SANS Analyst Program Topical Content Offerings

The SANS Analyst Program produces leading analyst reports on emerging and mission-critical topics. The following list of topics reflects custom content ideas available for sponsorship. These reports are developed by SANS instructors and subject matter experts. Papers are promoted through an associated webcast and all webcast registrants are shared as leads for sponsors. For more information, contact your SANS Account Manager or email us at vendor@sans.org.

Compliance and Risk Management

Practice Area	Technology or Processes	Title and Description
Cyber Insurance	Risk assessment; risk management; risk reporting and ranking; security controls assessment; security controls frameworks	**Getting Real About Cyber Insurance** This content covers the drivers for acquiring cyber insurance, progress made in ranking risk, and the reason cyber insurance clauses are and must differ from insurance in the physical realm. It also includes advice on how to protect against new developments, such as insurers utilizing cyberwar clauses to deny claims.
Data Governance	Asset identification and classification; continuous monitoring/assessment; risk ranking and reporting; compliance management	**GDPR, State Laws and Brexit — OH MY** This content helps organizations make sense of new data protection regulations, including advice on improving and automating compliance and risk management programs.
Data Protection	Data encryption (PKI, TDE, etc.); key management; application and device encryption	**Protecting Data in a Post-Quantum World** This paper examines the potential impacts of quantum computing on PKI, AES and other current crypto programs, along with a comparison of potential solutions coming out of NIST.
Digital Contracts	Blockchain; PKI; smart contracts	**Blockchain: Hype or Fiction?** This paper examines the benefits and viability of the resource-heavy Blockchain for potential business uses such as supporting digital contracts. It also reveals the risks associated with using the Blockchain (for example, a single point of failure when a key goes missing).
Risk Management/ Risk Measurement	Vulnerability management and assessment; risk ranking and reporting; threat detection and threat management	**Risk-Based Vulnerability Management** This paper details the criteria for managing risk versus just managing vulnerabilities. That means mapping risk across people, processes and technologies; comparing risk data with threat data; and maintaining a risk threshold.
Risk Management/ Threat Management	Vulnerability assessment; pen testing; DevOps	**Red Team, Blue Team, Purple Team** This paper demonstrates simulations from the MITRE ATT&CK™ Knowledge Base as it explains how to assess for vulnerabilities against attack readiness for more powerful prevention, detection and response capabilities.

Compliance and Risk Management *(continued)*

Practice Area	Technology or Processes	Title and Description
Secure by Design/ Supporting Digital Transformation	Secure DevOps; assessment, application and data-level encryption; IDM/IAM; network and endpoint security; intelligence and threat hunting	**Go Native: Securing Apps and Workloads Spinning Up in the Cloud** Large cloud providers including AWS and Azure now offer numerous choices in embedded and third-party tools for spinning up security along with apps and workloads in the public cloud. The paper provides advice on how to select the best security for cloud workloads.

Security Operations

Practice Area	Technology or Processes	Title and Description
APIs	API security; DevOps; security automation and integration; purple team assessments	**Friend or Foe? How to Manage Your APIs** This tutorial reveals the need for APIs, which are particularly common for integrating security operations. It then explains common threats to APIs such as man in the middle, identity and parameter attacks, and includes advice on closing API-related vulnerabilities.
Business of SOC	SOC structure; SOC service policies; integration and automation	**Setting Up a Service-Oriented SOC** This paper provides advice for organizations building their internal SOCs on how to apply a service and chargeback model to support the larger organization.
Cloud	Incident response/ forensics; network and endpoint security; analytics/ intelligence; threat hunting	**Responding to Incidents in the Cloud** Collecting data and system information from the cloud for forensics became a bigger problem for SANS survey respondents this year. This paper provides education about the tools and techniques organizations need to gain better visibility into cloud incidents.
Detection and Response	Cyber threat intelligence; threat hunting; deception	**Which Came First? The Hunt, the Deception or the Intelligence?** This paper looks at how these three capabilities work together to enrich and improve detection and response activities.
Digital Transformation	Cloud; DevOps; AI; IoT	**Enabling Digital Transformation** What is digital transformation and how do you enable it with security? Every aspect of business is or will be digitized, including critical operational technology (OT) systems such as those that failed in the Boeing 747 MAX. Responsible developers/engineers and their IT managers must understand the business and its associated risks.
Prevention and Detection	Endpoint security; network security/monitoring; incident response	**Next-Gen Network Firewalls Meet Next-Gen EDR** This paper examines advances in network firewalls and EDR, including SANS survey stats on how the two practice areas are coming together in cloud and on-premises environments.

Security Operations *(continued)*

Practice Area	Technology or Processes	Title and Description
Risk Management	Risk metrics and reporting; security metrics and reporting; threat metrics and reporting	**Moving Beyond Fear-Based Security to Risk-Based Operational Management** Executives and managers need metrics that indicate if and how their security is working, what tools and strategies are not, and where to make new investments. This paper describes how to automate and utilize risk metrics for reporting to management and regulators while improving risk posture.
Security and Response	AI; security automation; threat hunting; threat modeling	**Maturity Curve for AI in Security Operations** The majority of respondents to the SANS 2019 AI survey believe that their use of AI is improving accuracy and timing of detection and response. They also believe that AI is not maturing fast enough. This paper examines the AI maturity curve as it compares to practical uses of AI for security and response operations.

Don't see what you want? Pick your own topic! SANS also develops topical papers, guides and product reviews based on sponsor request.
For more information, please contact your SANS Account Manager or email us at vendor@sans.org.