداخته می‌شود. سرفصل مطالب این دوره عبارتند از:

- آشنایی با انواع مراکز امداد امنیت رایانه‌ای
- معرفی تشکیلات و تخصص‌های مورد نیاز
- معرفی نحوه راه‌اندازی و مدیریت مراکز امداد امنیت رایانه‌ای
- معرفی سرویس‌ها و خدمات

Computer Security Incident Response Team (CSIRT)

Part of the Network security glossary:

A Computer Security Incident Response Team (CSIRT, pronounced "see-sirt") is an organization that receives reports of security breaches, conducts analyses of the reports and responds to the senders. A CSIRT may be an established group or an ad hoc assembly.

There are various types of CSIRTS. An internal CSIRTs is assembled as part of a parent organization, such as a government, a corporation, a university or a research network. National CSIRTs (one type of internal CSIRT), for example, oversee incident handling for an entire country. Typically, internal CSIRTS gather periodically throughout the year for proactive tasks such as DR testing, and on an as-needed basis in the event of a security breach. External CSIRTs provide paid services on either an on-going or as-needed basis.

CERT (Computer Emergency Readiness Team) lists the following among the roles of CSIRT members:

- Manager or team lead.

- Assistant managers, supervisors, or group leaders.
- Hotline, help desk, or triage staff.
- Incident handlers.
- Vulnerability handlers.
- Artifact analysis staff.
- Platform specialists.
- Trainers.
- Technology watch.

The specific services provided vary from one CSIRT to another. A computer security incident can involve a real or suspected breach or the act of willfully causing a vulnerability or breach. Typical incidents include the introduction of viruses or worms into a network, DoS (denial of service) attacks, unauthorized alteration of software or hardware, and identity theft of individuals or institutions. Hacking in general can be considered a security incident unless the perpetrators have been deliberately hired for the specific purpose of testing a computer or network for vulnerabilities. (In that case, the hackers can form part of the CSIRT, in a preventive role.) CSIRTs may provide proactive services, such as end-user security training, besides responding to incidents.

Response time constitutes a critical consideration in assembling, maintaining and deploying an effective CSIRT. A rapid, accurately targeted, and effective response can minimize the overall damage to finances, hardware, and software caused by a specific incident. Another important consideration involves the ability of the CSIRT to track down the perpetrators of an incident so that the guilty parties can be shut down and effectively prosecuted. A third consideration involves "hardening" of the software and infrastructure to minimize the number of incidents that take place over time.

Alternate terms for CSIRT include CIRC (Computer Incident Response Capability), CIRT (Computer Incident Response Team), IRC (Incident Response Center or Incident Response Capability), IRT (Incident Response Team), SERT (Security Emergency Response Team) and SIRT (Security Incident Response Team). Internal CSIRTs often use one of the terms along with an identifier. The national CSIRT in the United States, for example, is US-CERT.

This was last updated in August 2012

Contributor(s): Stan Gibilisco

Posted by: Margaret Rouse

Related Terms

Definitions

- web server security

  - Web server security is the protection of information assets that can be accessed from a Web server. *(SearchSecurity.com)*

- Common Vulnerabilities and Exposures (CVE)

  - Common Vulnerabilities and Exposures (CVE) provides unique identifiers for publicly known security threats. *(SearchFinancialSecurity.com)*

- evil twin

  - An evil twin, in security, is a rogue wireless access point that masquerades as a legitimate hot spot. *(SearchSecurity.com)*

Glossaries

- Network security

  - Terms related to network security, including definitions about intrusion prevention and words and phrases about VPNs and firewalls.

- Internet applications

  - This WhatIs.com glossary contains terms related to Internet applications, including definitions about Software as a Service (SaaS) delivery models and words and phrases about web sites, e-commerce ...

Dig Deeper

Continue Reading About Computer Security Incident Response Team (CSIRT)

- Carnegie Mellon's Software Engineering Institute explains how a CSIRT works, and how to effectively organize, maintain, and deploy one.

People Who Read This Also Read…

- Defining an incident response process when short staffed
- CIRT is an essential security strategy for every Indian organization
- NIST incident response plan: Four steps to better incident handling
- Developing an incident response plan
- How to assign responsibilities for a CSIRT

ویستا فن‌آوری فردا
مشاوره، اجرا، تامین و ارائه تجهیزات
آموزش دوره های تخصصی IT، مخابرات، مدیریت
شناسه ملی: ۱۴۰۰۷۲۹۶۴۲۹

- همچنین قبل از ثبت‌نام حتماً نسبت به مطالعه دقیق سرفصل دوره‌ها و پیش‌نیاز آن‌ها اقدام نمائید.

دوره‌های تخصصی آزمایشگاه تخصصی آپا در تابستان 1393

کد دوره	عنوان دوره برای دریافت سرفصل دوره‌ها برروی عنوان آن کلیک کنید.	مدت زمان	زمان برگزاری	شهریه دوره
APA 91	امنیت برنامه‌های کاربردی تحت وب مبتنی بر PHP	24 ساعت	شنبه و سه‌شنبه ساعت 18 - 20	2000000 ریال
APA 92	امنیت برنامه‌های کاربردی تحت وب مبتنی بر .NET	20 ساعت	یک‌شنبه و چهارشنبه ساعت 18 - 20	1800000 ریال
APA 93	استراتژی امنیتی دفاع در عمق (Defense in depth)	12 ساعت	دوشنبه ساعت 16 - 18	1200000 ریال
APA 94 APA 94-2	آزمون نفوذپذیری شبکه‌های رایانه‌ای	24 ساعت	یک‌شنبه و چهارشنبه ساعت 16 - 18 ساعت 14 - 16	2400000 ریال
APA 95	طراحی، پیکربندی و امنیت در بستر مجازی شبکه	30 ساعت	شنبه و سه‌شنبه ساعت 16 - 18	3000000 ریال
APA 96	امنیت شبکه‌های محلی بی‌سیم	16 ساعت	دوشنبه ساعت 18 - 20	1400000 ریال
APA 97	جرم‌یابی قانونی شبکه و جرم‌یابی قانونی حافظه‌ی سیستم عامل ویندوز	28 ساعت	شنبه و سه‌شنبه ساعت 14 - 16	2500000 ریال
APA 98	تحلیل بدافزار	18 ساعت	یک‌شنبه و چهارشنبه ساعت 14 - 16	1600000 ریال
APA 99	**متقاضیان آزمون پایان دوره (شرکت‌کنندگان قبلی دوره‌های آزمایشگاه)**			300000

آدرس: خیابان بهشتی، بعداز وزرا
ساختمان کشتیرانی، شماره ۳۰۳
کد پستی: ۱۵۱۱۶۱۶۱۱۱

۸۸۵۵۴۹۶۳-۸۸۵۰۸۰۸۰
www.vistaac.com
Info@vistaac.com

ویستا فن‌آوری فردا
مشاوره، اجرا، تامین و ارائه تجهیزات
آموزش دوره های تخصصی IT، مخابرات، مدیریت
شناسه ملی: ۱۴۰۰۷۲۹۶۴۲۹

مجنین برای اولین بار برخی دوره‌ها با هدف زمان‌بندی بهتر برای شرکت‌کنندگان، در پایان هفته نیز برگزار می‌شود.

(لطفاً بخش‌های مختلف این فراخوان از جمله اطلاعات دوره‌ها، آزمون انتخابی پایان دوره، صدور گواهی‌نامه و نحوه ثبت‌نام را به‌صورت کامل مطالعه نمائید.)

دوره‌های تخصصی آزمایشگاه تخصصی آپا در زمستان 1392				
کد دوره	عنوان دوره *	مدت زمان	زمان برگزاری	شهریه دوره
APA 81	امنیت برنامه‌های کاربردی تحت وب (PHP)	22 ساعت	شنبه و چهارشنبه ساعت 16 - 14	1600000 ریال
APA 82	پیکربندی امن تجهیزات شبکه (مقدماتی)	20 ساعت	شنبه و دوشنبه ساعت 18 - 16	1600000 ریال
APA 83	پیکربندی امن تجهیزات شبکه (مقدماتی)	20 ساعت	چهارشنبه ساعت 20 - 16	1600000 ریال
APA 84	پیکربندی امن تجهیزات شبکه (پیشرفته)	20 ساعت	شنبه و دوشنبه ساعت 20 - 18	1600000 ریال
APA 85	پیکربندی امن تجهیزات شبکه (پیشرفته)	20 ساعت	پنج‌شنبه ساعت 20 - 16	1600000 ریال
APA 86	آزمون نفوذپذیری شبکه‌های رایانه‌ای	24 ساعت	یک‌شنبه و سه‌شنبه ساعت 18 - 16	1800000 ریال
APA 87	آزمون نفوذپذیری شبکه‌های رایانه‌ای	24 ساعت	پنج‌شنبه ساعت 8 الی 14	1800000 ریال
APA 88	امنیت شبکه‌های محلی بی‌سیم	20 ساعت	یک‌شنبه و سه‌شنبه ساعت 16 - 14	1400000 ریال
APA 89	تحلیل بدافزارها (مقدماتی)	22 ساعت	یک‌شنبه و سه‌شنبه ساعت 20 - 18	1600000 ریال
APA 90	**متقاضیان آزمون پایان دوره (شرکت‌کنندگان قبلی دوره‌های آزمایشگاه)**			300000 ریال

آدرس:خیابان بهشتی، بعداز وزرا
ساختمان کشتیرانی،شماره ۳۰۳
کد پستی: ۱۵۱۱۶۱۶۱۱۱

۸۸۵۵۴۹۶۳-۸۸۵۰۸۰۸۰
www.vistaac.com
Info@vistaac.com

همچنین قبل از ثبت‌نام حتماً نسبت به مطالعه دقیق سرفصل دوره‌ها و پیش‌نیاز آن‌ها اقدام نمائید (برای دریافت فایل pdf سرفصل دوره‌ها بر روی عنوان آن‌ها کلیک نمائید).

دوره‌های تخصصی آزمایشگاه تخصصی آپا در زمستان 1393				
کد دوره	عنوان دوره	مدت زمان	زمان برگزاری	شهریه دوره
APA 101	امنیت برنامه‌های کاربردی تحت وب مبتنی بر PHP	24 ساعت	یک‌شنبه و سه‌شنبه ساعت 16 - 14	2400000 ریال
APA 102	پیکربندی امن تجهیزات شبکه (مقدماتی)	20 ساعت	یک‌شنبه و سه‌شنبه ساعت 18 - 16	2000000 ریال
APA 103	پیکربندی امن تجهیزات شبکه (پیشرفته)	20 ساعت	یک‌شنبه و سه‌شنبه ساعت 20 - 18	2000000 ریال
APA 104	آزمون نفوذپذیری شبکه‌های رایانه‌ای	24 ساعت	روزهای زوج ساعت 20 - 18	2800000 ریال
APA 105	طراحی، پیکربندی و امنیت در بستر مجازی شبکه	30 ساعت	روزهای زوج ساعت 18 - 16	3600000 ریال
APA 106	سامانه‌های VoIP و پیکربندی امن آن	30 ساعت	روزهای زوج ساعت 19 - 16	4000000 ریال
APA 107	بستر نرم‌افزاری Yii.1	22 ساعت	شنبه و دوشنبه ساعت 16 - 14	2400000 ریال
APA 109	متقاضیان آزمون پایان دوره (شرکت‌کنندگان قبلی دوره‌های آزمایشگاه)			300000 ریال

آزمايشگاه تخصصي آپا دانشگاه فردوسي مشهد در راستاي اهداف آگاهي‌رساني و پشتيباني در زمينه امنيت فناوري اطلاعات و ارتباطات، دوره‌هاي آموزشي تخصصي را در زمستان 1393 برگزار مي‌كند .اين دوره‌ها در عنوان‌هاي امنيت برنامه‌هاي كاربردي تحت وب مبتني برPHP، پيكربندي امن تجهيزات شبكه)مقدماتي و پيشرفته)، آزمون نفوذپذيري شبكه‌هاي رايانه‌اي، طراحي، پيكربندي و امنيت در بستر مجازي شبكه، سامانه‌هاي VoIP و پيكربندي امن آن، و بستر نرم‌افزاري Yii.1 برگزار مي‌شود .تاريخ شروع دورها از 11 بهمن 1393 است و علاقه‌مندان تا 9 بهمن مي‌توانند براي ثبت‌نام اقدام نمايند. براي دريافت سرفصل دوره‌ها و اطلاع از جزئيات ثبت‌نام و برگزاري مي‌توانيد به نشاني اينترنتي

ومین دوره رقابت های هکرها و نفوذگرها با عنوان "نفوذ و دفاع در فضای مجازی" در خردادماه سال آینده از سوی دانشگاه صنعتی .شریف برگزار می شود

مرکز آگاهی رسانی، پشتیبانی و امداد حوادث رایانه ای (آپا) دانشگاه صنعتی شریف با حمایت مالی و تخصصی مرکز ماهر سازمان فناوری اطلاعات ایران و پشتیبانی عملیاتی شاخه دانشجویی انجمن رمز ایران به منظور آگاهی رسانی، آموزش و ترویج فرهنگ .امنیت فضای تبادل اطلاعات اقدام به برگزاری دومین دوره رقابت هکرها کرد

این دوره از رقابت های نفوذ و دفاع در فضای مجازی که در خرداد ماه سال آینده برگزار می شود، شرکت کنندگان در سه محور " هک و نفوذ"، " طراحی پوسترها و کاریکاتورهای ترویجی" و " روشهای کاربردی نوین و خلاقانه در نفوذ و دفاع" به رقابت می .پردازند

در بخش مسابقه هک و نفوذ، تیمهای شرکت کننده، در دو مرحله مقدماتی و نهایی به رقابت خواهند پرداخت. در هر دو مرحله ، کشف شواهد (Web Attack) ، نفوذگری در وب(Trivia) تیمهای شرکت کننده به چالشهای مطرح در حوزه دانش عمومی امنیت و رمزنگاری (Exploiting) ، نوشتن کد سوء استفاده(Reverse Engineering) ، مهندسی معکوس(Forensics) الکترونیکی .پاسخ خواهند داد (Cryptography)

در بخش معرفی روشهای کاربردی نوین و خلاقانه، مقاله های تخصصی برگزیده شرکت کنندگان ارائه می شود. ارائه آخرین .روشهای کاربردی نوین و خلاقانه در نفوذ و دفاع در فضای مجازی و تبادل دانش در این حوزه، هدف اصلی این بخش است

متقاضیان برای شرکت در این بخش از مسابقات نفوذ و دفاع در فضای مجازی تا 22 اردیبهشت ماه سال 91 مهلت دارند تا مقالات .خود را ارسال کنند

نمایش پوسترهای ارسالی شرکت کنندگان در حوزه امنیت از دیگر بخشهای این رقابتها است. طراحی پوستر یا کاریکاتورهایی موثر، جهت آگاهی رسانی و فرهنگ سازی در زمینه امنیت در سطح جامعه و مخاطبین عام، هدف اصلی برگزاری این بخش از رقابتها .است

طرحهای برتر در این بخش، بر اساس نظرات و رای بازدید کنندگان نمایشگاه این آثار در روزهای برگزاری مجموعه رقابتها .انتخاب می شوند. آخرین مهلت ارسال آثار تا 2 اردیبهشت ماه 91 تعیین شده است

.مسابقه اصلی این رقابت ها و اهدای جوایز به منتخبین بخشهای در روز چهارشنبه 3 خرداد ماه در دانشگاه شریف خواهد بود