2018 SANS Analyst Program Topical Calendar

SANS Institute is the most trusted and by far the largest source for information security training in the world.

The SANS Analyst Program produces leading-edge analyst reports about emerging and mission-critical topics. Under the Analyst Program, SANS instructors and subject matter experts develop objective, third-party thought leadership content that is educational to the 300,000-member SANS portal community. Sponsors of this content have access to decision makers and influencers who are aware of risks and always looking to improve their security and response capabilities.

Tags	Description
Business Partner Risk, Insider Threat, Monitoring and Access Controls	**Business Partner Breaches on the Rise!** Attackers knocked down Equifax, Deloitte, the SEC and other agencies like dominoes. This paper looks at why partner attacks are on the rise, who's accountable and how to monitor and protect against such attacks.
Application Security, Application Lifecycle, Continuous Monitoring, SOC, Security and Threat Management, Incident Response	**SOC and DevOps.** According to SANS surveys, developers are leading the charge in DevOps/SOC convergence. This paper details the proper application of secure lifecycle practices in the fast-moving world of DevOps, and what role the SOC plays in securely maintaining business apps.
Threat Hunting, Intelligence, Prevention and Detection	**Threat Hunting with Intelligence.** This paper introduces the concept of continuously hunting for threats proactively, and how to use intelligence to enrich the data you are hunting with.
ID/IAM, Mobile Security, User Management, Multi-Factor Authentication	**How to Hit a Moving Target: Real-World Identity and Access Controls.** Employees, contractors, service providers, public and private clouds—managing access across diverse ecosystems is tough! This paper helps organizations map their access rules to real-life scenarios while accounting for future needs and controls.
Cyber Threat Simulations, Pen Testing, Incident Response, Hacking Back, Deception	**Arm Your Cyber Warriors.** This paper illustrates how realistic, simulated cyber events—such as the U.S. Army's Cybertropolis—can help bring defenders up to speed on combating the real-life challenges they face daily.
Compliance, Continuous Monitoring, European Data Rules, Data Security, GDPR	**GDPR Starter Guide.** Developed by SANS Senior Instructor Ben Wright, this paper and webcast provide a framework for organizations confused about what they need to change in order to become GDPR-compliant.
IT Infrastructure, IoT, IIoT, Critical Infrastructure, Endpoint Security, Security Control Frameworks, CSCs	**ICS Controls to Save the Infrastructure.** With the rise in IoT attacks, can tried and tested ICS practices be applied to other connected devices on today's networks? This paper explores ICS security frameworks and their applicability to managing IoT.
Pen Testing, Network Hygiene, Endpoint Security, Remediation	**Extreme Pen Testing.** The paper covers key best practices for IT hygiene, the need to trace exploits to their origins—then close loopholes on all endpoints.
Security Assessment, Security Benchmarking	**Benchmarking Security.** Organizations spend a lot of money on products, people and services to secure their extended enterprises. This paper will explain how organizations can see if their security provides ROI, how to develop a risk score, and how to prioritize future spending.
HIPAA, Healthcare IoT, Endpoint Security, Encryption	**Protecting Medical Devices.** Many healthcare organizations were swept up with Wannacry and other ransomware and wipeware in 2017. This paper, developed by SANS Health Care IT Expert Barb Filkins, will focus on risks and best practices for securing medical devices.
Insider Threat, User Awareness, User Enablement, Email Security, Browser Security	**Don't Blame the Users!** Help Them to Help You. This paper explores how to win over users, monitor their usage and protect their systems against a flood of increasingly sophisticated attacks.
Shadow IT, Inventory and Assessment, Continuous Monitoring, VM and Cloud Security, Network and Endpoint Security	**Managing Shadow IT.** Gartner estimates that shadow IT accounts for 30–40 percent of IT spend in large enterprises. This paper explains how unsanctioned technologies (hardware, software, virtual and cloud apps) creep into an organization, as well as security and compliance risks that accompany shadow IT.

SANS Analyst Program

Email Security, Authentication and Access Management	**DMARC Implementer's Guide.** The DMARC protocol is gaining traction as a secure method for email authentication and reporting. By the end of 2017, nearly 200,000 DNS servers were processing DMARC records. This paper will look at effectiveness of DMARC in preventing email-based attacks, and offer actionable advice.
Security Asset Review, SOC, Integration, Risk Scoring, Security Assessment	**Use What You've Got.** Does your organization fully understand the capabilities of the tools it's using to protect against and respond to events? This paper will outline a discovery process for inventorying security capabilities that you currently have and ascertaining what you still must acquire.
Threats and Trends	**Brace for It: 2018 Recap and Upcoming Trends Report.** In 2017, the biggest threat trend was ransomware. What was the main menace of 2018? In this paper, SANS Director John Pescatore will look at major events in 2018 and how to prepare for 2019.
Digital Contracts, Digital Currency, Disruptive Technology	**Blockchain: Disruptive Technology Report.** Bitcoin grabbed everyone's attention with its meteoric rise last year, but there's more to its success than cryptocurrency. This paper will explore Bitcoin's underlying blockchain technology, including its potential to transform dozens of industries—and how blockchain can be used maliciously.

Don’t see what you want? Pick your own topic! SANS also develops topical papers, guides and product reviews based on sponsor requests. Inquire with your sales manager or email vendor@sans.org.

SANS Analyst Program