ADELAIDESEC

AISA
Cyber | smart · safe · secure

Responding to ransomware in Industrial Control System (ICS)

In this presentation Seth will delve into the increase in ransomware used against industrial control system (ICS) and operational technology (OT). The ransomware used in these attacks has been both targeted and opportunistic in nature. The increase in ransomware attacks has resulted in ransomware becoming the most common cause of compromise in the industrial sector in the past year. Seth will explore and discuss lessons learned from the field how to effectively prepare for, respond to, and remediate ransomware incident in ICS environments.

Over the past five years, Dragos has observed an increase in ransomware used against ICS and OT environments. Previous research conducted by Dragos shows that adversaries are using ransomware to target OT environments more frequently. The ransomware used in these attacks has been both targeted and opportunistic in nature. Targeted ransomware demonstrates ICS-specific capabilities. This is observed by examining the technologies exploited by the ransomware and the potential for operational impacts.

Opportunistic ransomware that lands in OT networks typically disregards underlying operations, and frequently reaches the environment through bleed-over from corporate network infections, bridging the IT/OT divide due to poor network segmentation or lack of other mitigating controls. The increase in cyber attacks has resulted in ransomware becoming the most common cause of compromise. Discover using lessons learned from the field how to effectively prepare for, respond to, and remediate ransomware incident in ICS environments.

Presenter:
SETH ENOKA

TECHNICAL SECURITY AND INCIDENTS
10:45 AM – 11:25 AM
HALL A

ADELAIDESEC

AISA
Cyber | smart · safe · secure

An intelligence practitioner's view on the Australian cyber threat landscape

What do geopolitics, physical security, supply chains and terrorists have in common?

Considering herself to be an "intelligence person first" and "cyber person second", Claudia will draw on her unique expertise in intelligence, physical security and cyber security to ponder this question. She will discuss why an intelligence-led, holistic approach is so important to addressing cyber security.

As the Lead Cyber Intelligence Analyst for Australia's largest end-to-end cyber security provider, Claudia brings an unparalleled view of the Australian cyber threat landscape.

This presentation will be peppered with unique insights into the shape and size of the most significant cyber incidents across the country, including those that don't make the news.

Presenter:
CLAUDIA MULLER

GOVERNANCE, RISK, COMPLIANCE AND STRATEGY
10:45 AM – 11:25 AM
PANORAMA ROOMS 2 & 3

ADELAIDESEC

AISA
Cyber | smart · safe · secure

Get the SAST outta here! Why AST-based static analysis is failing our software engineers and where to go from here

Application Security (aka AppSec) broadly covers what practices we can do to secure our software systems. AppSec practitioners use a variety of automated tools as well as having domain knowledge of the web, programming languages, and general software engineering processes.

In this presentation we will discuss Static Analysis tools (SAST) which inspect source code for security bugs and tell engineers how to fix them. In the past, web applications followed a simple design, the N-tier architecture, and we had such frameworks as MVC and Spring to support this. These needed securing, so a lot of tooling was built to support this. The general design of those tools were to take a relatively constrained combination of programming languages (Java and C#), transpile them into an analysable format, and then run data-flow analysis across them to produce a results file. Unfortunately, they are no longer fit for purpose. Our applications are increasingly becoming ephemeral microservices, we've gone full circle back to event-land, and developers now have complete freedom in their tooling and development processes. That, and the delivery expectations of a modern development shop are fundamentally different, so these tools are now redundant. But never fear! There are alternative methods, and although they might seem simple, they're the way to ultimately go to fit into the new world.

Join this presentation as we discuss the general history of static analysis tooling, where it's falling over, and where the AppSec and broader Product Security industry is heading in this space.

Presenter:
COLE CORNFORD

TECHNICAL SECURITY AND INCIDENTS
11:30 AM – 12:10 PM
HALL A

ADELAIDESEC

AISA
Cyber | smart · safe · secure

Reading the blockchain: What does it tell us about ransomware?

You can read academic journals, you can read trashy romance novels, but did you know you can also ‘read’ a blockchain?

In this presentation we will discuss what a blockchain is, the information publicly available and how we can leverage that information to gain insights into illicit actors and organisations.

Bitcoin first entered our vocabulary in 2008 when evolutionary libertarian ‘Satoshi Nakamoto’ broadcast his vision and ethos of an advanced digital finance age on the world. As such, bitcoin possesses several privacy attributes by design. But don’t be fooled: pseudonymous and anonymous are NOT the same thing. Thanks to intelligence and address attribution, we are afforded a rather detailed insight into bitcoin activity, including when it is used by illicit actors.

So, what does it tell us about ransomware? Who are the groups involved? After a ransom is paid, where does the bitcoin go? Well… let’s take a look.

Presenter:
JONNO NEWMAN

GOVERNANCE, RISK, COMPLIANCE AND STRATEGY
11:30 AM – 12:10 PM
PANORAMA ROOMS 2 & 3

ADELAIDESEC

AISA
Cyber | smart · safe · secure

Track the attack: Enhancing operations by tracking interactive intrusion campaigns with MITRE

With MITRE recently choosing South Australia for its first international applied research centre, it is timely to look at the value and importance of using a framework such as ATT&CK for research into the behaviours and tradecraft of today's adversaries. In this presentation Jai and Hayden will go through how the ATT&CK framework can support organizations in areas such as threat hunting, security operations, and threat intelligence dissemination.

In addition, they will demonstrate real-world examples of how the Falcon OverWatch team uses ATT&CK for tracking intrusions, mapping adversary tradecraft and memorializing the data. Lastly, Jai and Hayden will go through why using a framework such as ATT&CK, to track and document adversary behaviour is crucial to a mature threat hunting function.

Key takeaways:

- Gain a practical understanding of how to use the ATT&CK framework
- Understand why it's beneficial to track and document the behaviours of adversaries
- See how ATT&CK can support threat hunters and defenders alike
- Learn to use ATT&CK as a tool to simplify communication and reporting of adversary tradecraft to stakeholders

Presenters:

JAI MINTON & HAYDEN DIMMICK

TECHNICAL SECURITY AND INCIDENTS

1:15 PM – 1:55 PM

HALL A

ADELAIDESEC

AISA
Cyber | smart · safe · secure

Embedding new ISO 27002:2022 requirements into your ISMS

In this presentation, Yvonne will go beyond the basic mapping of old ISO 27002 to new. She will give a reflection on past experiences and outline what you need to get in place to certify to the new standard.

Covering some of the basic triggers needed to support change for those that are already certified, enabling you to progress slowly or jump in to become one of the first to be certified under the new ISO 27001 standard!

For those that are not currently certified or just want to 'comply' to the requirements, Yvonne will also outline some of the new control areas, looking at how these changes can be of benefit to your security program.

Key takeaways:

- Create a plan to update your certification to ISO 27002:2022
- Understanding the new control requirements and how they can enhance your security program

Presenter:
YVONNE SEARS

GOVERNANCE, RISK, COMPLIANCE AND STRATEGY
1:15 PM – 1:55 PM
PANORAMA ROOMS 2 & 3

ADELAIDESEC

AISA
Cyber | smart · safe · secure

Security considerations for machine learning systems

In this presentation, Joshua will discuss ‘Adversarial Machine Learning’ and Machine Learning (ML) security issues more broadly, framing this as an important emerging challenge for cyber security. Joshua will outline ML security considerations and practices from a few different perspectives including development, deployment, red teaming and governance.

ML techniques and technologies have developed rapidly in recent years and are now being adopted across a wide range of applications – from autonomous vehicles to cyber security tools. ML is viewed as key to unlocking value in data, providing predictive insights and autonomous decision making, at a scale and tempo not otherwise possible. But there are downside risks. While issues around ethics, bias, explainability and privacy have gained some broad awareness, there is less recognition of ML vulnerability and insufficient thought to security and robustness.

Presenter:
JOSHUA GREEN

TECHNICAL SECURITY AND INCIDENTS
2:00 PM – 2:40 PM
HALL A

ADELAIDESEC

AISA
Cyber | smart · safe · secure

The continuing criminal enterprise: A 20 year review of cyber crime development

It is always said that the threat from cyber crime has evolved. But the real threat – the organised crime groups behind the malware – has stayed fairly constant.

Drawing on more than 20 years' experience investigating (and in some cases arresting) cyber criminals, Alex will discuss about how the landscape has evolved and changed as both criminals and network defenders have gotten better, smarter and more sophisticated.

Alex will present a light speed journey through the history, current day and potential future of cyber crime and some of its most colourful characters.

Presenter:
ALEX TILLEY

GOVERNANCE, RISK, COMPLIANCE AND STRATEGY
2:00 PM – 2:40 PM
PANORAMA ROOMS 2 & 3

ADELAIDESEC

AISA
Cyber | smart · safe · secure

Lessons learned from Lapsus$

A new breed of criminal has emerged in hacker town and the most notorious amongst them, goes by the name Lapsus$. This hacking group uses DDoS and other threats to target some of the giants in the tech world – Microsoft, Samsung, Nvidia, and more recently, Okta.

In January 2022, Okta, who is an authentication company that is used by more than 15,000 organisations, was breached by Lapsus$. In Okta's investigation it was found that the threat actor actively had control of an individual workstation that was used by a Sitel support engineer, with access to Okta resources. The hackers were ultimately unable to perform any configuration changes or authenticate any Okta accounts.

In this presentation Brett, CSO APJ from Okta, will outline how Okta's platform inhibited and frustrated this attempt, discusses the investigation and findings as well as offering some broader lessons learned from the event.

Presenter:
BRETT WINTERFORD

TECHNICAL SECURITY AND INCIDENTS
2:45 PM – 3:25 PM
HALL A

ADELAIDESEC

AISA
Cyber | smart · safe · secure

Passwords, antigravity and why security threats flow uphill

In today's digital world, password management isn't just some abstract idea that might make your life easier. It's a critical part of comprehensive security — passwords are often the first place that hackers look for easy entry into vulnerable computers and devices.

A 2016 Verizon study found that 63% of confirmed data breaches involved weak, default, or stolen passwords, while recent high-profile password leak stories involving companies like LinkedIn, resonate throughout social media. So, no matter how strong you think your passwords are, remember this: hacking software can test up to 10 billion password combinations in seconds!

As a forensic examiner, Sam's exposure to a large volume of cases and specialist tools has given him large insight into how people create passwords especially when they are forced to comply with arbitrary company rules. Its 2022 and kids and spouses' names are all the rage, now they just have exclamation marks at the end!

In this presentation, Sam will explore why physically enabled breaches of small companies now easily flow upstream to affect larger businesses and hurt consumers in the long run. Armed with this information, hopefully it will inspire you to move towards a passwordless authentication and two-factor authentication (2FA) as soon as possible!

Presenter:
SAM BRUCE

GOVERNANCE, RISK, COMPLIANCE AND STRATEGY
2:45 PM – 3:25 PM
PANORAMA ROOMS 2 & 3