Independent Schools Queensland - ICT Managers Forum

Landmarks on your Cyber Security Journey

May 2023

SECURE
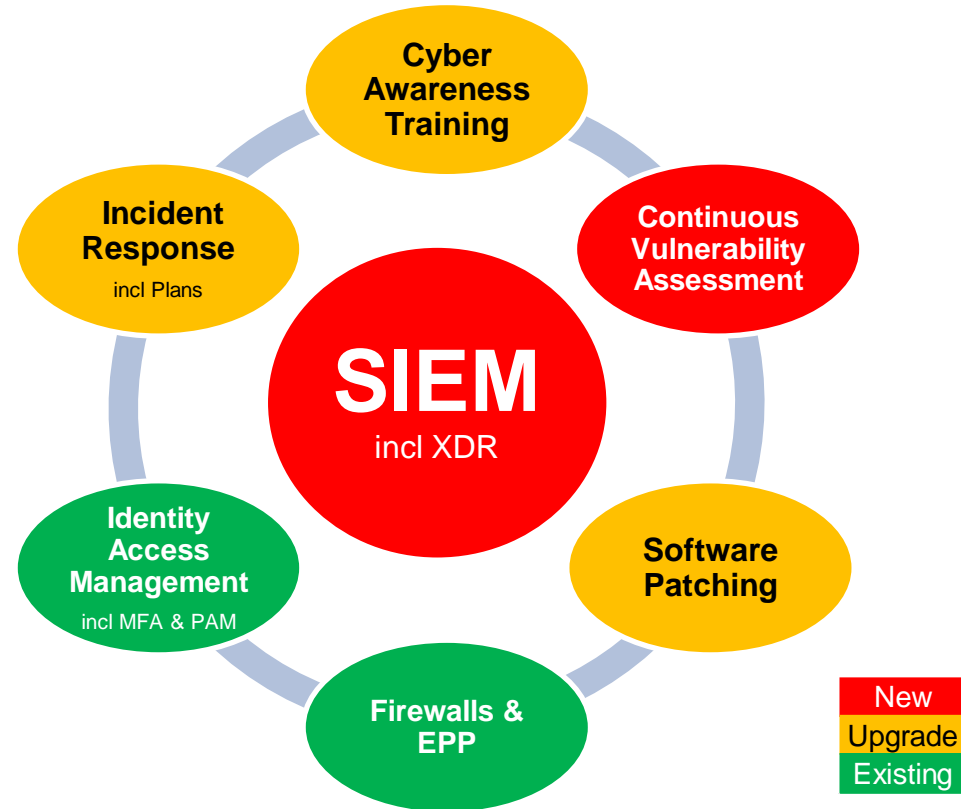ISS

Defence in Depth Security

Current Situation

Large technology environments
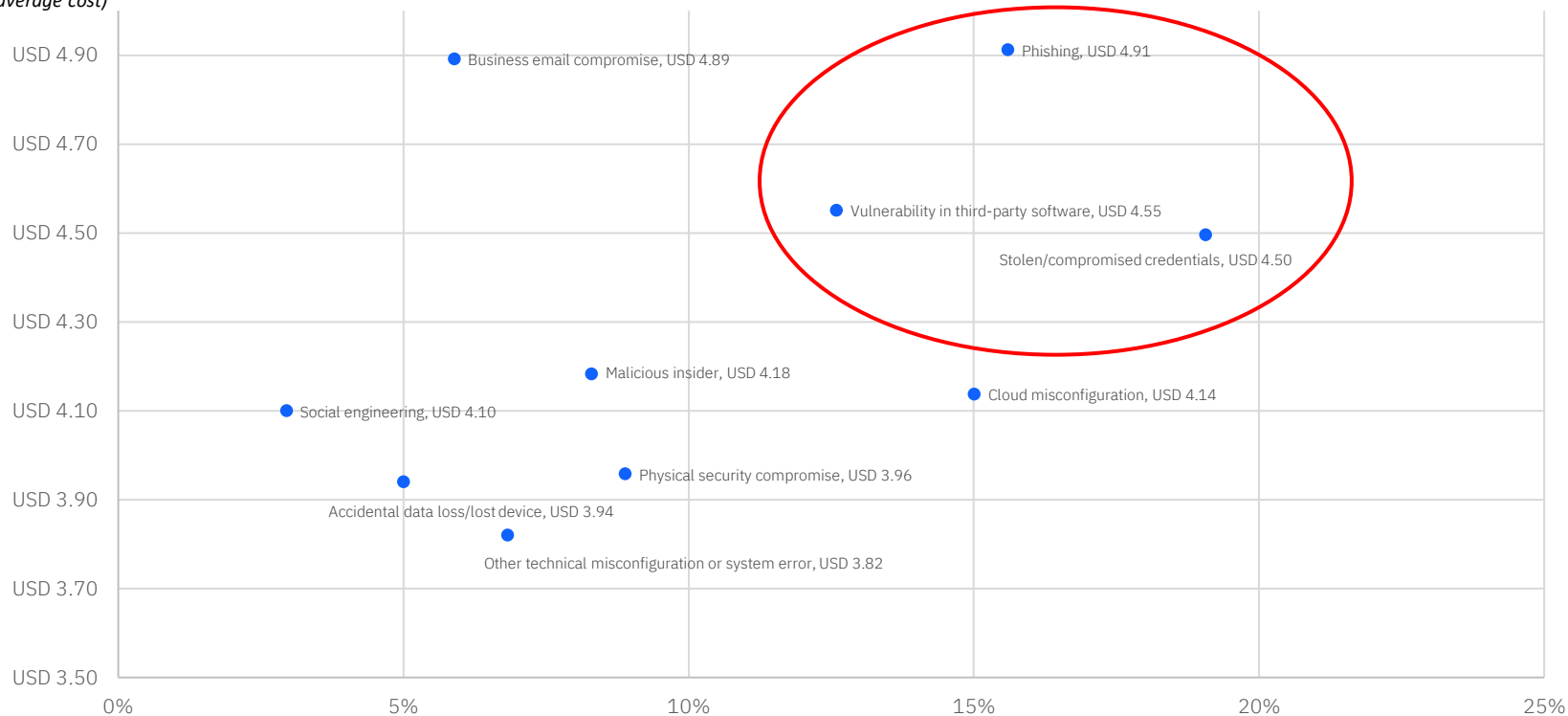
with many users

Complications

Limited budgets

Lack of human resources
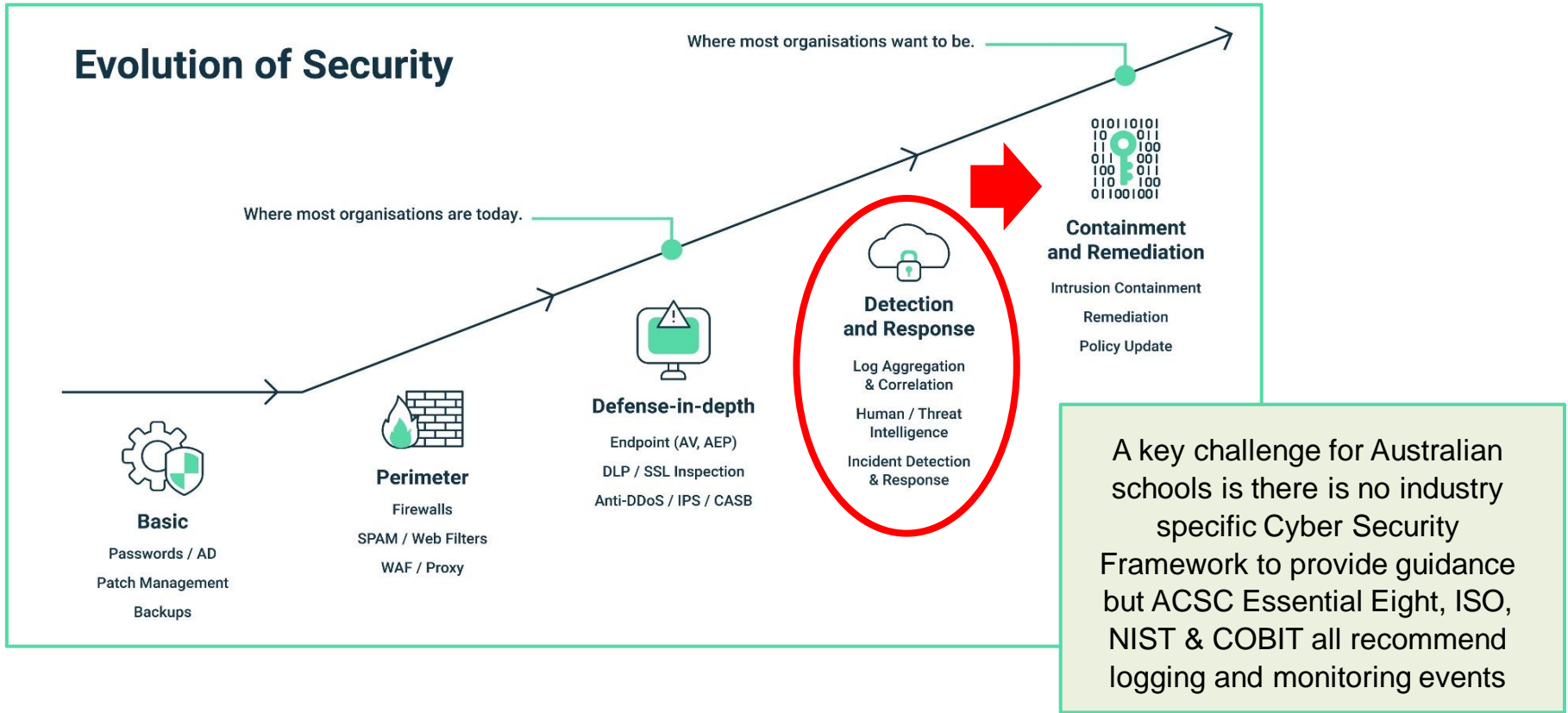
Lots of security vendor speak

- Cyber Awareness Training
- Continuous Vulnerability Assessment
- Incident Response incl Plans
- SIEM incl XDR
- Software Patching
- Identity Access Management incl MFA & PAM
- Firewalls & EPP

New
Upgrade
Existing

Cost of Data Breach

Cost USD millions (average cost)

USD 4.90 — Business email compromise, USD 4.89 • Phishing, USD 4.91

USD 4.70

USD 4.50 — Vulnerability in third-party software, USD 4.55 • Stolen/compromised credentials, USD 4.50

USD 4.30

USD 4.10 — Malicious insider, USD 4.18 • Cloud misconfiguration, USD 4.14 • Social engineering, USD 4.10

USD 3.90 — Physical security compromise, USD 3.96 • Accidental data loss/lost device, USD 3.94 • Other technical misconfiguration or system error, USD 3.82

USD 3.70

USD 3.50

0%   5%   10%   15%   20%   25%

Source: Ponemon Institute – Cost of Data Breach report 2022

Frequency of data breach by initial attack vector

Cyber Maturity Roadmap

A key challenge for Australian schools is there is no industry specific Cyber Security Framework to provide guidance but ACSC Essential Eight, ISO, NIST & COBIT all recommend logging and monitoring events
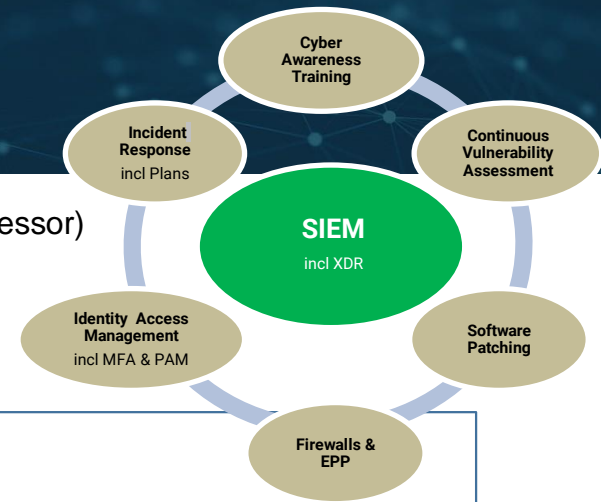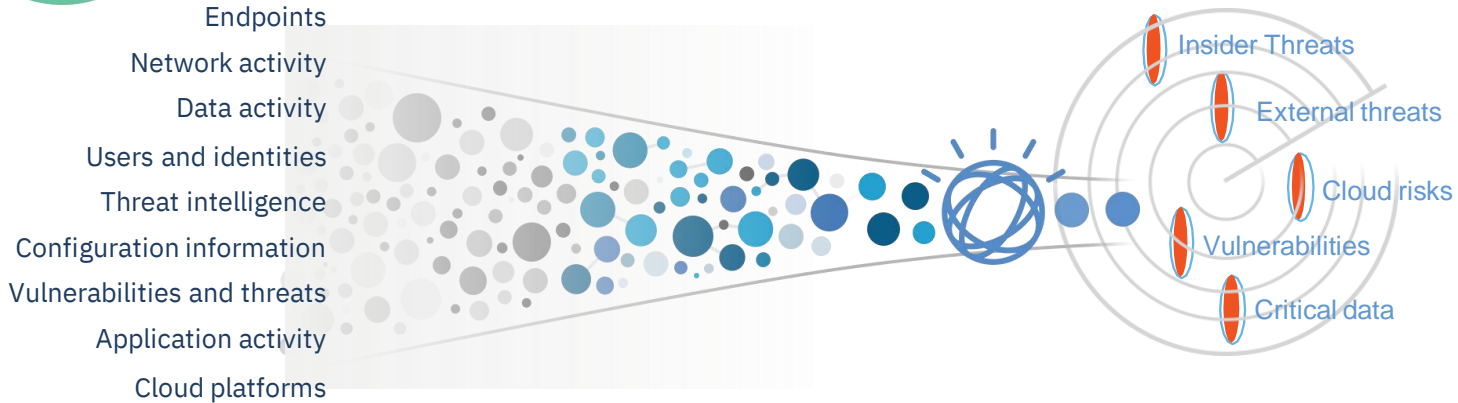
School Case Study

Security Event Monitoring

- IBM QRadar Virtual SIEM Appliance (Event Collector + Processor)

- IBM QRadar Threat Intelligence (X-Force) subscription

- Dedicated Security Analyst point of contact

SIEM TECHNOLOGY

24/7 SOC RESOURCES

THREAT INTELLIGENCE

Cyber Awareness Training

Incident Response
incl Plans

Continuous Vulnerability Assessment

SIEM

incl XDR

Identity Access Management
incl MFA & PAM

Software Patching

Firewalls & EPP

IBM QRadar (SIEM)
Complete Visibility, Prioritised Threats

Endpoints
Network activity
Data activity
Users and identities
Threat intelligence
Configuration information
Vulnerabilities and threats
Application activity
Cloud platforms

Insider Threats
External threats
Cloud risks
Vulnerabilities
Critical data

IBM QRadar (SIEM) ingests and **Correlates** events from all available log sources in **Real-Time** ensuring threat alerts are **Prioritised**

ISQ offers

Security Event Monitoring

Security Event Monitoring	Secure ISS	School Resource
Deployment of virtual appliance(s) to collect and store security logs	☑	
Integration into IBM QRadar Management Console (SIEM)	☑	
Tuning	☑	☑
Monitoring & Detection (24x7)	☑	
Security Analyst - Reporting and Notification Period (8x5)	☑	
Threat Intelligence (IBM X-Force + collection/sharing of school threats)	☑	
Cloud Security Monitoring	☑	
Incident Management (Triage, Investigate, Analyse)	☑	
Security Operations Centre Touchpoints:	☑	
Live Updates of Security Incidents	☑	
Monthly Security Operation & Governance Reporting	☑	
Incident Response (Disrupt & Contain)		☑
Incident Remediation		☑

SIEM

Incl XDR

- Cyber Awareness Training
- Continuous Vulnerability Assessment
- Software Patching
- Firewalls & EPP
- Identity Access Management incl MFA & PAM
- Incident Response incl Plans
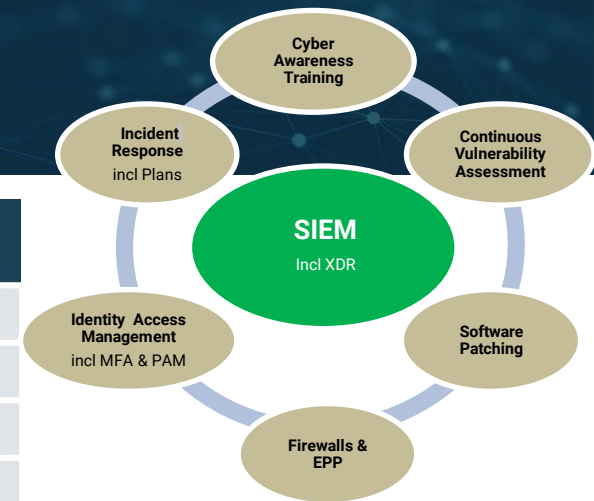
- **Pricing is $1 per month, per enrolled student**

- 12-month subscription

- Reporting & Notification is on an 8 x 5 basis except for P1 & P2 events (24 x 7)

- Secure ISS is available for Incident Disruption & Containment services (additional charges apply $350 p/h)

Security Event Monitoring with XDR

- Extend your schools Detection and Response capability through EDR technology on your endpoints

- We recommend Sentinel One – Singularity Complete as it consistently tops the MITRE Engenuity™ ATT&CK® Evaluation https://secure-iss.com/wp-content/uploads/2022/11/mitre-22-wp.pdf

- Coupled with our Security Event Monitoring service schools benefit from a 24 x 7 Monitoring, Detection & Response XDR capability to mitigate attacks in your environment

- Includes all the service inclusions of Security Event Monitoring along with Sentinel One – Singularity Complete licences for your Servers and Privileged Users
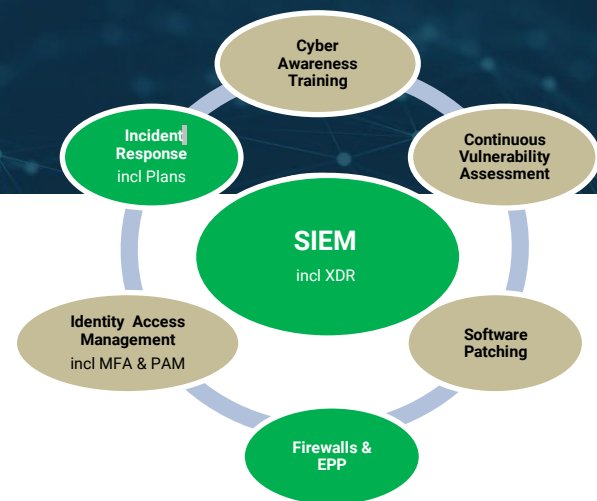
For ISQ members we are offering Security Event Monitoring with XDR at
$2 per month, per enrolled student

Current School Users
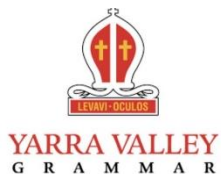
To find out more

- Visit www.secure-iss.com

- Follow us on Linkedin https://au.linkedin.com/company/secure-iss

- Or if you would like to meet to discus the offers further please contact:

> Ian Cooper
> Commercial Director
> 0448 761-634
> icooper@secure-iss.com

Thank You