SANS 2019 Analyst Program Topical Content Offerings

The SANS Analyst Program produces leading analyst reports on emerging and mission-critical topics. These reports are developed by SANS instructors and subject matter experts with their own followings in the SANS community. Sponsors can help drive topic awareness to a qualified audience of decision makers and influencers who are seeking objective data to help their organizations invest resources in successful IT security operations.

Secure By Design

Access and Authentication	**Good Riddance to Passwords** SOLD OUT Passwordless computing is now closer to becoming reality — starting with the public cloud. This paper examines whether or not these new multi-factor methods are truly more convenient to users and administrators and how they improve security. It will also provide resources and case studies to help readers prepare their infrastructures.
Access and Authentication	**Zero Trust. Insiders/Outsiders/Partners — All Are Suspect** This model considers all insider, business partner and outside access requests to be potentially malicious. This paper will describe how the zero trust model works in today's open networks and how to integrate the model into existing IDAM and security monitoring and reporting systems.
Cloud & DevOps	**Go Native: Securing Apps and Workloads Built For and In the Cloud** This paper looks at how to embed security and risk management into cloud apps, and how to select service providers to support an organization's workload and data protection capabilities.
Cloud & DevOps	**Service Mesh Architectures for the Cloud** This paper explains the concept of mesh fabric in comparison to containers. It will also discuss where to apply protections and assessments on the control and data planes for visibility, security and resiliency.
Vulnerability Management/ Risk Assessment	**Red Team, Blue Team, Purple Team: The Value of Automated Breach and Attack Simulations** This paper will explain how to assess for vulnerabilities and attack readiness together for more powerful prevention, detection and response capabilities across applications. It will also demonstrate simulations from the MITRE ATT&CK™ Knowledge Base.
Vulnerability Management/ Risk Assessment	**Risk-Based Vulnerability Management** SOLD OUT The hot thing about vulnerability management today is the move toward reporting risk, not just listing vulnerabilities and repairs. This paper explains the difference between old-school vulnerability management and today's more thorough, continuous assessments to map risk across people, processes and technologies.
Vulnerability Management/ Risk Assessment	**Uncover Blind Spots on Your Network** Most IT pros know that they have blind spots or dark space on their networks—unregistered devices and apps, unused or unmonitored network address spaces, machine-to-machine connections, and cloud apps they cannot see or don't know about. This paper will educate both the security and the IT operations professionals on how to see into dark spaces to find, assess and control these unknown computing actions.

SOC & Incident Response (IR)

Cyber Resiliency, SOC, Supply Chain, SLAs, Backup and Storage	**Resiliency: Still Just a Buzzword?** This resource-rich whitepaper will outline the policy and engineering framework updated by Mitre in March 2018. Organizations in both the public and private sectors that want to achieve resiliency in operations (keep the lights on) and in security programs can apply these ideas.
Endpoint & Network Controls, Behavior Monitoring, Threat Hunting	**Holistic Monitoring Across Endpoints, Apps and Network Activities** This paper will detail an attack chain model and the resulting system and network actions that indicate malicious behavior. It will then explain how endpoint plus network monitoring and detection capabilities work together to predict an prevent suspicious activities.
IoT, Deception, Incident Response	**Deception Meets IOT** Deception is finding many use cases in enterprise systems, cloud systems, and now in IoT environments. It is increasingly being used to deflect attacks and learn from them in order to predict and prevent.
SOC & IR Integration, Security Maturity	**SOC Maturity** By now, SOCs should be integrated and partnering with their IT ops and incident response departments, but most SANS Surveys show that technology silos still exist. This paper will chart the SOC maturity curve and guide readers on how to assess and increase SOC maturity.

Hacking and Threats

Crypto Mining, Malware, Endpoint Security	**Crypto Jacking** This paper explains the organizational risks associated with devices and systems, including IoT devices, that are being hijacked to mine crypto for digital currencies.
Crypto Mining, Malware, Endpoint Security	**Firmware Hacking** This paper will show how to map and incorporate specific security policies to known firmware exploit methodologies, including at the supply chain layer (where rogue components may be installed during development). It will also cover protections against layered, remote attack methods that work their way down to the firmware.
Current Threats, Exploits & Vulnerabilities	**Topic of the Month** Since attack techniques change and move up and down the stack, this will serve as placeholder for new findings and techniques discovered by SANS Internet Storm Center and other industry groups. This would be a short “SANS spotlight” paper developed in five weeks or less, that is focused on new, current or pervasive Threat or Attack methods of interest to the SANS community. It will also include a press release and a webcast to reach the audience immediately with the relevant news.
Data Theft, Dark Web, Data Protection, Brand Protection	**Hanging Out on The Dark Web: Stolen Business & User Data** This paper will reveal the type of data for sale on the dark web, which is essentially an underground, mostly-criminal mirror to the Internet requiring Tor to access rather than a regular browser. A SANS Analyst will explain how to monitor for misuse of business and client data and what to do when these types of data are discovered on the dark web.

Management Issues

Risk Management, Security Metrics, Continuous Improvement	**Moving Beyond Fear-Based Security to Risk-Based Operational Management** It is no longer enough to tell the CTO the sky is falling. Executives and managers need metrics that show if and how their security is working, what tools and strategies are not, what initiatives to scrap, and where to make investments. This paper focuses on the types of information senior-level executives need from their risk management programs in order to meet these and other objectives.
SOC Efficicacy, SOC Structuring, SOC-as-a-Service	**How Many People Do You Need in Your SOC?** SANS surveys show SOCs are understaffed! While measurements vary, this paper will discuss ways to assess whether or not staffing meets the organization's demand, based on factors such as network maturity, size and complexity. It would also look at other hard and soft measurements, such as mean time to detect and respond, rate of false positives, potential loss prevention, etc.
SOC Management, SOC-as-a-Service, SLAs and Charge Backs	**Setting up a Service-Oriented SOC** This paper will provide advice for organizations building their internal SOCs on how to apply a service and charge-back model to support the larger organization.

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.