Workshop Summary
Australian Cyber Conference 2023

There is an extensive range of workshops available during the 2023 Australian Cyber Conference. In order to assist you in planning your attendance, please see a summary outline below. Please note that numbers are strictly limited for attendance at each, and offered on a first in best dressed basis – we recommend you consider arriving to the meeting room early to join the line and save your place. No pre-reservations are allowed.

Some workshops have pre-requisites or require you to bring along your own device, please ensure you review below;

ROOM 109	TUESDAY 17 OCT | 9:00-13:00
COMPANY/ TOPIC	**Expanding Your Threat Hunting Skillset - Paula Januszkiewicz**
OUTLINE	In this workshop, you will enhance your threat hunting abilities and acquire knowledge to effectively detect and analyze security threats within your network. The workshop covers a wide range of techniques and tools for identifying and analyzing threats, providing you with a comprehensive understanding of the most effective methods.
PRE-REQUISITES	NIL

Room 111 / 112	TUESDAY 17 Oct | 9:00-13:00, repeated 14:00-18:00
COMPANY/ TOPIC	**SANS Workshop - Hacker Tools, Techniques and Incident Handling Workshop: Cloud Edition**
OUTLINE	The workshop will cover some of the common techniques used by Threat Actors to target Cloud environments.We will talk about some common considerations to keep in mind for Incident Response in Cloud, scanning and attribution of systems, password attacks against M365, insecure storage, SSRF and IMDS attacks and Cloud post exploitation. The workshop will include a lot of demos and real world examples. This content is from SANS flagship course SEC504: Hacker Tools, Techniques, and Incident Handling. The participants will walk away with an understanding of how attackers target Cloud environments and how incident handling can be done in the Cloud.
PRE-REQUISITES	NIL

ROOM 101 / 102	TUESDAY 17 OCT | 13:40-16:40
COMPANY/ TOPIC	**OffSec Workshop - OSDA/SOC200**
OUTLINE	This workshop will provide attendees with an opportunity to get hands on with the tools used in the Offensive Security OSDA Certification for SOC. The workshop will be in two sections., The first will provide an introduction to using a SIEM to monitor a network for potential security intrusions, and then walk the students through the first phase of an attack in real time. Students will then have the opportunity to test their skills against follow on phases. The second section will provide an introduction to threat hunting using the US Department of Homeland Security MALCOLM toolset, and then walk students through a hunt through a set of pcap files. The students will leave the workshop with hands-on familiarity with the types of tools used in a modern SOC.
PRE-REQUISITES	Please bring your own laptop.

Workshop Summary
Australian Cyber Conference 2023

ROOM 110	TUESDAY 17 OCT | 10:45-12:45
COMPANY/ TOPIC	**Microsoft Immersion Workshop - Shadow Hunter**
OUTLINE	Join our hands-on workshop to test your defense skills and gain practical experience protecting workloads. In this gamified experience, a hacker has just gained network access through a security camera in the building. Their goal is to breach your enterprise and access sensitive information. Your job as a sophisticated cybersecurity analyst is to stop them in their tracks. Who should attend: • Chief security and information officers • IT security decision makers • Security architects After completing this workshop, you will: • Understand how to provide enhanced protection and security through Microsoft Defender for Cloud and Microsoft Azure Network Security for hybrid and multicloud environments. • Understand the benefits of using AI and automation in Microsoft Sentinel to help you detect threats quickly, respond effectively, and fortify your security posture. • Expand your expertise and learn how comprehensive protection from Microsoft Security works with your ecosystem and can help you close gaps in coverage.
PRE-REQUISITES	Please bring your own laptop.

ROOM 110	TUESDAY 17 OCT | 13.40-15:40
COMPANY/ TOPIC	**Microsoft Immersion Workshop – Into the Breach**
OUTLINE	Join our gamified workshop experience where you'll participate in the incident response investigation of a ransomware attack on the Health Network. Dive into the simulation and apply your in-depth knowledge of Microsoft Defender for Office 365 and Microsoft Sentinel to stop the hack. Who should attend: · Architects · IT professionals · Cyber defence analysts and incident responders After completing this workshop, you will: · Understand how to use integrated, automated, extended detection and response (XDR) to increase efficiency and effectiveness with Microsoft Defender to keep you secure against threats to identity, endpoints, data, apps and infrastructure. · Be able to detect, investigate and respond to threats using automated investigations and self-healing capabilities. · Know ways to locate threat indicators and entities using advanced hunting features to explore raw data across security pillars. · Recognise how to view alerts and remediate threats across your Microsoft 365 environment from a single dashboard.
PRE-REQUISITES	Please bring your own laptop.

Workshop Summary
Australian Cyber Conference 2023

ROOM 206	TUESDAY 17 OCT | 10:45-11:25, repeated 11:35-12:15, 13:40-14:20, 14:30-15:10 and 16:00-16:40
COMPANY/ TOPIC	Cybermindz
OUTLINE	A powerful, experiential session which will allow participants to enjoy a full 35-minute immersion into a facilitated state of deep calm through the world leading iRest Protocol led by Cybermindz.org founder Peter Coroneos. In addition, attendees will gain an understanding of the neuroscience behind the success of the protocol and how we are mobilising to bring this burnout prevention and restoration tool to cyber teams — first in Australia, and now the US.
PRE-REQUISITES	NIL

ROOM 109	TUESDAY 17 OCT | 14:30-17:00
COMPANY/ TOPIC	BSI Workshop - ISO/IEC 27002:2022 - Information security controls update
OUTLINE	The ISO/IEC 27002 standard, which serves as a reference for establishing controls for information risk management, has been updated. These changes reflect the concern of organizations globally around new risks that have emerged in a more digitized world, thus facilitating the continuation of your digital transformation plans and/or adoption of new cybersecurity strategies. Most likely your organization will need to refresh the controls that have been adopted around your management system and/or information security best practices. Details/Takeaways: The changes to ISO/IEC27001 and ISO/IEC 27002 in 2022 represents a leap forward in the effectiveness of Information Security Management Systems (ISMS). Quick and effective adoption of the latest global best practice is essential to ensure trust in your organization's ability to protect information. Join us to understand not only what is changing, but why, and how to use these changes to improve protection of your information assets whilst aligning with global cybersecurity frameworks. Key changes include: Updated controls aligned with current business practices and associated threats New "attributes" to enable alignment with different risk management methodologies including global cybersecurity frameworks Simplified and streamlined grouping of controls Greater clarity on management requirements in line with ISO harmonized structure This session will cover the changes, the benefits in adopting them, guidelines on how to implement them and how to get the most from your updated ISMS.
PRE-REQUISITES	NIL

Workshop Summary
Australian Cyber Conference 2023

ROOM 102	WEDNESDAY 18 OCT | 09:00-17:00
COMPANY/ TOPIC	**An Introduction to Software Reverse Engineering - Paul Black**
OUTLINE	This course aims to provide the participants with a knowledge of the basics of software reverse engineering, with a focus on practical insights. We start with common static and dynamic analysis tools, and then cover a simplified Intel 64 architecture, and progress to the operation of a subset of common instructions, that are vital to program understanding. We will teach the usage of the X64Debugger, and the Ghidra Disassembler/Decompiler. Practical exercises will be provided to reinforce the training concepts.
PRE-REQUISITES	The attendees should have at a minimum a basic knowledge of coding. A laptop running Windows 10 or 11, admin access, at least 8 GB of RAM, and one gigabyte or more of free storage space. The tools used in the training are publicly available, and will be provided on USB storage, or downloaded according to preference. This training session is based onbenign binaries and avoids special handling requirements. Please have the following software already downloaded - • JDK: https://java.com.en • Ghidra: https://github.com/NationalSecurityAgency/ghidra/releases • Strings: https//learn.Microsoft.com/en-us/sysinternals/strings • CFF Explorer: https://ntcore.com/?page_id=388 • Quickhash: https://www.quickhash-gui.org • Detect It Easy https://www.majorgeeks.com/files/details/detect_it_easy.html • X64DBG: https://x64dbg.com

ROOM 109	WEDNESDAY 18 OCT | 09:00-17:00
COMPANY/ TOPIC	**Lumify Workshop - Security+ - Foundations of cybersecurity and Investigating the skills and best practices needed to navigate dynamic attack landscapes**
OUTLINE	Join CompTIA's Dr. James Stanger and Lumify Group's Louis Cremen in a full-day workshop investigating the foundational skills and best practices new and existing employees need to address today's morphing attack surfaces. Louis and James will discuss the skills that CIOs, CISOs, and hiring managers around the world demand. During the workshop, we will be conducting practical labs and modelling the attack lifecycles of various attacks. Throughout, attendees will be learning about the foundational protocols, processes, and practices that create a uniquely-skilled worker and looking at what to expect with the next update to Security+ (SY0-701). • Where hackers reside today: Is it all about the applications? • A deep dive into foundational protocols (e.g., DNS, TCP, DHCP, TLS, HTTP/HTTPs) • How APIs work, and why that's important • Threat modelling using the MITRE ATT&CK Model and other lifecycle methodologies • Identifying IoCs and pivot points in various attack surfaces, from the cloud to on-premise • Practical encryption and authentication, including SSH and 2FA • What's new - CompTIA Security+ (SY0-701)
PRE-REQUISITES	There are no formal prerequisites for this session. Understand, however, that this session is designed to give a strong overview of the knowledge and best practices covered in the Security+ 701 exam. However, this course will discuss technical elements of protocols such as HTTP, HTTPS, Server Message Blocks (SMB), and various hacker lifecycles. Optional Downloads / Labs (see next page) This will be a lab-intensive day. James and Louis will demonstrate hands-on labs using VirtualBox, Ubuntu Linux, Kali Linux, Windows 7, and Security Onion. If students wish to follow along, then they can bring their own notebook computer with the following installed: • VirtualBox (or VMWare, if you prefer). • Ubuntu 22.04 (two instances) • Kali Linux 2023.2 • Windows 7 (a "victim system") • The following Security Onion image: https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md Please note: It is not a requirement for students to have their own labs and we will demonstrate and discuss labs during the workshop.

Workshop Summary
Australian Cyber Conference 2023

ROOM 110	WEDNESDAY 18 OCT | 09:00 - 12:00
COMPANY/ TOPIC	ALC Workshop - Secure Software Development
OUTLINE	As a seasoned white hat hacker, Arni designed this workshop to provide participants with the most current knowledge in web application security. The primary objective is to enhance participants understanding and ability to combat the most significant security threats prevalent today, as identified by the Open Web Application Security Project (OWASP) in their widely recognized Top 10 list
PRE-REQUISITES	NIL

ROOM 111 / 112	WEDNESDAY 18 OCT | 12:40-15:10
COMPANY/ TOPIC	BSI Workshop - Building resilient supply chains – A security perspective
OUTLINE	In today's rapidly changing security landscape, organizations are encountering heightened unpredictability. Consequently, they confront evolving security difficulties that affect their objectives, growth, and brand perception. Stakeholders have intensified their attention and examination of supply chain security, necessitating a systematic approach to address this challenge. This session seeks to offer direction on ensuring the security of the supply chain, encompassing evaluating the security environment, establishing appropriate security measures, ensuring compliance management, and aligning security protocols, procedures, and controls to enhance resilience. Details/Takeaways Organizations are facing increasing uncertainty in today's volatile security environment. As a result, they face security challenges which are evolving and impacting organizational goals, growth and brand reputation. There has been an increased focus and scrutiny on supply chain security by stakeholders and this poses a need to address this challenge systematically. This session aims to provide guidance on: Security assurance of supply chain Assessment of its supply chain's security environment Determining security measures Adequacy of supply chain risk controls Manage statutory, regulatory and stakeholder compliance obligations Align security procedures, processes and controls of the supply chain to ensure resilience.
PRE-REQUISITES	NIL

ROOM 110	WEDNESDAY 18 OCT | 12:50-15:50
COMPANY/ TOPIC	ALC Workshop - Cyber Security First Responder
OUTLINE	This workshop is a crash course to help equip front line staff with the capability and knowledge to be able to respond to an incident in an effective and timely manner. Knowing how to act promptly during an incident can significantly reduce the incident's negative impact and ensure that an incident response investigation can be performed without delay.
PRE-REQUISITES	NIL

Workshop Summary
Australian Cyber Conference 2023

ROOM 109	**THURSDAY 19 OCT | 10:00-15:00**
COMPANY/ TOPIC	**Lessons from the Field: Hacker's Perspective on Your Infrastructure - Paula Januszkiewicz**
OUTLINE	During this workshop, you will learn what are the key threats to the Modern Workplace and what can be done to mitigate them using cutting-edge tools and expert knowledge. We will also share our own experience from projects delivered worldwide.
PRE-REQUISITES	NIL

ROOM 111/112	**THURSDAY 19 OCT | 10:00 - 12:30**
COMPANY/ TOPIC	**AUSCL Workshop - Interactive Executive Risk Focused Cyber Tabletop**
OUTLINE	The importance of cyber tabletop and simulation exercises have been a key cyber resilience theme during 2023. When performed well these exercises allow an organisation and its senior management to understand the key dilemmas and crisis issues that will arise from a complex cyber event, and to practice their decision making and coordination skills. Increasingly, evidence that an organisation regularly conducts cyber tabletops is also being demanded by regulators, clients and stakeholders. Historically tabletops have focused on the technical steps that must be taken by cyber security incidents and incident response teams. While these steps remain important, often the most challenging issues for organisations involve navigating the way in which senior management and leadership must be engaged throughout a crisis, and responding to the cross functional and business decisions which can influence reputational harm, business interruption and legal exposure. To effectively address these issues, tabletops should be designed to explore executive risk issues. This session will provide audience members with the opportunity to engage with and vote on a simulated exercise which has been specifically designed to address executive and senior management risk. The session will be supported by a cross functional panel of experts that will consider the responses and walk audience members through the various issues which arise from a scenario. Audience members attending the session will gain valuable insights into how tabletops of this nature can be delivered and be empowered with the confidence to conduct similar exercises for their organisation. The session will also provide audience members with the opportunity to ask questions and seek guidance on how scenarios can be designed and most effectively delivered.
PRE-REQUISITES	NIL
ROOM 206	**THURSDAY 19 OCT | 10:15-10:55, repeated 11:05-11:45, 13:00-13:40, 13:50-14:30 and 14:40-15:20**
COMPANY/ TOPIC	**Cybermindz**
OUTLINE	A powerful, experiential session which will allow participants to enjoy a full 35-minute immersion into a facilitated state of deep calm through the world leading iRest Protocol led by Cybermindz.org founder Peter Coroneos. In addition, attendees will gain an understanding of the neuroscience behind the success of the protocol and how we are mobilising to bring this burnout prevention and restoration tool to cyber teams — first in Australia, and now the US.
PRE-REQUISITES	NIL

Workshop Summary
Australian Cyber Conference 2023

ROOM 110	THURSDAY 19 OCT | 10:15-12:15
COMPANY/ TOPIC	**Microsoft Immersion Workshop - Into the Breach**
OUTLINE	Join our gamified workshop experience, where you'll participate in the incident response investigation of a ransomware attack on the Health Network. Dive into the simulation and apply your in-depth knowledge of Microsoft Defender for Office 365 and Microsoft Sentinel to stop the hack. Who should attend: • Architects • IT professionals • Cyber defence analysts and incident responders After completing this workshop, you will: • Understand how to use integrated, automated, extended detection and response (XDR) to increase efficiency and effectiveness with Microsoft Defender to keep you secure against threats to identity, endpoints, data, apps and infrastructure. • Be able to detect, investigate and respond to threats using automated investigations and self-healing capabilities. • Know ways to locate threat indicators and entities using advanced hunting features to explore raw data across security pillars. • Recognise how to view alerts and remediate threats across your Microsoft 365 environment from a single dashboard.
PRE-REQUISITES	Please bring your own laptop.

ROOM 111/112	THURSDAY 19 OCT | 13:00 - 15:30
COMPANY/ TOPIC	**AUSCL Workshop - InfoSec and Insurance - What You Need to Know to be a Critical Stakeholder**
OUTLINE	One of the most important developments over the past few years has been the wider business community acceptance that cyber security risk is no longer just a problem that IT teams and InfoSec must manage, and that broad cross functional support is necessary for an organisation to adopt robust approaches for cyber risk management and resilience. This development has seen organisations adopt a broader range of investments in risk management, recovery and risk transference. A consequence of this trend has been the increased take-up of cyber and technology risk insurance products both domestically and globally. Historically many businesses have treated insurance decisions as being primarily within the role of a chief risk officer, or financial officer. However, information security and information technology teams are increasingly becoming a critical component in helping organisations identify and obtain the appropriate cyber and technology risk insurance and are also one of the stakeholder groups within the organisation that are most decisive in obtaining benefits from insurance, and whose needs must be considered to ensure that products are properly sourced and designed. The purpose of this session is to explore how IT and InfoSec leaders can demonstrate why it is important that they have an appropriate seat at the table where insurance decisions are being made, provide key insights into how their skillsets will be impactful in any journey that their organisation undertakes when considering insurance and validating that insurance policies are fit for purpose and will meet the needs of cyber security stakeholders. The session will include a work through of real world scenarios and outcomes that demonstrate the value of IT and InfoSec input. The session will also explore the reason for key questions asked by insurance underwriters and provide insight to help audience members understand how insurance questions can be most effectively answered, and why certain controls and capabilities are particularly important to insurance carriers. The session will also conclude by giving audience members practical insights into key takeaways which they can use within their own organisation to determine whether insurances obtained for cyber and technology risks are appropriate, and whether their organisation is obtaining effective value for money for any insurance decisions made.
PRE-REQUISITES	NIL