kaspersky

SECURITY ANALYST SUMMIT

Phuket, Thailand
October 25-28

EVENT KIT

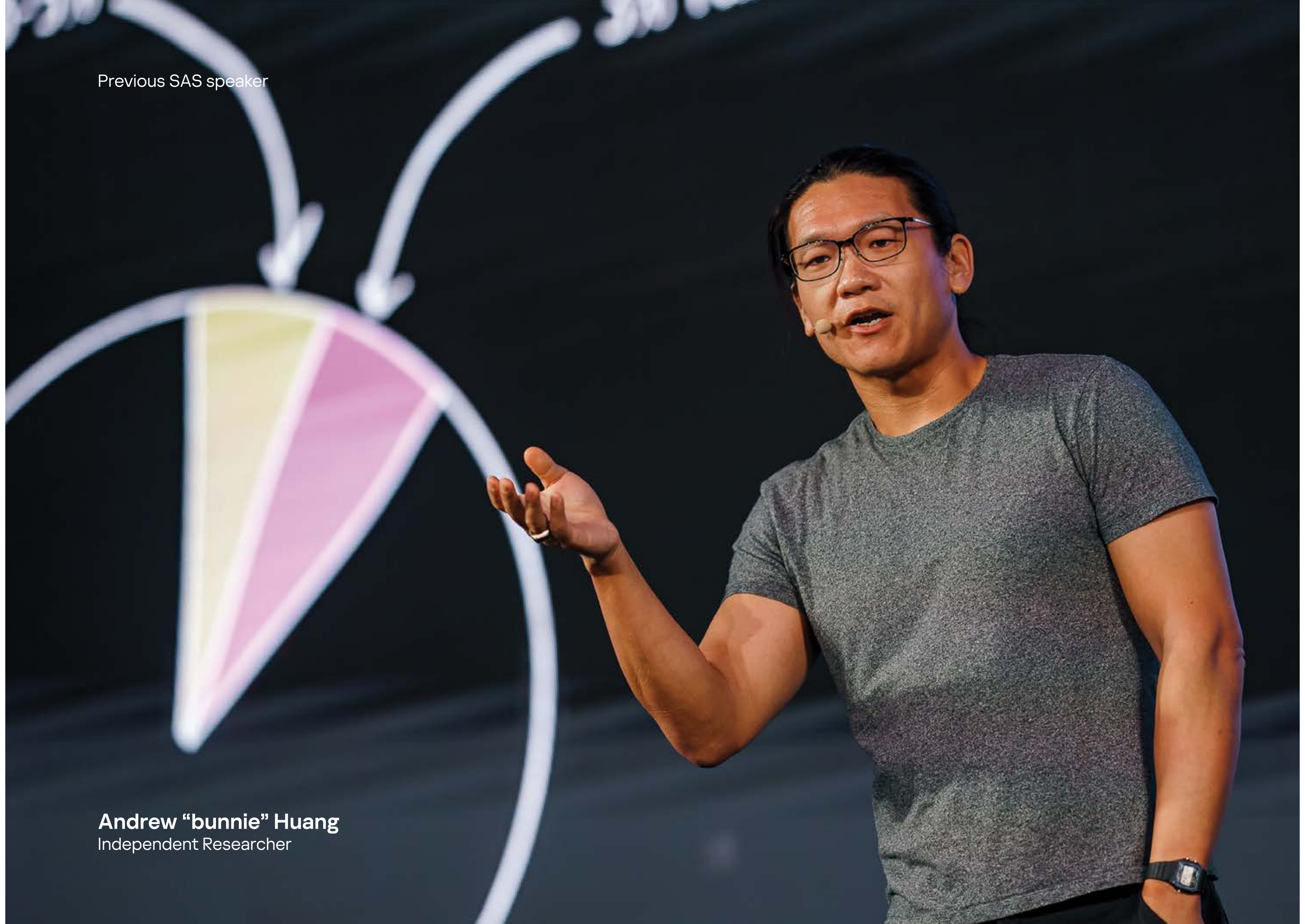
SECURITY ANALYST SUMMIT 2023

The Kaspersky Security Analyst Summit (SAS) is a prominent event that attracts high-caliber anti-malware researchers, global law enforcement agencies, CERTs and senior executives from financial services, technology, healthcare, academia and government agencies in order to shed light on cutting-edge cybersecurity researches and modern problems in the industry.

The previous events were joined by members of leading global companies, such as Samsung, Adobe, Microsoft, BlackBerry, Cisco, Boeing, Interpol, the World Bank, Team Cymru, The ShadowServer Foundation, ICSA Labs and Fidelis Cybersecurity Solutions.

The conference provides an exclusive atmosphere that encourages debate, information sharing and display of cutting-edge research, new technologies, and ways to improve collaboration in the fight against cyber-crime.

Previous SAS speaker



Andrew “bunnie” Huang
Independent Researcher

Kaspersky Security Analyst Summit 2023 will discuss the following topics:

- Advanced cyberthreats, APT actors and cyberwarfare
- Critical infrastructure and ICS/OT security
- Supply chain attacks and open-source software security
- Ransomware incidents and how to be protected from it
- Zero-day vulnerabilities and exploits
- Dark web trends and analytics
- Artificial intelligence (AI), machine learning (ML) and cybersecurity
- IoT attacks and security
- Tools and methods to support and increase user privacy

Previous SAS speakers

Juan Andres Guerrero-Saade
Chronicle Security

Joe FitzPatrick
SecuringHardware.com

Eva Galperin
Electronic Frontier
Foundation

Inbar Raz
CSIS Security Group

SPONSORSHIP OPPORTUNITIES

PLATINUM PACKAGE
$25 000

- Three full SAS event passes. Hotel, transfers, meals and all summit activities included.
- One speaking slot (must be vetted by conference organizers).
- Free six-month subscription to Executive Summaries of Kaspersky Security Intelligence Services.
- Table-top or a place for a booth in conference registration area.
- Inclusion of your company's logo in all marketing material (banners, brochures, badges, agenda).
- Display of your company's logo on the SAS web site.
- Inclusion of your printed materials in conference package.
- Free participation in one training course before SAS for two company's employees
- Free participation in three Kaspersky Expert trainings

GOLD PACKAGE
$15 000

- Two full SAS event passes. Hotel, transfers, meals and all summit activities included.
- Free three-month subscription to Executive Summaries of Kaspersky Security Intelligence Services.
- Inclusion of your company's logo in all marketing material (banners, brochures, badges and agenda).
- Display of your company's logo on the SAS web site.
- Inclusion of your printed materials in conference package.
- Free participation in one training course before SAS for one company's employees
- Free participation in two Kaspersky Expert trainings

*all prices are in USD

SILVER PACKAGE
$10 000

- One full SAS event pass. Hotel, transfers, meals and all summit activities included.
- Inclusion of your company's logo in all marketing material (banners, brochures, badges and agenda).
- Display of your company's logo on the SAS web site.
- Inclusion of your printed materials in conference package.
- Free participation in one Kaspersky Expert trainings

Kaspersky Expert trainings

xtraining.kaspersky.com

TRAINING

MALWARE FORENSICS FROM A DISTANCE

VITALY KAMLUK

Principal Security Researcher,
Head of Research Center, APAC
Kaspersky

NICOLAS COLLERY

Active Defence Team Lead
DBS Bank

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

This workshop aims to share knowledge of live triage and analysis of remote compromised systems to assist incident response, digital forensics, or malware discovery and in-place analysis. There are many other applications of the techniques and tools that the participants are encouraged to explore on their own.

Although the knowledge shared during the workshop can be applied independently of the tools proposed, it starts with the attendees building their own toolkit for remote threat reconnaissance. It features Bitscout, a project based on a collection of free open-source software for Linux, that is extendable with any set of tools the analyst wants to embed before or in the middle of the operation. Incident response to live cyberattacks requires silent navigation through compromised assets, sometimes in large distributed networks. The popular approach relies on EDR or other live agent-based solutions. However, the activation of security agents and obvious activities on live compromised systems may trigger alerts of advanced threat actors. Once alerted, a clean-up operation and destruction of evidence can happen. Moreover, offline system analysis may not be easy due to the physical distance to the compromised system or scale of the network. This is where remote stealthy threat discovery with “scoutware”, software for threat hunting and instant system analysis, becomes incredibly useful. Bitscout, used for the workshop is just one such toolkit.

In addition to working with local virtual machines during the workshop, the attendees will be provided with access to 60+ live servers to be analysed simultaneously to simulate large-scale compromise – online access will therefore be required.

CLASS REQUIREMENTS

Level:
Intermediate or above

Prerequisites:
- Knowledge of Linux CLI and Bash scripting
- Experience with virtualization and networking
- General understanding of popular OS architectures
- Understanding how to handle malware and compromised systems

Hardware:
A laptop with x64 CPU

Class:
Limited to 15 participants

Duration:
1 day

Date:
October 25, 2023

TRAINING

SURICATA FOR INCIDENT RESPONSE AND THREAT HUNTING

TATYANA SHISHKOVA

Lead Security Researcher,
Global Research & Analysis Team
Kaspersky

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

Suricata is the foundation for effective intrusion detection and prevention. With cyber attacks on the rise it's more crucial than ever for businesses, enterprises or cybersecurity consultancies to have a comprehensive security strategy in place. And that's where Suricata rules come to the rescue.

The "Suricata for Incident Response and Threat Hunting" course is the ultimate training program taught by Kaspersky's leading security researcher who has spent years on the front lines of cyber defense, Tatyana Shishkova. She will share unique insights and sophisticated tips and tricks, giving you an unparalleled understanding of the IDS/IPS within the Suricata rules framework.

The course is created for companies aiming to power up their security policy and individual learners, looking to advance their career in cyber security. Whether you're a beginner specialist or a seasoned professional in security or SOC analysis, security administration, malware research or incident response, it will give you the knowledge and skills to stay ahead of the ever-evolving threat landscape.

Learn how to write and implement Suricata rules to detect and block even the most advanced threats. Gain a deep understanding of how the framework works, and how to use it for identifying and responding to attacks in real-time. Get practical experience to enhance your network security with hands-on exercises and various real-life scenarios.

By the end of this training you will be better able to:

- Understand what is a NIDS and how to use it
- Write Suricata rules for different protocols
- Utilize tips and tricks to create fast and efficient rules
- Learn about typical network attacks
- Analyze suspicious traffic and recognizing traffic anomalies
- Learn how to identify and fix a false alarm
- Learn how to use Suricata for threat hunting
- Gain new skills through a practical challenge in virtual environment

CLASS REQUIREMENTS

Level:
Intermediate

Prerequisites:
- Basic knowledge of network protocols
- Familiarity with regular expressions (optional)

Hardware:
Laptop with VMWare /
VirtualBox virtualization solution

Class:
Limited to 15 participants

Duration:
1 day

Date:
October 25, 2023

TRAINING

THREAT INTELLIGENCE ANALYST TRAINING

NIKITA NAZAROV

Head of Threat Exploration
Kaspersky

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

After participating in this training, participants will be familiar with what Threat Intelligence is, what its role is in CSIRT, and how it helps to detect and analyze external threats and enables the effective operation and interaction of different teams. The course covers cyber threat intelligence domains and principles that are designed to build up comprehensive protection - from strategic plans to operational procedures.

Topics covered:

- Cyber Threat Intelligence
- Intelligence-Driven Defense
- Levels of Threat Intelligence
- TI & CSIRT
- Maturity levels
- Data Collection, Normalizing, Dissemination
- SIGMA, IOC
- Threat Landscape
- Cognitive Biases

CLASS REQUIREMENTS

Level:
Middle and senior-level CTI analysts,
SOC analysts, IS specialists

Prerequisites:
- Be familiar with MITRE ATT&CK and Cyber Kill Chain
- Experience in Incident Response / Security Operation Center processes / Threat Hunting / Threat Intelligence

Hardware & Software requirements:
- CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory.
- 8 GB (Gigabytes) of RAM or higher is mandatory.
- Attendees should have the capability to have Local Administrator Access within their host operating system.
- Internet access in the training location.
- 7Zip, http://www.7-zip.org/

Class:
Limited to 15 participants

Duration:
1 day

Date:
October 25, 2023

TRAINING

REVERSE ENGINEERING WITH GHIDRA

IGOR KUZNETSOV

Chief Security Researcher,
Head of Research Center, Russia
Kaspersky

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

This training is a unique opportunity for established reverse engineers, security researchers and malware analysts seeking to upgrade their skills, to join a Kaspersky GReAT expert to learn the advantages of using Ghidra - setting up the environment, working with structures, data types, automating routine tasks, and more.

The main event will be a live reversing session of a metasploit stager shellcode and a showcase sample of the Calypso APT. Participants will also be able to follow Igor's steps and tinker with real-life samples.

We will walk you through Ghidra's toolset, set up the environment and use Ghidra to analyze a metasploit stager shellcode. This will include using built-in datatypes, importing auxiliary headers, getting familiar with both the disassembly listing and the decompiler.

The training also includes exploration of Ghidra scripting in both Java and Python to restore API functions by hashes, and then reconstruct and use custom data structures while reversing a Calypso APT sample.

CLASS REQUIREMENTS

Level:
Medium and Advanced

Prerequisites:
- Understanding of x86 and x86_64 assembly, Windows API
- Basic knowledge of Python and Java
- Experience with reverse engineering code in IDA or Ghidra

Hardware, Software:
- Laptop with VMWare / VirtualBox virtualization solution

Class:
Limited to 15 participants

Duration:
1 day

Date:
October 25, 2023

TRAINING

HUNT APTS WITH YARA LIKE A GREAT NINJA

COSTIN RAIU

SERGEY MINEEV

Principal Security Researcher,
Global Research & Analysis Team
Kaspersky

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

Have you ever wondered how Kaspersky Lab discovered some of the world's most famous APT attacks? Now, the answer is within your reach. This training will lead you through one of the essential tools for the APT hunter: the Yara detection engine.

If you've wondered how to master Yara and how to achieve a new level of knowledge in APT detection, mitigation and response, it all breaks down to a couple of secret ingredients. One of them is our private stash of Yara rules for hunting advanced malware.

During this training you will learn how to write the most effective Yara rules, how to test them and improve them to the point where they find threats that nobody else does. During the training you will gain access to some of our internal tools and learn how to maximize your knowledge for building effective APT detection strategies with Yara.

Topics covered:

- Brief intro into Yara syntax
- Tips & tricks to create fast and effective rules
- Yara-generators
- Testing Yara rules for false positives
- Hunting new undetected samples on VT
- Using external modules within Yara for effective hunting
- Anomaly search
- Lots (!) of real-life examples
- A set of exercises for improving your Yara skills

CLASS REQUIREMENTS

Level:
Medium and Advanced

Prerequisites:
Knowledge of the Yara language and basic rules

Hardware:
Own laptop

Minimum Software to install:
Yara v. 3.6.0

Class:
Limited to 15 participants

Duration:
1 day

Date:
October 25, 2023

TRAINING

PRACTICAL OSINT: DETECT AND REACT

YULIYA NOVIKOVA

Head of Digital Footprint Intelligence
Kaspersky

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

As your business grows, so does the complexity and distribution of your IT environments. This presents a challenge in protecting your digital presence that is widely distributed and outside of your direct control or ownership. The interconnected nature of modern environments provides many benefits, but it also expands the attack surface, making it increasingly important to have an accurate understanding of your organization's online presence. As attackers become more sophisticated, it's critical not only to monitor your digital footprint but also to track changes and respond to up-to-date information about any exposed digital assets.

Training from Kaspersky analysts demonstrates how to detect and deal with a variety of digital risks that may target companies assets. Our experts will provide a deep dive into OSINT techniques that are used to reveal external threats of different nature - vulnerabilities of external infrastructure, phishing, data leakages, darknet threats and others. The key outcome of the training is an approach and action plan that will help companies' security team to mitigate risks and build proactive protection.

Topics:

- Understanding threat landscape for organizations
- Tailored OSINT: methods and tools
- Network reconnaissance
- External threats analysis: vulnerabilities
- External threats analysis: phishing
- External threats analysis: data leakages
- Darkweb deep dive: how to access and how to use
- Prioritization of threats
- Building protection strategy with tailored threat intelligence
- Composing action plan for security team

CLASS REQUIREMENTS

Level:
Middle-level CTI analysts, SOC analysts, IS specialists

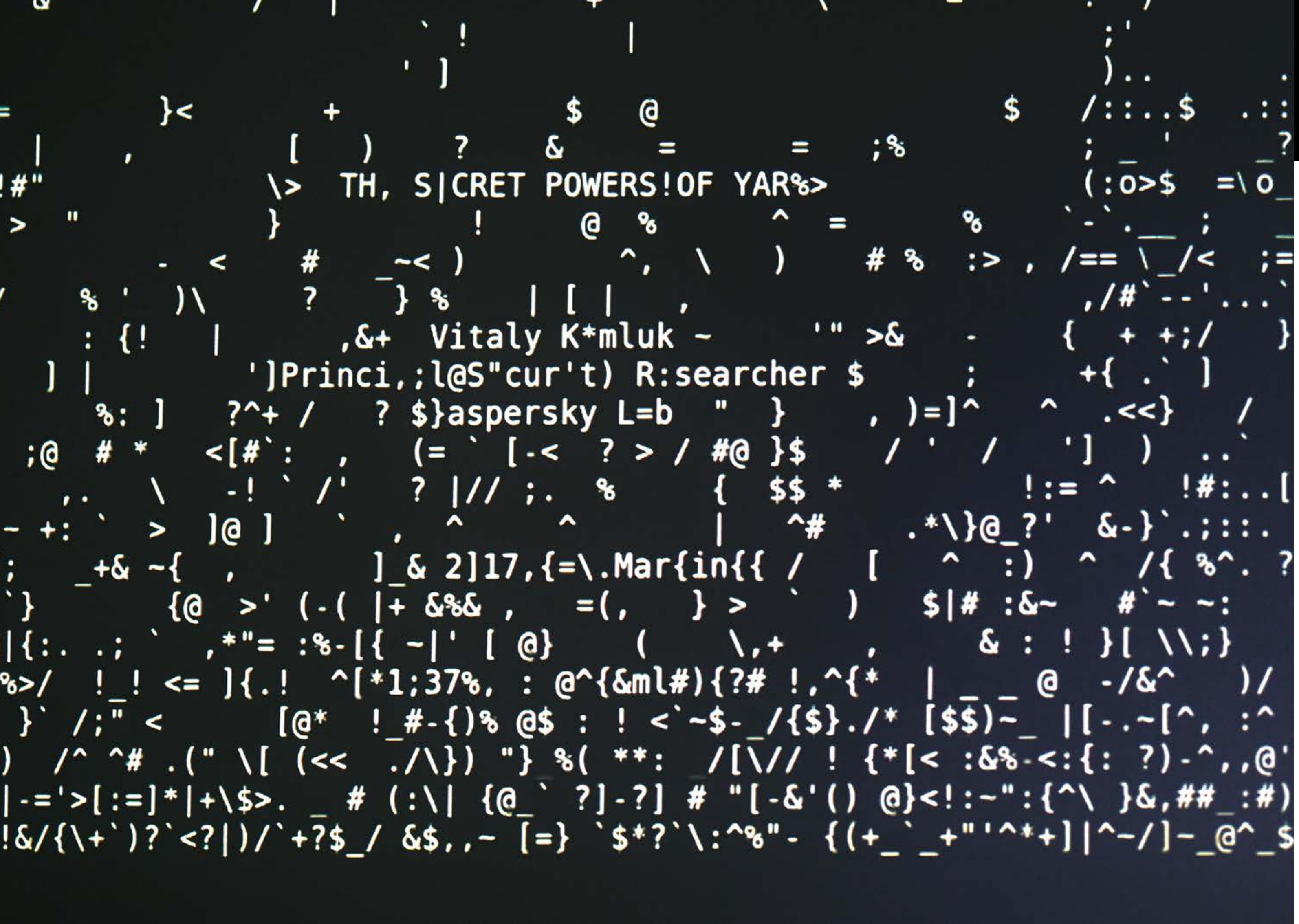
Prerequisites:
- Experience in Incident Response / Security Operation Center processes / Threat Hunting / Threat Intelligence
- Basic Python knowledge

Hardware and Software requirements:
- CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory.
- 8 GB (Gigabytes) of RAM or higher is mandatory.
- Attendees should have the capability to have Local Administrator Access within their host operating system.
- Internet access in the training location.

Class:
Limited to 15 participants

Duration:
1 day

Date:
October 25, 2023



TRAINING COURSE FEES

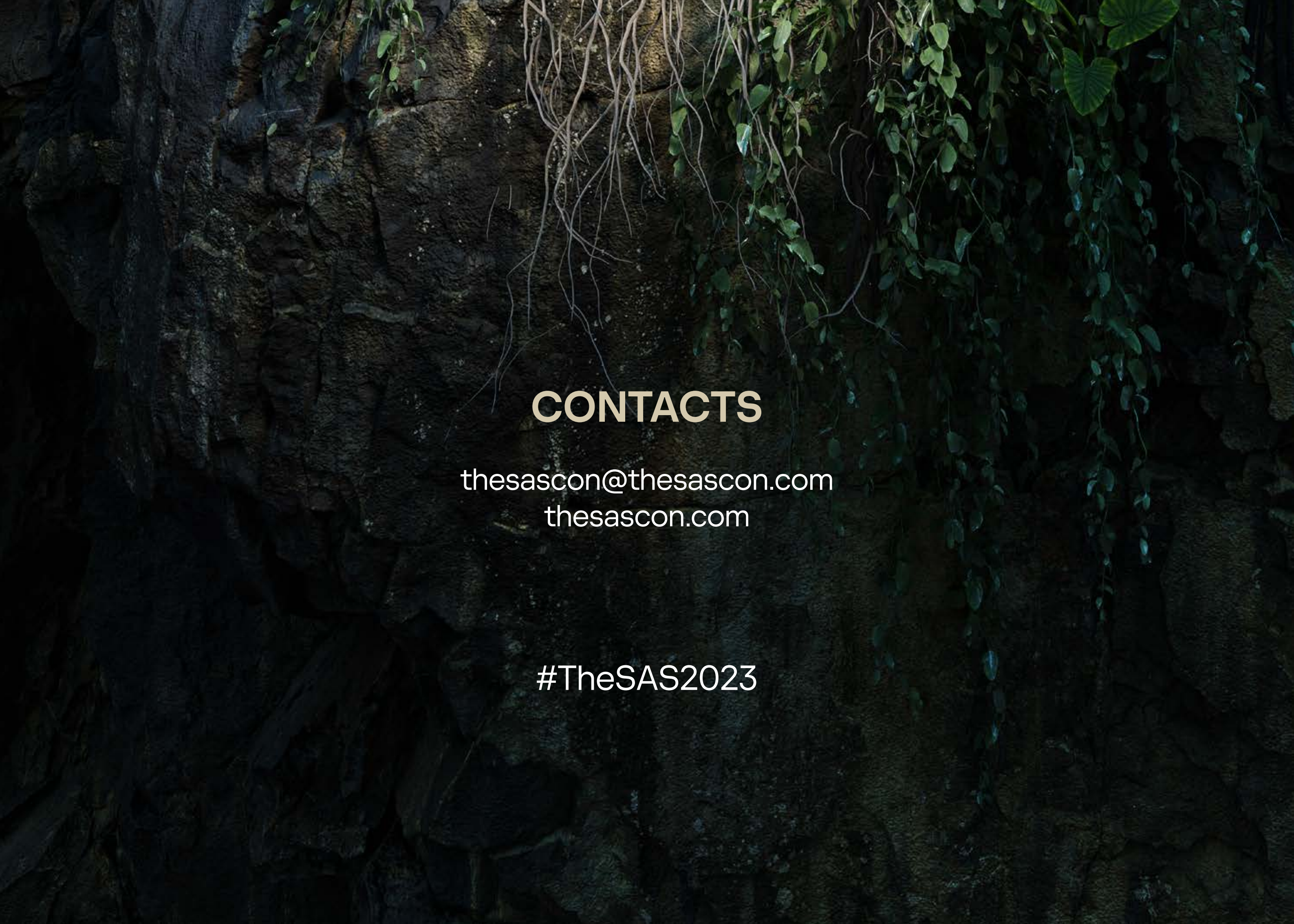
SAS 2023 training fee	✓
Hotel accomodation 2 nights + breakfast (October 24-26 2023)	🛏
Lunches & coffee-breaks	✓
EARLY-BIRD (ends on July 15, 2023)	$2 500
REGULAR (ends on August 31, 2023)	$2 800

LOCATION

Phuket, Thailand
October 25-28, 2023

JW Marriott Phuket Resort & Spa 5*

Phuket, Thailand, 83110
231 Moo 3 Mai Khao, Talang



CONTACTS

thesascon@thesascon.com
thesascon.com

#TheSAS2023