



# Security Information and Event Management

## DEFEAT THREATS WITH ADVANCED DETECTION, AND A UNIFIED VIEW OF YOUR IT SECURITY

In a volatile and fast changing threat landscape, security information and event management (SIEM) plays a vital role in keeping your business productive by defending your IT infrastructure against malicious attacks and protecting vital business and customer data.

Built on the industry-leading Splunk Enterprise, Harbour IT Security Information and Event Management offers a fast, efficient and scalable solution for staying on top of security threats. Managed from our Sydney-based security operations centre (SOC) by a team of experienced, certified security analysts, Harbour IT SIEM not only solves common security use cases, but detects and defends against advanced threats as well. With advanced analytics-based detection and automated response processes, Harbour IT SIEM also decreases time to remediation.

### HARBOUR IT SIEM BENEFITS:

- Adhere to compliance standards
- Reduce security risks
- Maintain auditable records of security information and events
- Detect and respond to threats
- Gain access to our Certified Security Experts
- Improve troubleshooting and incident response with centralised, searchable logs
- Protect your business by staying ahead of ransomware
- Built on industry leading SIEM platform - Splunk

### HARBOUR IT SIEM

#### Threat detection

Correlate events from multiple sources to detect threats faster.

#### Improved incident response

Limit damage and reduce recovery time and cost

#### User monitoring

Pinpoint breaches and uncover misuse

#### Threat intelligence

Recognise abnormal activity, assess the risks, and prioritise your response

#### Advanced analytics

Automated analysis and machine learning produces insights from masses of data

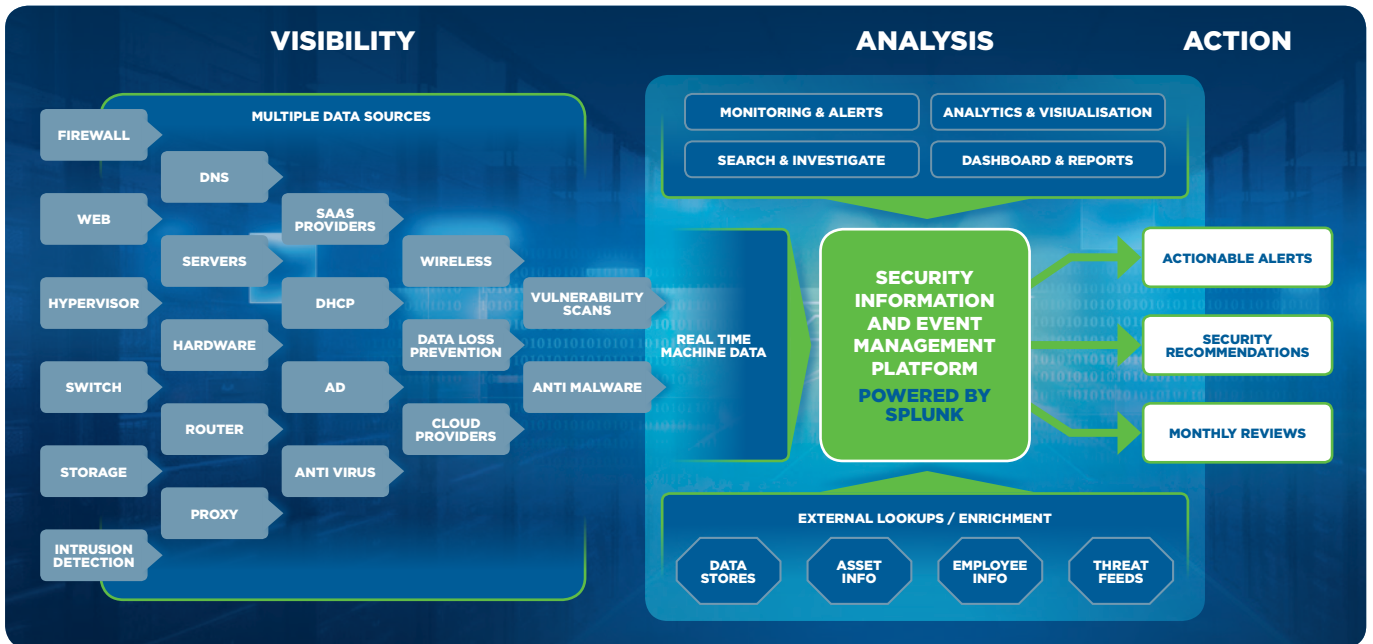
#### Advanced threat detection

Monitor, analyse and detect threats across the kill chain

**SMART DETECTION AND SECURITY EVENT MANAGEMENT ARE CRITICAL TO ANY ORGANISATION'S SECURITY MANAGEMENT FRAMEWORK.**



*John Levido*  
Head of Security Solutions, Harbour IT



## SMART, SCALABLE, ANALYTICS-DRIVEN SIEM

With a multitude of access points to your business infrastructure and data, security information and event management (SIEM) is an essential means of staying ahead of security threats, both external and internal. However, it can be complex to set up your own system, expensive to maintain and requires highly trained staff for ongoing management.

Harbour IT makes it simple and cost effective to enjoy the benefits of an industry-leading SIEM in your business. Get machine learning, automation and data insights on your side in a smart, highly responsive and agile security information platform. Powered by Splunk, Harbour IT SIEM gives your business the technology advantage against cyber attacks with a proven, big data-based security intelligence platform that will also reduce the workload of your IT team.

Harbour IT SIEM can also be deployed as part of our complete suite of security services and solutions.

**TO ENQUIRE ABOUT HARBOUR IT SIEM, SEND US AN EMAIL AT: [ENQUIRIES@HARBOURIT.COM.AU](mailto:ENQUIRIES@HARBOURIT.COM.AU)**

### KEY FEATURES:

- Instantly centralises and aggregates security events
- Correlates threat detection across a range of data sources
- Detects ransomware outbreaks
- Supports any machine data plus a variety of collection mechanisms
- Provides ad hoc searching and reporting for advanced breach analysis
- Generates insights for detailed investigation and incident analysis
- Reports on security and compliance
- Managed by Harbour IT's certified security engineers

**LEARN MORE AT: [HARBOURIT.COM.AU/IT-SECURITY/SIEM](https://www.harbourit.com.au/it-security/siem)**

**SYDNEY** Building A, The Park Estate, 5 Talavera Rd, Macquarie Park NSW 2113

**MELBOURNE** Level 10, 401 Docklands Drive, Docklands, VIC 3008

**BRISBANE** Ground floor, West Tower, 410 Ann Street, Brisbane, QLD 4000