2016 SANS Analyst Program Editorial Calendar

SANS Institute is the most trusted and by far the largest source for Information Security Training in the world.

Under the direction of Deb Radcliff, two-time Neal Award winning security writer, the SANS analyst program produces leading edge analyst reports on emerging and mission critical topics. Papers are developed by SANS instructors and subject matter experts with their own followings in the SANS community. Through Analyst papers and their associated webcasts, SANS helps sponsors drive topic awareness to a qualified audience of decision makers and influencers who are actively seeking objective data to help their organizations successfully invest resources in successful IT security operations.

Pub Date	Whitepaper / Webcast Project	Associated event	*Starts
	1st quarter		
1/25/2016	SANS First IT Security Spending Survey		9/1/2015
2/1/2016	Continuous Intelligence	Cyber Threat Intelligence February * Washington, DC	11/15/2015
2/15/2016	SANS PCI DSS Update	RSA February/March * San Francisco	12/1/2015
3/3/2016	Security as an Enabler: Business Speak Gets You Further	Security Operations Center (SOC) March * Washington, D.C.	1/5/2016
3/27/2016	Third Annual Endpoint Security Survey	SANS 2016 March * Orlando	10/15/2015
	2nd Quarter		
4/11/2016	Threat Hunting (A New SANS Survey)	Threat Hunting and Incident Response Summit April * New Orleans	11/15/2015
4/30/2016	SANS 4th Annual Application Security Survey		12/12/2015
5/9/2016	3rd Annual Health Care Survey	Healthcare Summit May * Denver OR Phoenix	12/21/2015
6/6/2016	Third Annual Incident Response Survey	Digital Forensics, Incident Response June * Austin	1/15/2016
6/15/2016	SANS 2nd Annual Cyberthreat Intelligence Survey	SANSFIRE June * Washington DC	1/15/2016
	3rd quarter		
7/1/2016	5th Industrial Control Systems Security Survey	Industrial Control Systems July * Houston	2/1/2016
8/1/2016	Getting to Multifactor Authentication		5/15/2016
8/8/2016	Is It Fixed Yet? (A NEW SANS Survey on Vulnerability Remediation)	Blackhat USA August * Las Vegas	3/1/2016
9/1/2016	Active Defense, Offensive Countermeasures and Cyberdeception	Cyber Defense Summit August * Nashville	6/15/2016
9/10/2016	Can You Hear Me Yet? Raising the Security Bars with Quick Wins (A NEW SANS Survey)	Cyber Defense Summit August * Nashville	4/1/2015
9/19/2016	Critical Security Controls Come of Age: A Maturity Model for the Controls		7/5/2016
9/26/2016	SANS' 2nd Survey on Cloud Security	SANS Network Security 2016 September * Las Vegas	4/20/2016
	4th Quarter		
10/10/2016	Infrastructure First! Critical Foundations for Security Maturity	Security Leadership Summit October * Dallas	7/2/2016
10/17/2016	How Mature is Your Security? (A NEW SANS Survey)	Security Leadership Summit October * Dallas	5/15/2016
10/24/2016	3rd Security Analytics Survey		5/20/2016
11/14/2016	What Are Their Vulnerabilities? SANS' 2nd Survey on Continuous Monitoring	SANS Pen Test Hackfest Summit November * Washington DC	6/15/2016
12/10/2016	SANS 3rd Financial Services Survey		7/1/2016

*Note: Start Date and Sponsorship Close Date are the same.

For more information, please contact your SANS Account Manager or vendor@sans.org.
SANS Analyst Program Executive Editor: Deb Radcliff dradcliff@sans.org.

SANS Analyst Program Custom Content Suggestions for 2016

Don't see what you like on the 2016 SANS Analyst Program Editorial Calendar?
Here are some topics SANS has identified for custom sponsorship opportunities in 2016:

Topic Area	Topic	Security Tech/Processes Involved
Anayltics/Intelligence	Continuous Intelligence: What is it? How is it applied? And how does it improve the bottom line?	Machine learning, security analytics, activity monitoring, cyberthreat intelligence (CTI), SIEM, advanced threat protection (ATP), incident response (IR)
	Security Intelligence: How much is too much? And why do you need more than one intelligence provider?	
AppSec	Invulnerable APIs: Testing and securing third-party interfaces	Secure DevOps, app testing and review (static and dynamic analysis, pen testing), RASP, WAF, vulnerability scanning
	RASP: Building web apps that can protect themselves without getting in their own way	
	DevOps: Who has time for security in a world of continuous code delivery?	
Connected Devices	Apple iOS laid bare at Black Hat: How more sophisticated, automated attacks on iOS impact enterprise defenses	NAC, MDM, network monitoring, SIEM endpoint security, data protection, encryption, IR
	Internet of Everything: Is everything an endpoint? And if so, what does that mean to enterprise security and risk management?	
CSCs	Overview of CSC 6.0 update and how to achieve maximimum benefit: More organized with different control groups reflecting today's challenges	All areas covered by the controls including access, encryption, network monitoring/visibility, IR readiness, SIEM and more
	CSCs as a maturity model: Where to take it from here	
	Break down of any specific control listed in CSC 6.0	
Data Security/Privacy	Following the data everywhere: Encryption and DLP schemas get with the times	DLP, encryption, data classification/management, deep packet inspection and decryption, monitoring/egress monitoring and optimization, access management, data center security, cloud security
	Data visibility and classification: Knowing what data you have is the first step to protecting it	
DDoS Defense	DDoS and the 10-second DDoS defense and recovery: Would it work for anyone but the Pentagon?	DDoS protection technologies, network visibility, ATP
	Dispersal defense: Can rearranging your servers really help thwart a DDoS attack?	
Embedded Systems and Security (ICS)	Moving beyond signature-based detection in embedded systems and IoT	Health care, retail, manufacturing endpoints, encryption, DLP, advanced threats, SIEM/analytics, CTI, vulnerability management
	Current risks aimed at ICS and options to defend them	
Financial/Retail	Doing business with the connected consumer: Security primer for banks, credit agencies and others building federated ecosystems with social networks and other connected-consumer businesses	Web, social media, consumer protections, retail systems, appsec, SIEM, intelligence and analytics
Health Care	Health care in the cloud: A review of the efficacy and security of using health care information exchanges	Cloud, data center, encryption, DLP, mobility, IoT, SIEM, analytics/intelligence
	Mobile delivery of health care applications: What are the risks, and how can you securely facilitate mobility now and in the future?	

SANS Analyst Program Custom Content Suggestions for 2016

Don't see what you like on the 2016 SANS Analyst Program Editorial Calendar?
Here are some topics SANS has identified for custom sponsorship opportunities in 2016:

Identity and Access Control	Cloud-driven federations: Merging ad hoc ecosystems of access, authentication and cloud	Access control/identity management, two-factor authentication using biometrics, phone-based authentication, federated identities, keycodes, etc.
	Your contractors are not always your friends: Controlling third-party access	
Perimeter Security	The open enterprise: Protecting digital assets all over the place	Network monitoring, firewalls, IDS/IPS, Unified Threat Model (UTM), access controls, SIEM
	Is a software-defined (hybrid cloud) perimeter the best replacement for the old perimeter?	
Security Governance and Leadership	Finding fault: Cyberinsurance and the battle over what constitutes "enough" security	Reputational services, social media monitoring, budgeting, benchmarking, risk/reputation management, compliance, maturity
	Protecting reputations: Voice, text, social media and the rest of the ecosystem that shapes reputations	
	CISO priorities: Budget, buy-in, reporting structures, cyber insurance, staffing and more	
Security Maturity	Never fully mature: What even the most mature companies need to do to push the curve	SIEM, vulnerability assessment and remediation, risk calculators, visibility, security awareness
	Finding the right mix: Maturity of individual programs could lead to competing goals. How do you coordinate across maturity program owners?	
Threat Identification	Threat hunting: Hype or help?	IR, analytics/intelligence, machine learning, active response
	Know what you know, learn what you don't: A beginner's guide to detecting unusual activities that cannot be covered up	
Vulnerability Management and Remediation	Vulnerability and threat intelligence: Where they converge and differ—and how to use both effectively to prevent and protect	Assessment, remediation, continuous monitoring, vulnerability management, appsec
	Continuous monitoring as applied to the new CSC 6.0 guidelines	