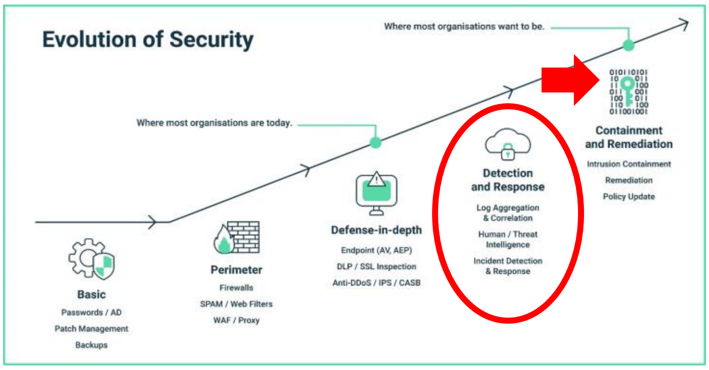
IBM Silver Partner

SECURE ISS

Security Event Monitoring

With Phishing, Third Party Software Vulnerabilities, Stolen/Compromised Credentials, Distributed Denial-of-Service (DDoS) and Ransomware attacks on the rise Secure ISS is proud to offer schools a 24/7 Security Event Monitoring service.

The service is designed to provide an additional detection layer to help protect your school's data and assets when threats evade common security controls.



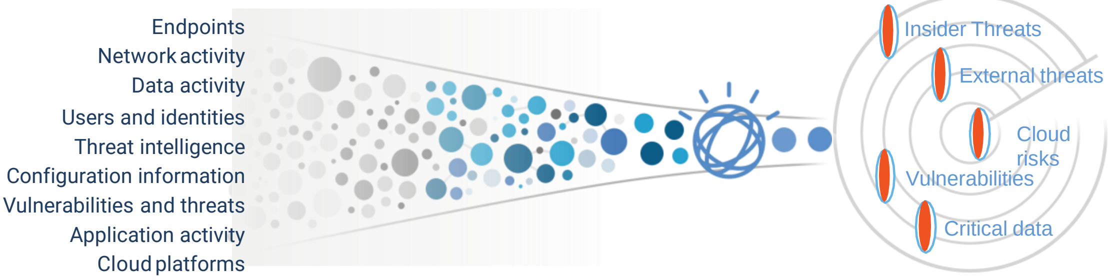
How it Works

A virtual IBM QRadar appliance is deployed in your school environment to collect and store security event logs from the following security controls and devices and forwards them to the Secure ISS 24/7 Security Operations Centre:

- Firewall Ingress / Egress
- Critical IT Servers
- Corporate Servers
- DMZ Servers
- Switches
- IoT Devices
- Endpoint Devices
- Cloud Security Logs

IBM QRadar (SIEM)

Complete Visibility, Prioritised Threats



Our market leading* IBM QRadar SIEM correlates this different information and aggregates related events to create single alerts resulting in accelerated incident analysis, response and remediation instructions from our experienced team of Security Analysts. **Gartner Magic Quadrant for SIEM*

People, Process and Technology

Importantly it's not just about the Technology but the coming together of People and Processes as well.

Our security team is based out of our 24/7 Security Operations Centre (SOC) with eyeballs on screen undertaking all triaging, investigations and issuing or actioning of remediation activities.

Coupled with processes including SOC Advisories and Monthly Governance Reporting and the application of threat intelligence feeds from IBM X-Force and AusCERT schools can benefit from an improved security posture.

SIEM TECHNOLOGY
24/7 SOC RESOURCES
THREAT INTELLIGENCE

Security Event Monitoring

Service Overview

Security Event Monitoring	Secure ISS	School Resource
Deployment of virtual appliance(s)	☑	
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 Operations & Governance Reporting	☑	
Incident Response (Disrupt & Contain)		☑
Incident Remediation		☑

Pricing

$1 per month, per enrolled student

- The pricing structure is based on the number of student enrollments, to provide a scalable solution for all schools.
- Pricing provided is an estimate only with a school IT architecture questionnaire to be completed during the onboarding process to confirm.
- All implementation costs are included in the monthly pricing.
- Pricing is based on a one (1) year minimum subscription term.
- Other services, including incident response and remediation activities, are also available.

Expected Outcomes

- On average our existing school customers experience 9,000 malicious interactions each day resulting in 12 security offences for investigation by our SOC analysts.
- By undertaking response activities (Disrupt, Contain & Remediation) customers save >80% of typical Managed Detection & Response (MDR) charges.
- On average ~1 actionable ticket per day is issued detailing preventative, incident response (disrupt & contain) and remediation instructions for school IT resource actioning.
- Our SOC analysts are always available via phone or email to assist if required.
- We recognise schools may also need assistance with responding to P1 System Compromise security events outside of normal business hours (further charges apply).

Benefits

The costs, both financially and reputationally, of a successful cyber attack on a school are considerable. With 24/7 Security Event Monitoring schools benefit from:

- Continuous, proactive, 24/7, 365 days a year; monitoring; additional layer of security.
- Visibility and faster detection, analysis and response to threats.
- Better compliance via monthly reporting, log collection and retention.

> *"Since engaging Secure ISS to support our Cyber Resilience program in early 2019, we've seen improved threat detection capability, visibility of what's going on and faster responses to incidents when they are happening. The partnership model implemented has combined the best of Secure ISS with our internal IT team to deliver value for money outcomes against our core IT Security objectives."*
>
> **Phil Callil**
> **Director of IT & Digital Learning**
> **Yarra Valley Grammar**