paloalto NETWORKS | UNIT 42

Cyber Risk Management workshop

PaCSON
PACIFIC CYBER SECURITY OPERATIONAL NETWORK

Helen Teixeira, Director | Unit 42 - JAPAC

Intelligence Driven. Response Ready

PALO ALTO NETWORKS

Agenda

1. Introductions - me & Unit 42
2. What is Cyber Risk Management?
   1. Process, terms & concepts
   2. Cyber risk analysis better practices
   3. Risk reporting
3. Why is this important?
4. Current challenges
5. Practical steps to effectively manage Cyber Risk
6. Key takeaways

1. Introductions

Dr Helen Teixeira

- **Consulting Director, Unit 42 JAPAC**
- Previously:
  - **Deep technical knowledge** combined with cyber risk management expertise
  - Former **Managing Director** in Big 4 Consulting
  - International experience and insights having operated across Brazil and JAPAC

- Co-Chair **FAIR Institute** Sydney Chapter since 2018, promoting cyber risk quantification for effective decision-making.
- Performed numerous independent cyber risk assessments and cyber program reviews across FSI, retail, education and the telecommunications sectors, providing defensible and prioritised risk remediation strategies for the most effective use of limited resources (people, time and budgets) and optimised return on security investments.
- Holds a PhD in Physics, and industry qualifications such as Certified Information Security Systems Professional ("CISSP"), GIAC Certified Web Application Penetration Tester ("GWAPT"), Open FAIR Foundation Certified, ISO 27001 Lead Auditor, former PCI DSS and Payment Application (PA DSS) Qualified Security Assessor.

UNIT 42 THREAT INTELLIGENCE & RESEARCH

200+ Threat Researchers

- Reverse engineering
- 10+ years of historical malware analysis growing by **30M** samples a day
- Threat modeling
- Multiple awards for vulnerability research

Depth and Breadth of Telemetry

- **85k+** customers
- **500BN** events per day from endpoint, network, cloud
- **1k+** Incident response engagements per year
- Managed Detection & Response & Threat Hunting

Partnerships and Open Source Data

- Open source gathering
- **75+** third party feeds
- Cyber Threat Alliance, **6M** observables/month
- Law enforcement, government, military partnerships

3. Why is this important?

Cyber related impacts

Confidentiality

Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information

Availability

Ensuring timely and reliable access and use of information

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity

Safety

Expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered

- **Privacy regulations**
  - **EU-GDPR**: Max 20,000,000 Euros or 4% annual turnover (whichever greater)
  - **UK-GDPR**: Max £17,500,000 or 4% annual turnover (whichever greater)
  - **AU Privacy Act 2018**
    - Notifiable Data Breach since 2018
  - **NZ Privacy Act 2020**

THE THREAT LANDSCAPE IS INTENSIFYING

Speed

45% of the time, compromise-to-exfiltration happened in less than a day

Scale

39% of IR cases, internet facing vulnerabilities were the initial access point

Sophistication

13 Days was the medium dwell time in 2023, decreased by half since 2021

6. Key takeaways

Key takeaways

Identify Crown Jewels

Resources (people, time & budgets) will always be limited

Prioritise Crown Jewel assets initially

Understand Attack Surface

You can’t protect what you don’t know

Continuous view of assets (external and internal) is key

Prepare & test for probable threats

Prepare for when, not if ..

Use data driven approaches and simulations to prepare & improve

Leverage partnerships

Know your key third parties

Leverage trusted partners for information sharing and support

UNIT 42®

BY PALO ALTO NETWORKS

Thank you