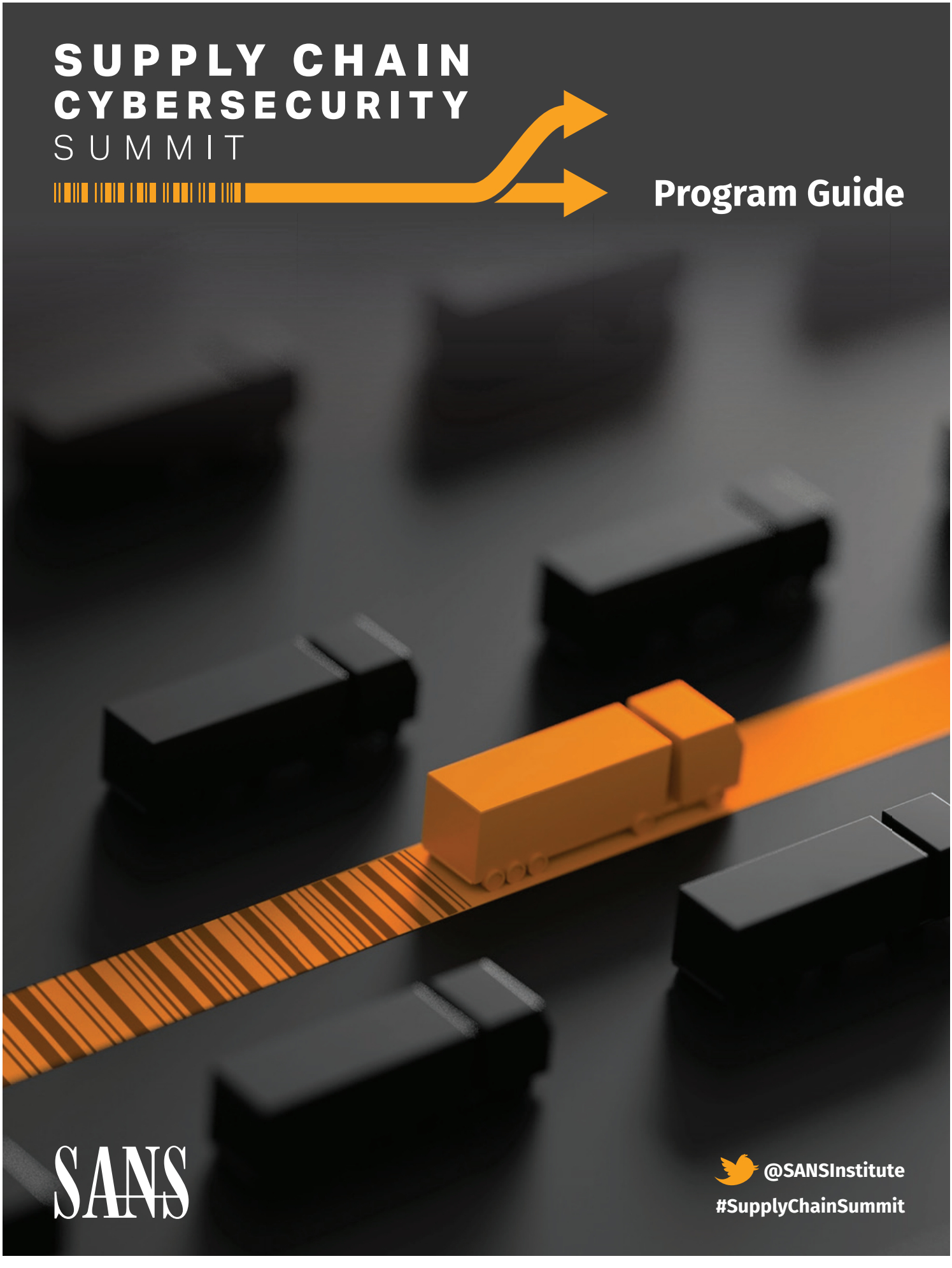
SUPPLY CHAIN CYBERSECURITY SUMMIT

Program Guide



SANS

@SANSInstitute

#SupplyChainSummit

Agenda

All Summit Sessions will be held in the F. Scott Fitzgerald A/B/C (unless noted otherwise).

All approved presentations will be available online following the Summit at ***sans.org/summit-archives***

Monday, August 12

7:00-9:00 am	**Registration & Coffee** (LOCATION: PRE-FUNCTION C)
9:00-9:15 am	***Welcome & Opening Remarks***
9:15-10:00 am	***Keynote: When Your OT Support Supports the APT*** Manufacturing, medical, and many other environments have extremely specialized (and expensive) operational technology (OT) devices. Due to a high degree of specialization, these devices are rarely maintained by the same organization that operates them. In some cases, these devices are merely leased from the manufacturer, remotely maintained by the manufacturer, then deployed in a customer's production network. While it is well understood that remote support technicians could achieve malicious effects through remote administration software, what about APT? How easily can an advanced attacker pivot from an infected remote support machine to the OT device (and ultimately to the customer network)? In this talk, Jake will walk through the mechanics of compromising OT equipment via remote support software complete with demonstrations of gaining access. ***Jake Williams*** *@malwarejake, Summit Chair & Senior Instructor, SANS Institute*
10:00-10:30 am	**Networking Break** (LOCATION: PRE-FUNCTION C)
10:30-11:15 am	***Own Your Software Supply Chain – Or It Will Own You*** Deliver Now! (we'll fix it later). Most of our suppliers are much more interested in this quarter's receivables than your company's health and safety. This session identifies then simplifies the problem and outlines what many major companies are doing to address the critical risk. ***John P. Martin****, Program Manager, The Boeing Company*
11:15 am – 12:00 pm	***The State of Your Container's Supply Chain*** Container security often focuses on runtime best-practices, while neglecting delivery of the software in the supply chain. Application, library, and OS vulnerabilities are a likely route to data exfiltration; while emerging technologies in the container ecosystem offer a new opportuninty to mitigate risk. Treating containers as immutable artifacts and injecting configuration allows us to "upgrade" images by rebuilding and shipping whole software bundles, thus avoiding configuration drift and state inconsistencies. This makes it possible to constantly patch software and to easily enforce governance of artifacts both pre- and post-deployment. In this talk we outline an ideal, security-hardened container supply chain, describe the current state of the ecosystem, and dig into specific tools. Grafeas, Kritis, in-toto, Clair, Micro Scanner, TUF, and Notary are covered, and we examine how to gate container image pipelines and deployments on cryptographically verified supply chain metadata. ***Andrew Martin*** *@sublimino, Co-Founder, ControlPlane*
12:00-1:15 pm	**Lunch** (LOCATION: PRE-FUNCTION C)

Monday, August 12

1:15-2:00 pm	***Neutralizing Risk from Customer Engagements*** A vulnerability assessment of a customer network found normal issues + China and Russia active in network + >15K outbound files in under 24 hours, some of which were steganography + no BCP, DRP, IRP, or Security Policies + Huawei gear + no visibility of network + no vendor management + no redundancy. The customer is in the communications sector of U.S. critical infrastructure, and located in a rural area covering three states with multiple military bases within the service area. How can we help this customer without impacting our own network and without transferring those risks to other customers, partners, and vendors? ***Keely Richmond*** *@trulykeely, Security Engineer, Check Point*
2:00-2:45 pm	***U.S. Air Force Implementation of Cyber-Supply Chain Risk Management (C-SCRM)*** This presentation will show how the U.S. Air Force is addressing C-SCRM activities as they relate to hardware assurance, software assurance, and trusted systems and networks. Topics include tasks associated with identifying assets in the inventory, getting threat information to the appropriate decision-makers, and having the right governance, risk, and compliance frameworks (such as the Cybersecurity Framework and Risk Management Framework) established and sufficiently mature enough to carry out the activities necessary. The presentation will cover various methodologies that can be used to conduct vendor and supplier assessments as well as the activities needed to leverage the vulnerability management process. The presentation will also look at some of the lessons learned from out-of-date and abandoned software. ***Alyssa Feola*** *@its_a_lisa, Cybersecurity Advisor, U.S. Air Force*
2:45-3:15 am	**Networking Break** (LOCATION: PRE-FUNCTION C)
3:15-4:00 pm	***Software Bill of Materials: Finding Consensus on Third-Party Code Transparency*** A "software bill of materials" that lists third-party dependencies can help both software suppliers and enterprise customers understand what is in the products they build, choose, and use. In 2018, the National Telecommunications and Information Administration (NTIA) launched an open process that used experts across many sectors to identify challenges in assembling, sharing, and using these data. A year later, NTIA stakeholders have made substantial progress in establishing a common vision of what constitutes a software bill of materials and how it can help security across the supply chain and empower the end customer. Participants have also identified a set of existing protocols to communicate dependency data. This talk will present progress and highlight successes in harmonizing standards as well as in sector-specific use cases. It will conclude with a list of the challenges that remain and how participants can get involved in establishing new practices and norms in software supply chain transparency. ***Allan Friedman*** *@allanfriedman, Director of Cybersecurity Initiatives, NTIA/U.S. Department of Commerce*

Monday, August 12

4:00-4:45 pm	***Selecting for Security: Searching for Risks from the Supply Chain in IoT Devices at Scale*** In this presentation, attendees will learn about supply chain risks specific to Internet of Things (IoT) products, gain an understanding of current challenges for manufacturers and users in addressing these threats, and leave with the tools to combat these risks in their enterprise. We will first cover the risks introduced to IoT products due to the unique supply chains involved in producing them. From this, we will cover the different ways that security-conscious companies making devices try to mitigate those risks, but also where they run into challenges. Finally, we review the industry best practices for assessing supply chain risks in potential products (e.g., vendor questionnaires, etc) – and where these methods fail to provide security. We will highlight the top five items that an IoT acquisition policy should verify (from a technical practitioner perspective) – specifically minimizing supply chain threats – and discuss methods for how these can be done today (discussing solutions that are simple and scrapy, homegrown or free/open-source). These are actionable take-aways that will arm attendees to make a difference immediately at their organizations. Recognizing the challenges faced in evaluations at scale, we will discuss how automated analysis is the future for helping empower companies to evaluate such issues at scale. ***Ryan Speers*** *@rmspeers, Firmware Analysis Lead; CEO, Pilot Security, Inc.*
5:00-7:00 pm	**Supply Chain Summit Networking Reception** Please join us for a complimentary reception with a selection of gourmet wines, cheeses, antipasti, beer and sliders. We'll meet in Ballroom Foyer C and spill onto the outdoor patio.

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Tuesday, August 13

7:00-9:00 am	**Coffee & Tea** (LOCATION: PRE-FUNCTION C)
9:00-9:45 am	***Third-Party Software Assessments for Modern Development*** Software is no longer delivered on a CD-ROM with occasional updates. Software delivery has become a continuous process for SaaS, mobile and desktop apps. So what value is a point in time assessment to understand the risk accepted by software users? Software assessments must become continuous and process based. There is also a need to balance the transparency desired by software users with the needs of vendors to be effective in software delivery and maintenance. We need continuous assessment with the right level of transparency to keep up with our rapidly changing and deeply nested software supply chains. ***Chris Wysopal**, Chief Technology Officer, Veracode*
9:45-10:30 am	***Developers as Tools: Lessons from Red Teaming*** Working as a Red Teamer has challenged my thinking and helped build solutions to previously unsolved problems. One of the more interesting solutions that I have helped engineer revolved around using the developer to enable the deployment of our tools. In this presentation, we will demonstrate the impact of a developer being compromised and the exponential impact that can result from it. In this Hands-On demo, we will reconstruct an engagement where a developer was compromised and the attacker (Red Teamer in this case) was able to inject malicious code into the production code base which in return enabled remote access to any user that executed that code. You will be able to see the impact from both the developer's point of view as well as the attacker. Afterwards, we will decomp the indicators and speak to best practices when using centralized code repositories and engineering production-based workflows. ***Martin Edwards**, Rendition Infosec, LLC*
10:30-11:00 am	**Networking Break** (LOCATION: PRE-FUNCTION C)
11:00-11:45 am	***Bring Your Own Threat: Supply Chain Attacks Using Personal IoT Devices in Companies*** According to statistics, 35% of IT Directors report more than 1,000 pieces of shadow IoT on their networks daily, 39% said they used personal devices connected to the enterprise network. Most popular devices were fitness, digital assistants and smart kitchen devices. Every single day we hear how consumer IoT is weak and in its infancy, still, according to the statistics, these devices are commonly allowed to join computer networks of many small, medium and big companies. What could go wrong? If we talk of software supply chain attacks, the situation is somewhat easier, but what about all those IoT devices, we don't really have insight into? How easy is it to infiltrate enterprise network using off the shelf commodity IoT? We'll present a proof of concept (live demo) of how this could theoretically happen. Using a simple camera with modified-firmware attacker may start the attack from the inside out which gradually leads to getting access into the network infecting acoffee maker, modifying router settings, and in the end deploying ransomware, rendering the whole network inoperable. In conclusion, we'll discuss possible attack vectors and solutions to this problem. ***Martin Hron** @thinkcz, Researcher, Avast Software*

Tuesday, August 13

11:45 am – 12:30 pm	***When Security Best Practices Meet Your Supply Chain*** IT is developed globally. Chip design and fabrication is done in China, Japan, Korea, UAE, and the US. IT R&D is done in China, the EU, IS, Japan, Korea, and the US. Software development is done, well, just about everywhere. Supply Chain Risk Management is increasingly a concern as we have seen examples where nation-states seek to implant or weaken IT products. This talk highlights the life cycle issues organizations face such as whether a product: adheres to a specification in a standard, has been tampered with, has been developed robustly, is authentic and is being supported correctly. It addresses the dependencies an organization has on best practices adopted by the developer to: source components responsibly, follow robust development practices, track versions and prevent malicious alterations, sign software to ensure no tampering during distribution, and provide timely updates. Norms for life cycle management is in and of itself a standards effort. We'll discuss how these norms have the greatest effect if the steward for their instigation is independent of government and has no financial interest in the choices. ***Curt Dukes**, EVP & General Manager, Center for Internet Security (CIS)*
12:30-1:30 pm	**Lunch** (LOCATION: PRE-FUNCTION C)
1:30-2:15 pm	***Supply Chain Integrity Through Hardware Material Analysis*** Supply chain integrity is an exceptionally difficult problem to address when globalization has pushed manufacturing and shipping routes all around the world multiple times over. The ability to understand the life cycle of each component of a finished product has escaped the grasp of the consumer. The US Government already has recognized the dangers of securing its supply chain and has put policies in place to prevent them from using hardware and software directly developed by countries on their sensitive country list; however, this is defeated by the difficulty of properly investigating third-party relationships within the direct vendor. Doing wholesale investigation further than one step down in the supply chain requires unilateral support from the vendor. Without vertical integration and accountability, it is challenging to determine the legitimacy of both hardware and software components. Security experts believe there is no easy solution that easily safeguards against these threats; however material analysis can be repurposed by various methods of X-ray imaging to remedy the worry of supply chain interdictions. ***MacKenzie Morris** @ZeroAltruism, Savannah River Nuclear Solutions*
2:15-3:00 pm	***Trust but Verify: An Argument for Security Testing Vendors*** Before a company shares data with an external vendor, an important question needs to be considered: Does this vendor have a mature security program that will keep the company's data safe? To answer this question, companies often employ a variety of vendor risk management strategies, including questionnaires, requests for documentation, and contract language, as well as a variety of new tools that scan the public face of a vendor. But are these strategies truly effective at gauging the vendor's security maturity? In this session, the presenters will argue that hands-on security testing is one of the best methods to measure security maturity, and that it is far more effective than any other strategy. You'll learn how best to incorporate security testing into your vendor risk-management program at any scale, scope your testing, interpret results, and overcome the common challenges that a security team can face with hands-on security testing. ***Rachel Black**, Senior Manager, Application Security One Medical* ***Kyle Tobener** @kylekyle, Director, Enterprise Security, Salesforce*
3:00-3:15 pm	**Networking Break** (LOCATION: PRE-FUNCTION C)

Tuesday, August 13

3:15-4:00 pm	***Hacking the Motherboard: Exploiting Implicit Trust in All of the Forgotten Places*** Last year, Bloomberg's Big Hack article gave everyone a (questionably accurate but) much needed scare that forced companies to evaluate their exposure to supply chain intervention attacks. But a wider acknowledgement of the problem doesn't make it go away. We need to understand the attack vectors and the inherent hardware vulnerabilities used by these backdoors, as well as the steps we can take to protect ourselves. We must have confidence in the systems and the technical infrastructure that supports our economy. This confidence currently relies on too much implicit trust – overlooking serious risks. Assurance in this area is hard won, manual, and costly. In this talk, I will dive into several recent hacks including the ASUS software update hijacking, the SuperMicro supply chain, allegations vs. reality. This discussion will include a technical overview of various types of hardware implants, the access they enable, and what we should be doing to detect and mitigate. Attendees will leave the talk with an in-depth understanding of what a hardware implant is, what types of implants provide what capabilities, and – with this knowledge – how to protect their enterprise from these attacks against a modern supply chain. ***Sophia d'Antoine*** *@Calaquendi44, Security Researcher, River Loop Security*
4:00-4:30 pm	***Takeaways and To-Do List*** Jake will summarize key themes and ideas from the two days of Summit talks and help you structure a to-do-list for improving your supply chain security when you get back to the office. ***Jake Williams*** *@malwarejake, Summit Chair & Senior Instructor, SANS Institute*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.