

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.

Date:		May 3 - 5, 2004
Event:	Training	Anti-Hacking for Computer Forensics
Location:		Arlington, Virginia
Description of Event:		<p>How to detect the crime, track the criminal, and assemble the evidence.</p> <p>The reported incidents of computer crime have more than doubled in the last year. Which just proves that you — no matter how robust your security strategy and practices are — need to know exactly how computer crimes are committed, how to assemble the evidence, and work with law enforcement for prosecution. In this 3 day class, you will discover the different types of computer threats and crimes, and investigate computer crime prevention techniques. You will find out how to identify, investigate, capture, analyze, preserve and process evidence. In this in-depth "crime" course, you'll gain the knowledge and tools you need to create a corporate computer crime policy. You will learn how to build the management response, technical, and tactical teams. You'll learn the laws regarding computer crime, and how to tell if your company has been a victim. You'll examine best practices for incident response. You'll also learn how to coordinate your efforts with law enforcement and maintain evidence chain of custody.</p> <p>When you're finished, you'll know what computer crime is, and isn't... and how to safeguard your organization's vital technology assets.</p> <p>Key topics:</p> <ul style="list-style-type: none"> • The basics of computer forensics • Proven investigative strategies • Tracking an offender on the Internet and intranets • Tips and techniques for incident response • Proper handling of evidence • Working with law enforcement
Cost:		\$1995
Time:		8:30 am – 4 pm
Registration		https://ssl20.pair.com/secuniv/reg.php

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.

Date:		May 3 – 5, 2004
Event:	Training	Anti-Hacking for Trojans, Viruses, Patch Management & Incident Response
Location:		Arlington, Virginia
Description of Event:		<p>How to manage viruses, trojans and malware... so they don't manage you.</p> <p>From Klez to SQLSnake Worms. The impact of Zero-day viruses to are nothing compared to what trojans are doing on your networks everyday. This 3-day class is <i>the only</i> hands-on class where you login <i>live</i> to worms, viruses, and trojans without the risk of infecting your network. NIMDA, CODE RED and others, learn what they do, work with the best in the industry. Use Confidence On-line, NORTON, SOPHOS, MCAFEE and other virus & anti-trojan software in Hands-On labs. Learn how the process of incident recovery protects your assets and enforces policy. Don't risk your corporate reputation or be a part of the \$895 M loss lost last year from these debilitating incidents. Live patch management demos detail patch management processes, host scans and how to mitigate risk. You'll examine attacks from both the enterprise and hacker points of view. You'll uncover the best tools and techniques for eradication, patching and recovery. You'll uncover the strengths and weaknesses of current anti-virus and anti-trojan software, and become an expert at separating false alarms and website spoofing and phishing from actual incidents and identity theft. You'll integrate new knowledge with past anti-virus experience to define your organization's recovery strategy. SU labs are designed to give you a chance to apply techniques learned in the class by actually using Windows-based trojan key loggers, worms and viruses while learning solutions for protecting internal and external users from the trojan and virus invasion. You will create a Patch Management Policies Program roadmap that works to contain and mitigate risk using PatchLink Update and establish your "network patching roadmap".</p> <p>In short, you'll learn everything you need to know to evaluate, create, and implement the virus & trojan incident management program to protect your uses and company and keep your organization up and running.</p> <p>Key topics:</p>

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.

		<ul style="list-style-type: none"> • Evolution of malware and incident management • Mitigate site spoofing & phishing • False alarms vs. real threats from virus & trojans • Filtering as effective containment technique • Discover the best tools and techniques for eradication, patching and recovery • Pros and cons of current anti-virus & anti-trojan software and techniques • Define a recovery strategy • Establish measurable goals for patch management and compliance
Cost:		\$1995
Time:		8:30 am – 4 pm
Registration :		https://ssl20.pair.com/secuniv/reg.php
May 5, 2004		
Date:		May 5, 2004
Event:	Webcast	Bluetooth Wireless
Description of Event:		Learn the latest on Bluetooth technology.
Cost:		free
Time:		1 P.M.
Website:		http://www.sans.org/webcasts/show.php?webcastid=90473
May 5, 2004		
Date:		May 5, 2004
Event:	Seminar	Global Cyber-Security: Confronting New and Reemerging Threats
Location:		Choate Room, Carnegie Endowment for International Peace 1779 Massachusetts Ave., NW Washington, D.C.
Description of Event:		A variety of speakers imminent in their field will discuss the matter of cyber-security.
Time:		5:30-7:00 pm
Registration :		jl287@georgetown.edu
Date:		May 6, 2004

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.

Event:	Webinar	Data Sharing-The Security Challenge
Location:		Online- Online events are simulcast over the web and a toll-free, call-in voice line. The presenter's computer broadcasts a live discussion or demonstration over the Internet, while the audio portion of the seminar is hosted over the toll-free conference call.
Description of Event:		A discussion focused on "Data Sharing: The Security Challenge." E-Gov, X-Gov, intergovernmental: Call it what you will, a fundamental challenge to its success is the ability to securely share data electronically with anyone, anywhere. Join us for this discussion of one of the most pressing topics in government IT. Explore key issues around security for e-government initiatives. Identify the basic components necessary for secure data sharing. Discuss real pilot initiatives and how to create a solution for your agency
Time:		11 a.m.
Cost:		Free
Registration :		http://www.macromedia.com/v1/company/events/onlineevents/gov_convocfm
May 3-7, 2004		
Date:		May 3-7, 2004
Event:	Security Booth	Spotlight on Security, Security Booth at Career Zone
Location:		FSA Career Zone, 7 th Floor
Description of Event:		FSA Security and Privacy Team is setting up a security booth in the Career Zone. The booth will feature training materials from the Security Library and information on security master degree programs from local universities.
Cost:		Free
May 12, 2004		
Date:		May 12, 2004
Event:	Training	Social Engineering Training
Location:		FSA Career Zone

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.

Description of Event:		FSA Security and Privacy Team will offer special training on social engineer through the Career Zone,
Cost:		Free
Time:		10 am- noon
Registration :		
Date:		May 10 - 12, 2004
Event:	Training	Architecture Security
Location:		Arlington, Virginia
Description of Event:		<p>How to plan and execute a security architecture that matches your technology infrastructure from top to bottom.</p> <p>This 3-day class brings the whole network together and delivers a secure infrastructure. Merge today's security technologies into your network with the assurance that your layering defense tactics and providing early warning systems. Bring together the separate, tactical, diverse parts of your network with the services, mechanisms, and objects that reflect the security policies, business functions, and technologies into a process involving risk assessment, policy, awareness, technology and security management, and audit functions. Building a security architecture involves close examination of current business processes, technical capability, information security documentation, and existing risk. Students will leave this class with a document template outlining a best practice for an information security architecture framework.</p> <p>Key topics:</p> <ul style="list-style-type: none"> • Defined policy and practice — including audit programs and compliance metrics • Physical security mechanics and human interaction • Network perimeter protection and countermeasures • Enterprise information access management — including remote access, network and data exposure, network account control, audit and accounting capability • Application development security • Network and platform systems safeguarding • Data availability and reliability issues

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.

		• Disaster recovery and contingency planning
Cost:		\$1495
Time:		8:30 am – 4 pm
Registration :		https://ssl20.pair.com/secuniv/reg.php
Date:		
		May 11-13, 2004
Event:	Conference	Technet International 2004
Location:		Washington, D.C. Convention Center
Description of Event:		FREE Registration! TechNet International 2004, "Combating Emerging Threats" is one of the largest C4I events in the nation. Professional development opportunities include: panel sessions on mobile & wireless technology security, emerging threats vs. critical infrastructure, and business continuity & emergency management; featured speakers, including Gen Myers, Chairman, JCS; Gen Eberhart, Commander NORAD & Commander Northern Command; The Honorable Michael Wynne, Acting Under Secretary of Defense for ATL; LtGen Shea, J-6, The Joint Staff; and GEN Franks (Ret.), former Commander, US Central Command.; PDC mini-courses; career transition seminar; and small business opportunity workshop.
Cost:		Free
Registration :		http://www.technet2004.org/
Date:		
		May 17 - 21, 2004
Event:	Training	Intrusion Detection II: Systems to Monitor Your Network
Location:		Arlington, Virginia
Description of Event:		Intrusion detection systems (IDS) give you the ability to detect when your networks or systems are being probed or attacked, or if they have been compromised in some manner. This critical monitoring capability is an essential component in any comprehensive enterprise network security program. IDS

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.

		<p>systems, however, have a reputation for being difficult and expensive to deploy, and can be time-consuming to properly manage. Many organizations that have implemented IDS in their infrastructures have a hard time developing the adequate processes for tuning the systems, monitoring their massive amounts of output, and responding to critical security events in a timely manner.</p> <p>In this 5 -day, hands-on class you will cover the ins and outs of intrusion detection systems. You will learn how IDS operates and the trade-offs between host-based and networked-based intrusion detection systems. You will discover methods for integrating and managing a network of IDS components; how to manage and administer IDS; where to position IDS sensors; what key freeware and commercial IDS tools are best where on your network; and how to determine if IDS should be outsourced or kept in-house. Using hands-on exercises, you will set up your own real-time IDS sensors. You will also detect and analyze an assortment of live hacker attacks and related probes and why you can't rely on IDS as your sole monitoring component. You will learn the difference between anomaly based and Signature based IDS that promise to make intrusion detection systems easier to manage and more effective as part of your information security strategy.</p>
Cost:		\$2495
Time:		8:30 am – 4 pm
Registration :		https://ssl20.pair.com/secuniv/reg.php

Date:		May 25, 2004
Event:	Training	Security and Privacy Awareness Day
Location:		FSA Learning Center at FSA Lobby Rooms 1101 A&B, 1102
Description of Event:		This is an all day security and privacy event with special guest speakers discussing the latest in security and fun activities.
Time:		8:30-4 pm

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.

Cost:		Free
Date:		May 24 - 28, 2004
Event:	Training	Network Penetration Testing Methods
Location:		Arlington, Virginia
Description of Event:		<p>How to look at your network through a hacker's eyes... and close the doors on unauthorized penetration.</p> <p>In this five-day course — the most robust and in-depth of its kind — you'll gain a hacker's-eye-view of your network and technology infrastructure. You'll uncover the hackers' favorite penetration techniques and how to protect against them. You'll learn how to gather viable data on your network's vulnerabilities using tools like Saint, NMAP, Nessus, SOLARWINDS, App Detective and more. You will cover techniques for assessing the security posture of firewalls and other perimeter defenses, and explore exploits that can breach firewalls in specific configurations. You will get proven tips on building a powerful network testing tool kit using both freeware and commercial tool alternatives so that you can frequently test for exploited TCP/IP network and computing platform-specific security vulnerabilities.</p> <p>You'll analyze the results, prioritize the high-value targets, and turn it all into a workable action plan in class. You will examine related vulnerabilities in the underlying operating system and connected TCP/IP application services. You will learn how to use commercial and freely available tools to test Web server configurations and uncover weaknesses in Web servers and browsers. You'll also learn how to build and maintain a target list, perform remote and host assessments in our Hands-On Labs!</p> <p>After all this, it's the hackers who will have to beware when it comes to your network.</p>
Cost:		\$2495
Time:		8:30 am- 4 pm
Registration		https://ssl20.pair.com/secuniv/reg.php

Security Events Calendar for May

For more information and to see previous calendars, go to http://fsanet.ed.gov/cio/products/it_security_portal/ and view the Events calendar on the left hand side of the page.