May 2016 SANS Cyber Security Webcasts

Date	Title	Description	URL
May 10, 2016	Connecting the Dots Between Your Threat Intelligence Tradecraft and Business Operations	Cyber threat intelligence can help you guide more informed risk management decisions. With strategic and operational threat intelligence you can better understand your weaknesses and strengths, focus on the key problem areas for your business, and know the most optimal solutions based on your limited resources.	http://www.sans.org/u/fzQ
May 11, 2016	This Phish Goes to 11	Testing your users and systems with generic phishing pretexts use to be enough, but now attackers are using open-source intelligence to customize their phishing campaigns.	http://www.sans.org/u/hC8
May 11, 2016	Using the Critical Security Controls to Prevent Ransomware in Healthcare	In this presentation, James Tarala, a Senior Instructor with the SANS Institute and over 15 years of healthcare IT experience will discuss practical steps organization can take to stop this threat. Using the CIS Critical Security Controls as a base, James will cover practical steps organizations can take on systems and network devices to prevent exposure to this rampant attack.	http://www.sans.org/u/gTW
May 12, 2016	Why Train and Who to Train for Education and Government	Join Randy Marchany (CISO, Virginia Tech) and Lance Spitzner (SANS Securing The Human) as they cover the different reasons higher education and state/local government need to conduct training and who they should train.	http://www.sans.org/u/hgL
May 12, 2016	How Aruba leveraged bug bounty hunters to battle test their networking solutions	Today's IT threats demand a more active role in detecting and responding to sophisticated attacks. Defenders can no longer simply press "scan" or hire a penetration test shop to protect their applications. That's where a crowd of bug hunters steps in, possessing the collective creative power to mimic bad hacker behavior in the wild.	http://www.sans.org/u/hgQ
May 13, 2016	Know Abnormal, Find Evil: Windows 10 Memory Forensics Overview	It's time to re-up your skills at hunting evil in memory by learning the new normal, Windows 10. Advance your memory forensics skills for what is expected to be the most rapidly adopted enterprise Windows version of all time. Find out what is new in Windows 10 OS artifacts, browsing history and memory management and how the memory forensic frameworks are keeping up.	http://www.sans.org/u/gAF

May 16, 2016	Shell items, more than meets the eye	It's time to revisit everyones favorite windows forensic resources; shell items. Whether you like to look at them as lnk files, jumplists, shell bags or registry entries they are everywhere. In recent years and in recent versions of Windows we keep finding more data within shell items we can use to make even more correlations and find more evidence!	http://www.sans.org/u/gU1
May 17, 2016	Windows Exploratory Surgery with Process Hacker	In this talk we'll rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS.	http://www.sans.org/u/fVd
May 17, 2016	Practical and Open Source Threat Intelligence	Threat actors are not magic and there is not an unlimited, unique list of threats for every organization. Enterprises face similar threats from similar threat sources and threat actors - so why does every organization need to perform completely unique risk assessments and prioritized control decisions? This presentation will show how specific, community driven threat models can be used to prioritize an organization's defenses - without all the confusion.	http://www.sans.org/u/aum
May 18, 2016	2016 Security Awareness Report	This webcast will be of special interest to anyone involved in planning, deploying or maintaining a security awareness program.	http://www.sans.org/u/hgV
May 18, 2016	Now I have to worry about BYoD and IoT threats?	BYOD and IoT are changing the way employees access your company's data. This webinar will examine how to apply the CIS Critical Controls in an BYOD and IoT world.	http://www.sans.org/u/gU6
May 18, 2016	Scapy and Snort, Packet Peanut Butter and Jelly	This webcast will discuss how Scapy can be combined with Snort to help you craft packets to use with Snort testing. You will also realize the power of Scapy and how it can be used for many different crafting scenarios.	http://www.sans.org/u/aur
May 19, 2016	systemd and You!	The major Linux distros have all embraced systemd as their default system startup environment. So if you're not using systemd now, you will be very soon. How did we get here? Why is systemd better than traditional Linux init or Upstrart? What are the key concepts you need to learn to get up and running with systemd quickly? What are advanced features that you can use to make your environment work better?	http://www.sans.org/u/gUb

May 19, 2016	How to Negotiate a Cyber Insurance Policy	When an enterprise purchases cyber insurance, negotiation can make a big difference. Sometimes you can get more value from the insurer simply by knowing to ask for a particular service or clause in the policy. This webcast will examine key topics to consider in negotiation, and explain some relevant war stories.	http://www.sans.org/u/amM
May 20, 2016	Next Level in Cyber Threat Intelligence Training	We invite you to join lead author Robert M. Lee as he covers core cyber threat intelligence concepts and provides an overview of the FOR578 Cyber Threat Intelligence class. Attend this webcast and be among the first to get a sneak peak of the changes, additions, exciting new tools and tradecraft added into the course.	http://www.sans.org/u/hh0
May 24, 2016	iOS Location Forensics	In this webcast, we will walk you through native iOS databases, plist files and 3rd party applications where this information is kept and tracked. We will also introduce you to scripts created to make data analysis easier by allowing you to do fast data correlation and build historical map of locations.	http://www.sans.org/u/hCd
May 25, 2016	Why So Many Endpoint Attacks Are Still Going Undetected - And What You Can Do About It	Ransomware attacks have surged over the past several months, with large-scale, targeted attacks on the rise. The RSA Incident Response team has recently responded to several of these incidents at client sites. Learn more about attack trends and what your organization can do to detect them.	http://www.sans.org/u/hCi