Insider Threat & The Trusted Insider

Site: www.shadowsight.io Phone: 1300 410 900 Mail: shadowsight@secmon1.com

Christopher McNaughton

Director SECMON1
Director ShadowSight™

Email christopher.mcnaughton@secmon1.com
Mobile – 0428183095

Previous Roles

General Electric (Global)

- Senior Director – Global Cyber Forensics, Investigations and Insider Threat

Victoria Police

- Detective - 24 Years (State Crime Squads and Divisional Branches)
- Computer Crime Squad , Senior Forensic Examiner – 8 Years

Academic Background

- Melbourne University
- The United Kingdom Royal Military Academy of Science

What is Insider Threat

An insider threat is a threat to an organisation that comes from people within the organisation and may involve fraud, the theft of customer or commercially sensitive information, unauthorised access or the sabotage of computer systems.

Insider Threat – Why Worry

1. Damage to reputation: If an insider were to leak sensitive or confidential information, it could result in a loss of public trust in the organization, damaging its reputation and potentially resulting in financial losses.

2. Financial losses: An insider threat could result in financial losses through theft, fraud, or other malicious activities. This could have a significant impact on the organization's bottom line and its ability to operate effectively.

3. Legal and regulatory consequences: Depending on the nature of the insider threat, an organization could face legal or regulatory consequences, such as fines or lawsuits, if it is found to have been negligent in protecting its assets.

4. Intellectual property theft: Insiders with access to proprietary information, such as trade secrets or intellectual property, could steal that information and use it for their own personal gain or to benefit a competitor, potentially harming the organization's competitiveness.

5. Cybersecurity risks: Insiders with access to sensitive data or IT systems could pose a cybersecurity risk by intentionally or unintentionally exposing vulnerabilities or bypassing security measures.

Why worry - Australian Government Advice

Information Security Manual

- Security Control: ISM-1625
- A trusted insider program is developed and implemented.
- As a trusted insider's system access and knowledge of business processes often makes them harder to detect, establishing a trusted insider program can assist an organisation to detect and respond to trusted insider threats before they occur, or limit damage if they do occur. In doing so, an organisation will likely obtain the most benefit by logging and analysing user activities.

Information Security Protective Security Policy Framework (PSPF)

- The PSPF identifies insiders as an emerging threat who can steal or destroy data and prevent systems from functioning
- The PSPF describes how organisations should manage the risk of malicious or unwitting insiders

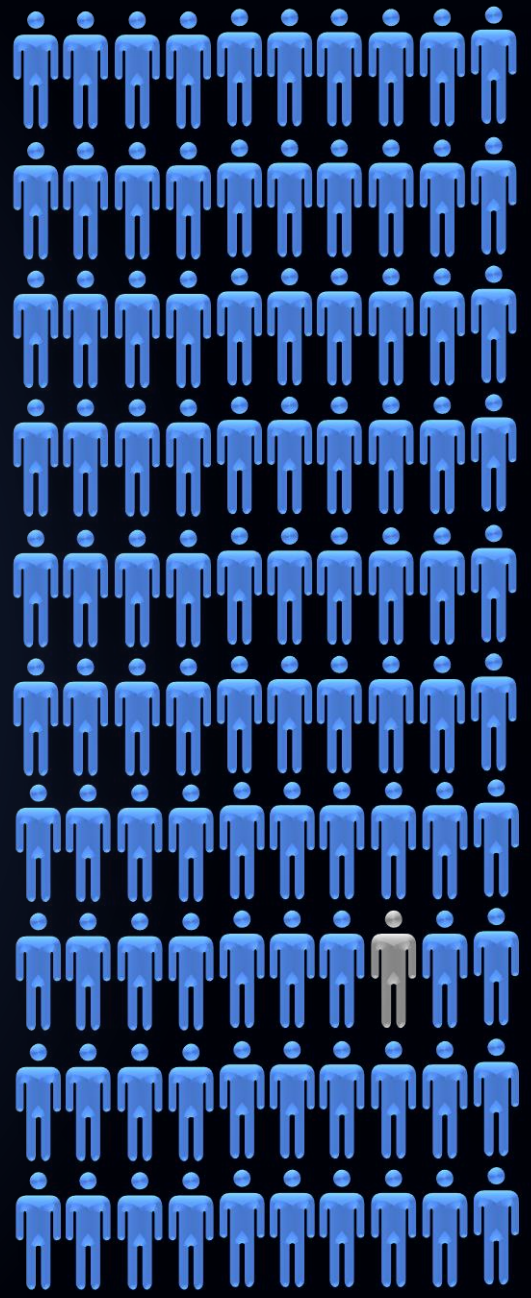
Insider Threat Motivators

- Inadvertent & accidental
- Lack of awareness
- Insufficient infrastructure
- Pressure to get the job done
- Enhancing opportunities in a future role
- Greed
- Revenge
- State sponsored attack
- The noble insider

Insider Threat – The Challenge

For companies of any size, Insider Threat – unsanctioned activity by employees – is often unintentional but potentially devastating.

Only 1% of activity is malicious



CASE STUDIES

Case Studies

Fraud

- Financial Institution
- Helpdesk Operator
- Detection sources - CRM, Doc management & Email

Result

- Arrested and charged

Data Leakage

- Financial Institution
- Database administrator
- Detection sources – Database commands & Email

Result

- Guidance provided

State Sponsored Attack

- Multi industry global organisation
- Application developer
- Detection sources – Endpoint software, Internet proxy & DLP

Result

- Terminated

Negative Sentiment

- Healthcare provider
- Administration officer
- Detection sources – Sentiment analysis, Email

Result

- HR engaged to support the staff member

SOLVING INSIDER THREAT

Insider Threat – Common Solutions

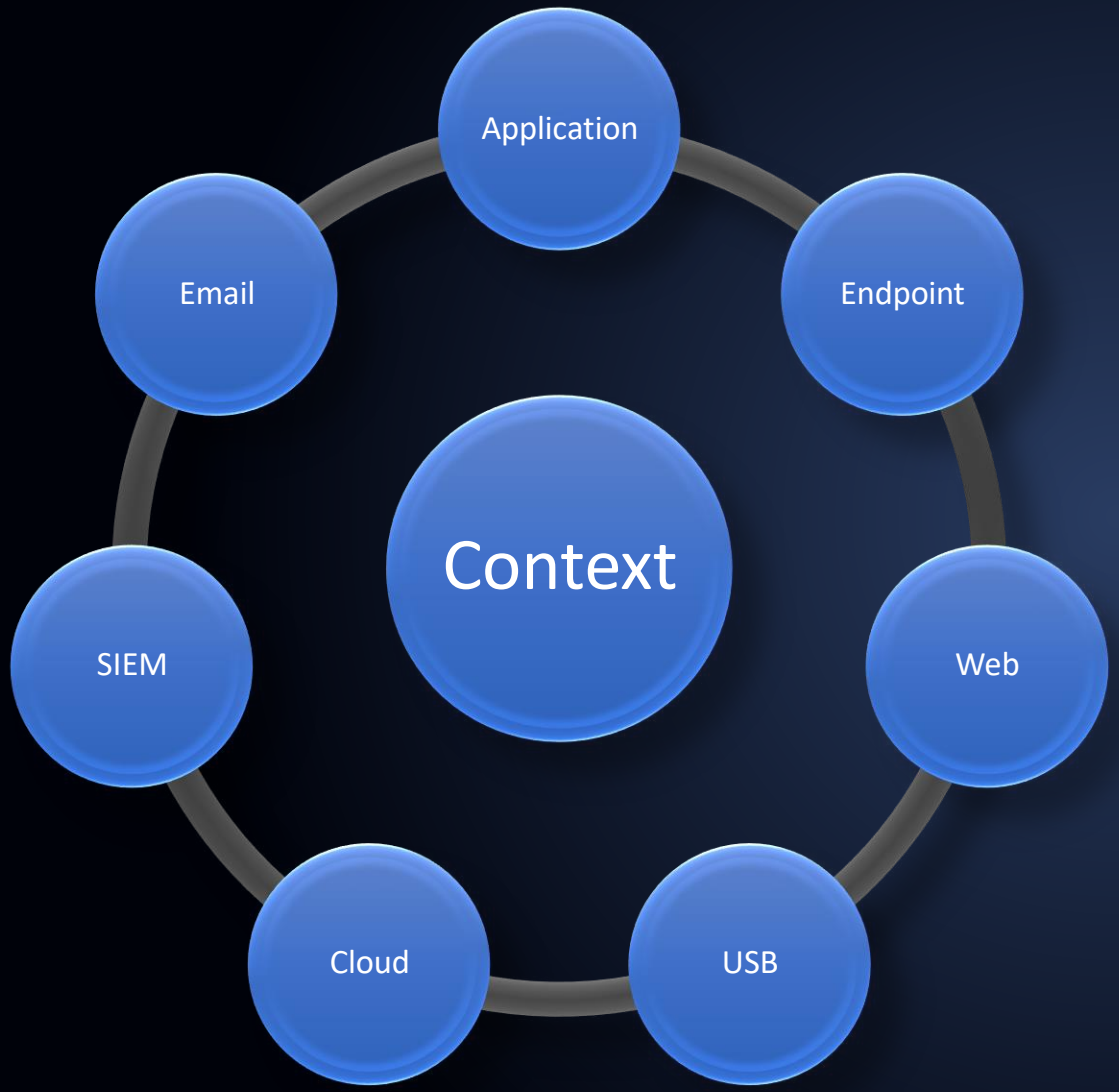
Existing approaches to managing Insider Threat often involve installing endpoint Insider Threat detection software or collecting every system log in the hope that malicious users will be identified.

This approach creates giant data sets with huge number of alerts that are impossible to consume. The result is an avalanche of false positives.

Imperatives to Success

- Review all user activity
- Alerts are timely & relevant
- Very low/no false positives
- Alert process integrated into the business

Leveraging Events and Context



User Behaviour Analysis

There are two key elements to successful user behaviour analytics (UBA)

- Contextual information (examples)
  - HR data
  - Data classification
  - Activity time of day
  - Negative sentiment
- Events

The contextual information provides an enhanced risk view of user activity

Correlation

Correlation of both contextual information and user activity from various key sources provides a very powerful picture of the user's mindset and intent.

Where do you start?

1. Assess the insider risk
    a. Fraud
    b. Data leakage
    c. Unauthorised access
2. Are there user activity logs?
3. Analyse the activity?
4. Report undesirable activity to the business

SHADOWSIGHT

What is ShadowSight

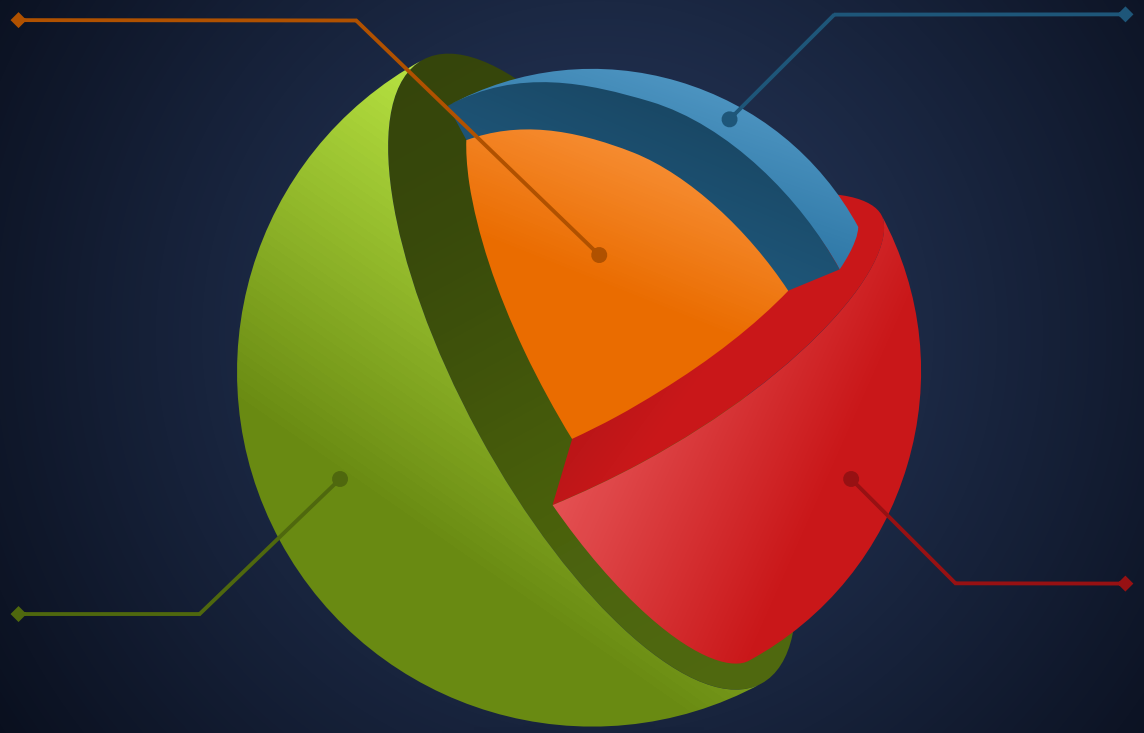
ShadowSight is an Insider Threat detection and response platform which incorporates.

- Risk based user activity analysis
- User activity historical database
- Supports both proactive and reactive investigations
- Machine learning based – It evolves with the business

ShadowSight Detection

ShadowSight™ Baseline
ShadowSight™ comes with many detection rules in place based on years of detection experience

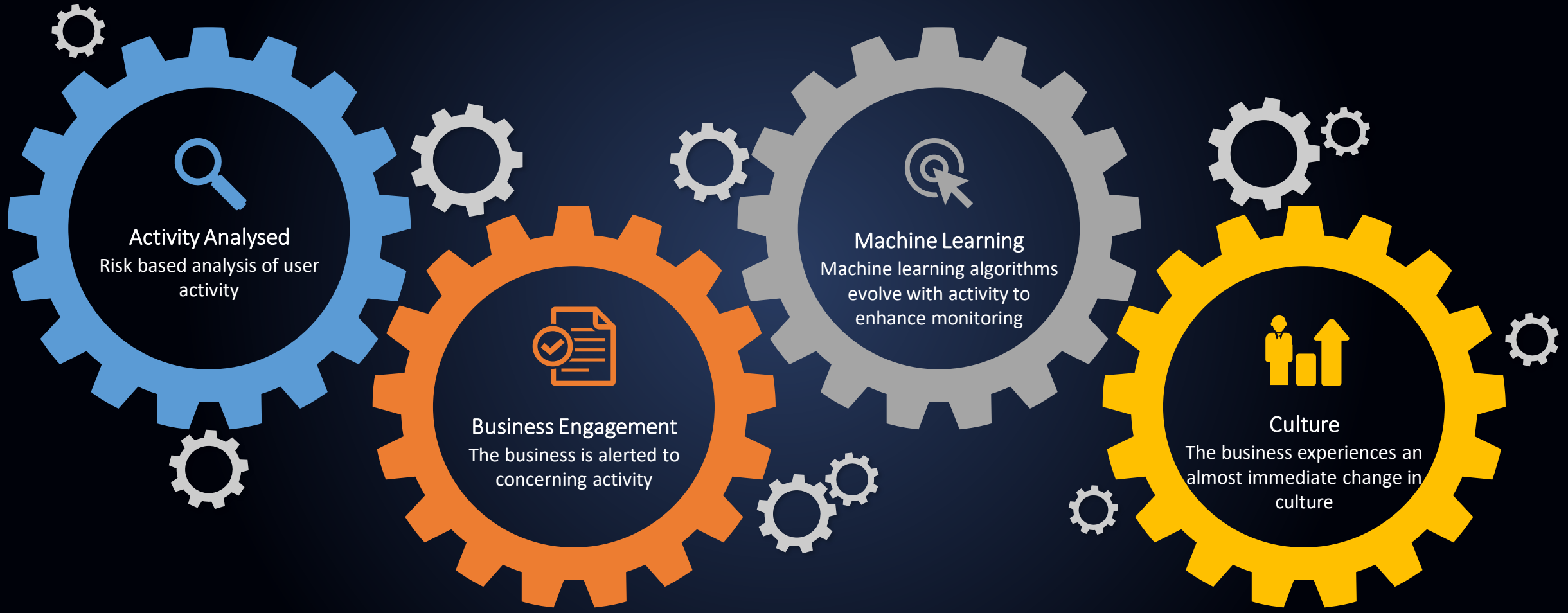
Business Context
Our initial assessment means we are incorporating the correct logs into ShadowSight™ to ensure it is analysing the appropriate user activity



Machine Learning
From day 1 ShadowSight™ is learning from your business and adjusting detections based on current threats, evolving trends and business change

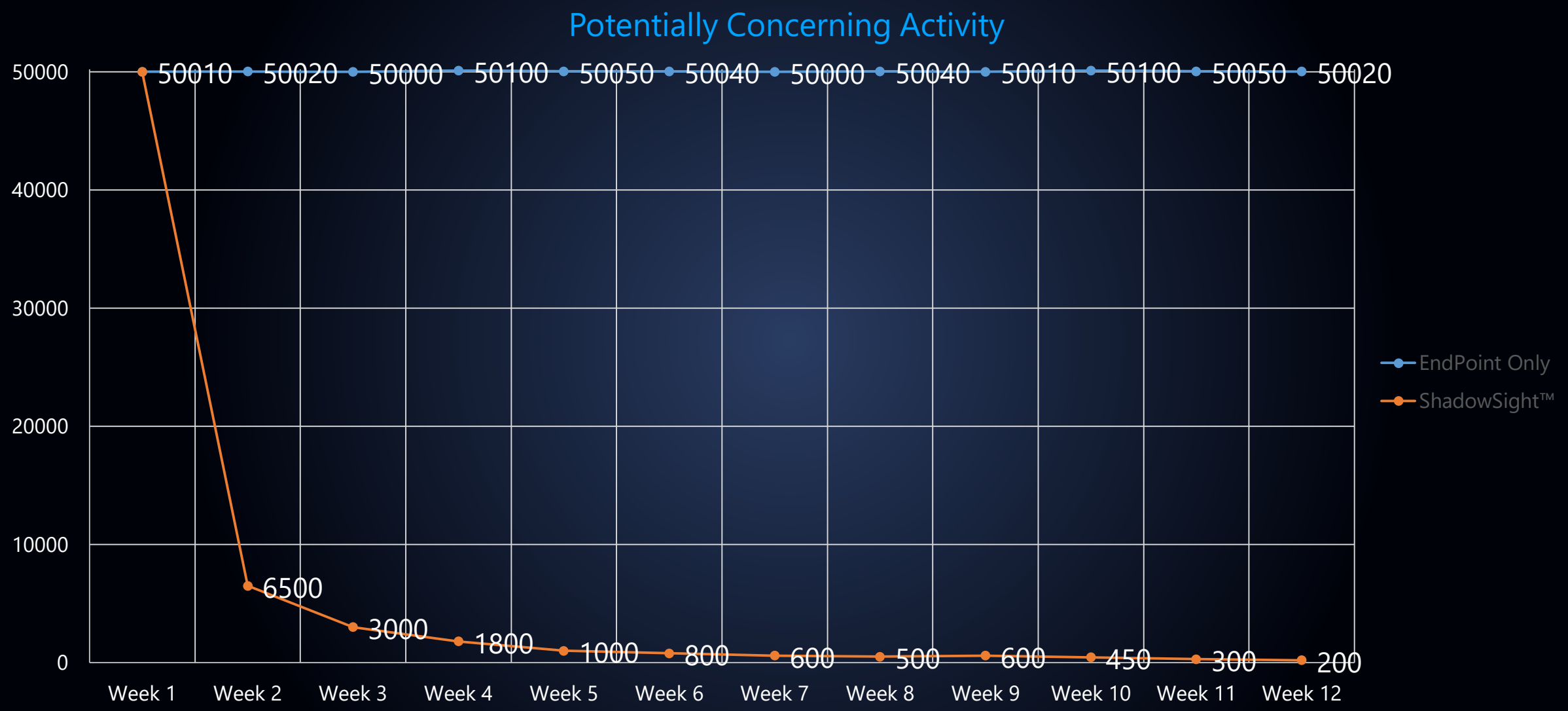
Policy Enhancement
As user activity trends change so do detection policies. This ensures ShadowSight™ further evolves with your business

How does ShadowSight work



SHADOWSIGHT

Insider Risk – Typical results



SHADOWSIGHT

Typical Results – Very few repeat occurrences

Existing client data

SHADOWSIGHT

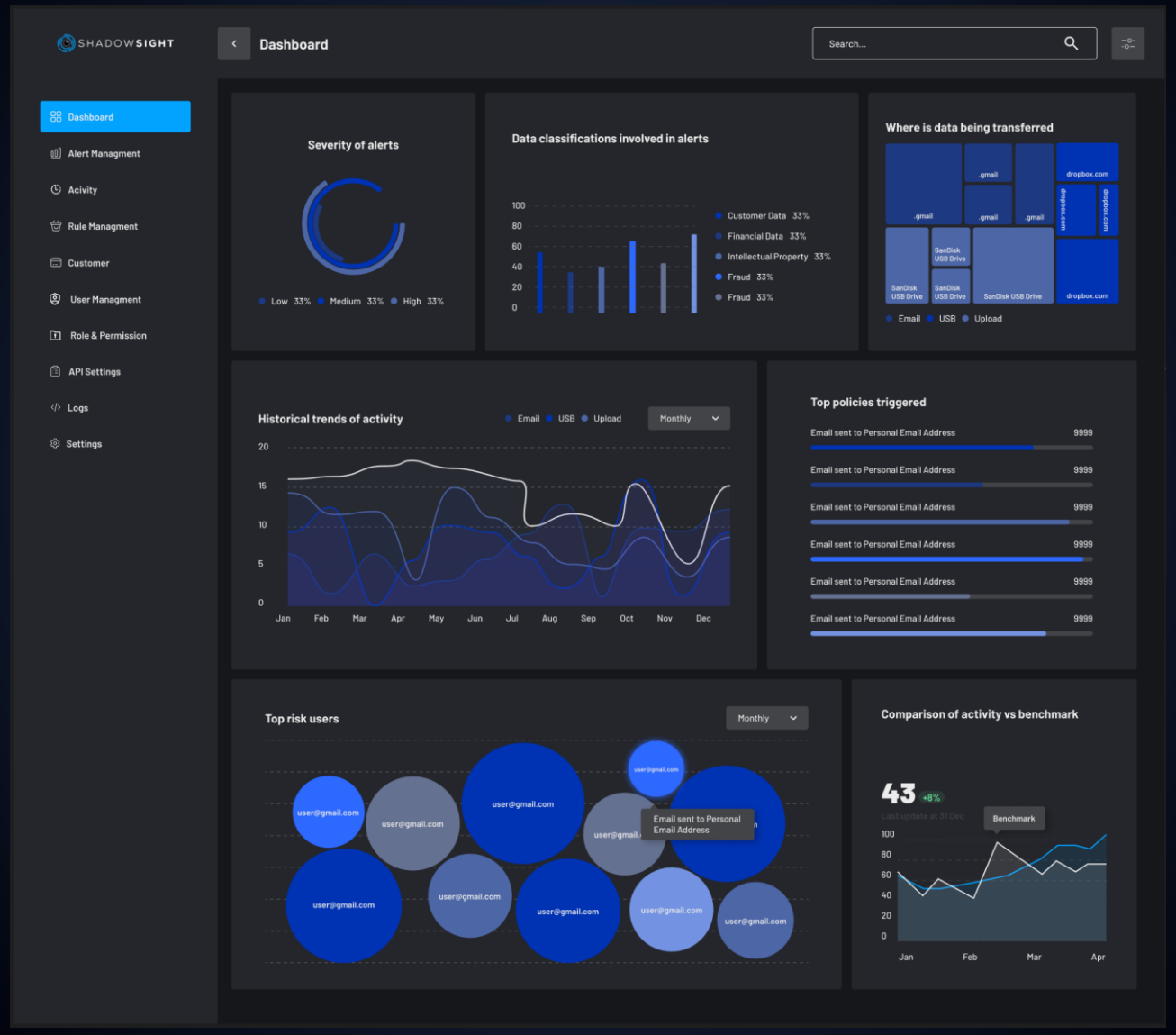
FOR FURTHER INFORMATION CONTACT US

Christopher McNaughton

- Email – cmcnaughton@secmon1.com
- Mobile – 0428183095
- Office – 1300410900

THE SHADOWSIGHT PORTAL

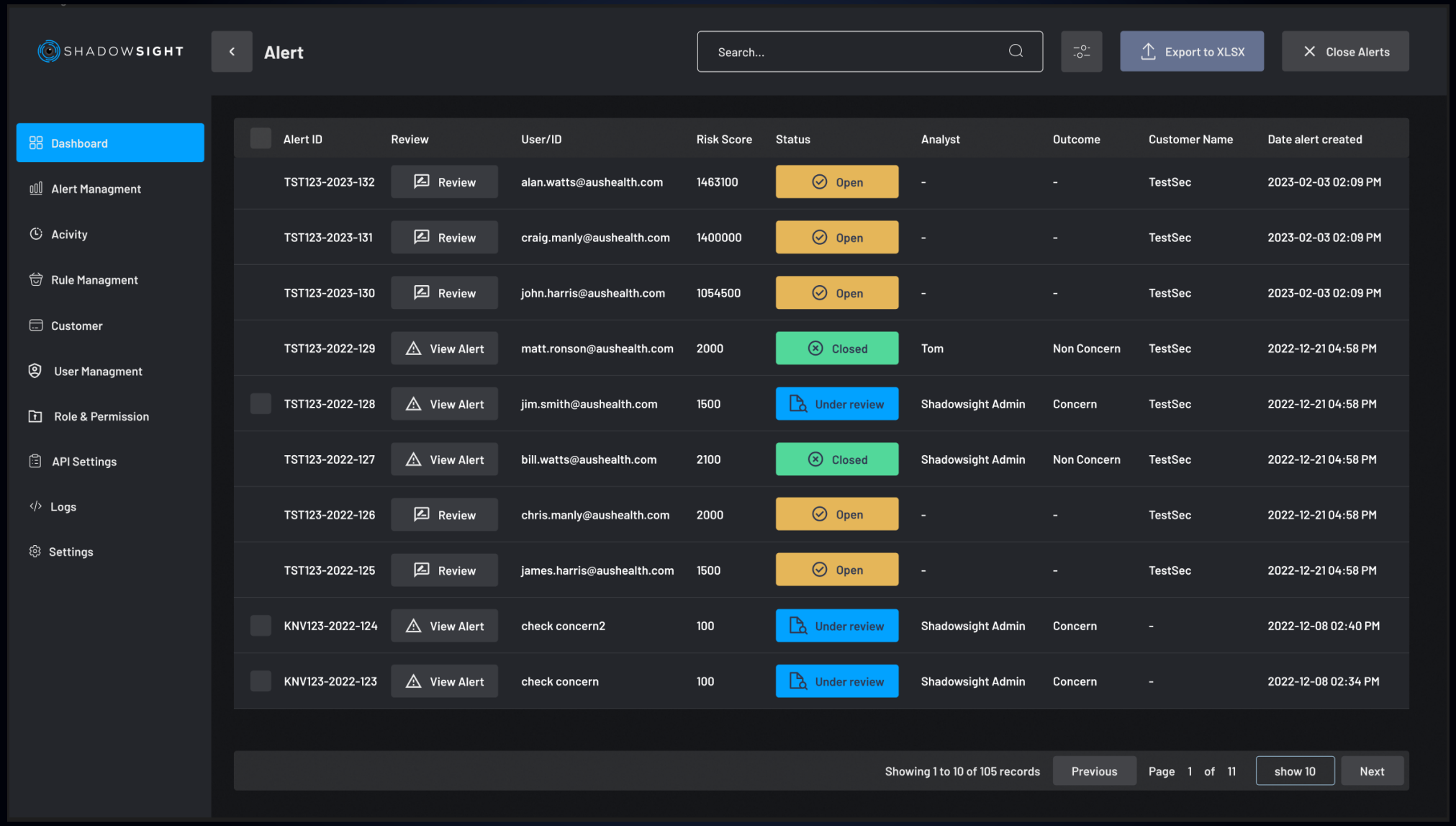
The ShadowSight portal - Dashboard



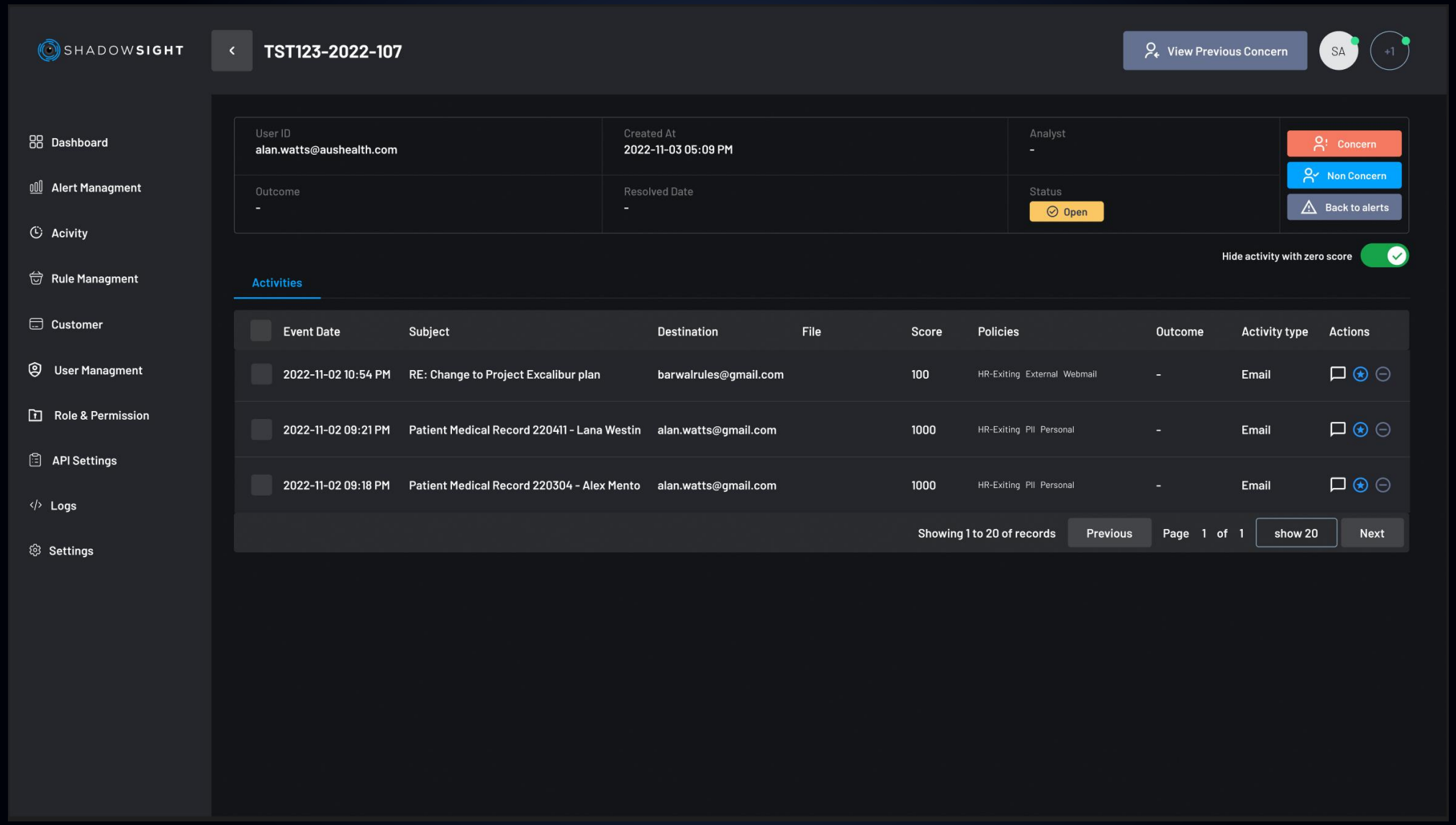
SHADOWSIGHT

Currently under development

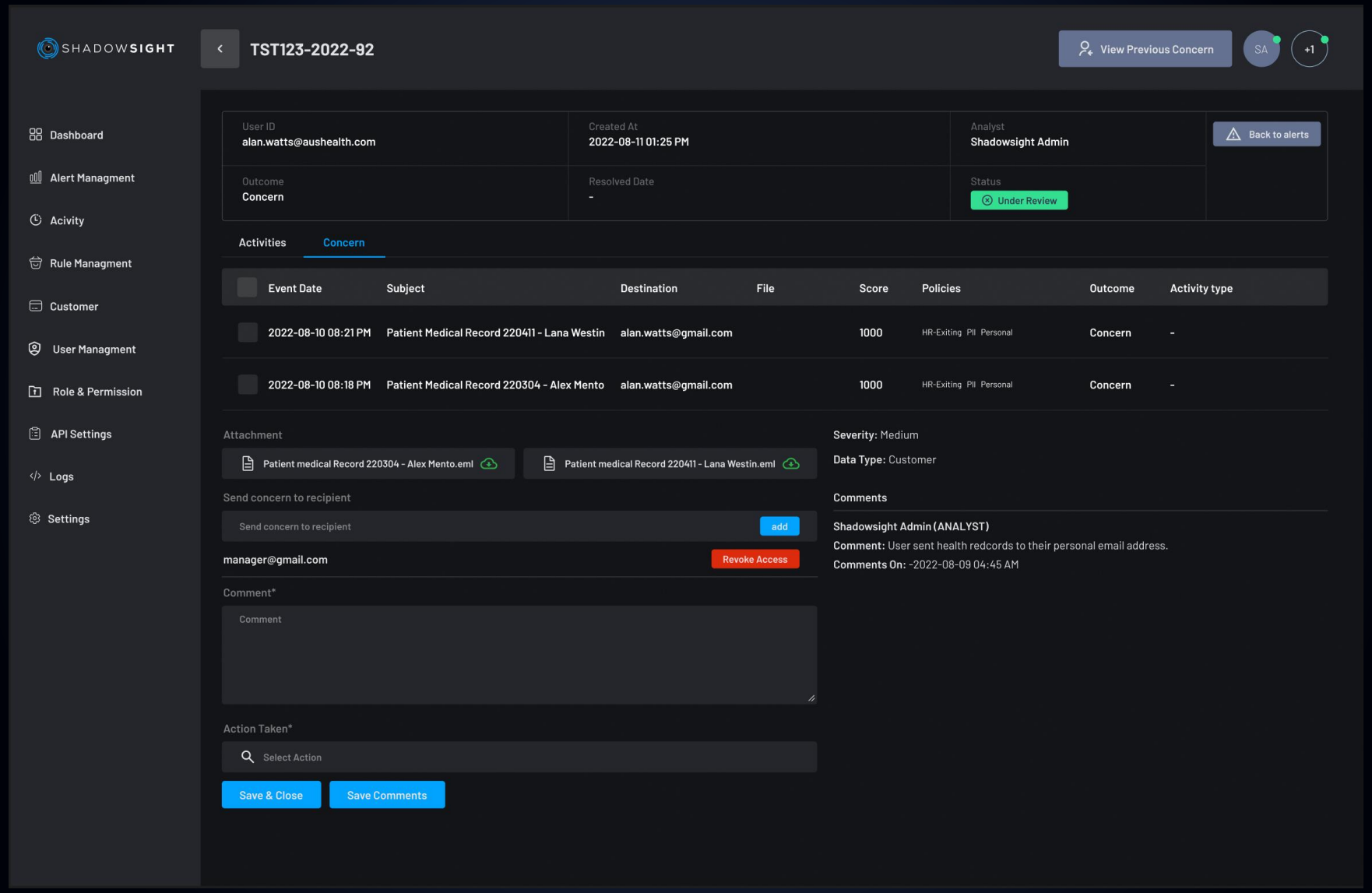
The ShadowSight portal – Alert Management



The ShadowSight portal – Activity Review



The ShadowSight portal – Manager Review



QUESTIONS?

APPENDICES

ShadowSight – Why it works so well

Week 1

- Implementation, business risk workshop, and staff communications
- Event & context analysis commences
- ShadowSight known risky behaviour rules utilised
- Business risk context rules applied
- Known good & enhanced monitoring rules applied
- Initial behaviour metrics available & analysed for trends
- Alerts generated for high risk events

Week 2 – Week 3

- Known good & enhanced monitoring rules continue to be refined
- Alerts generated for high to medium risk events
- Changes in staff behaviour seen with alerts reducing

Week 4

- Additional communications sent to staff based on activity seen
- Known good & enhanced monitoring rules continue to be refined
- Alerts generated for all risky events detected
- Clear changes in staff behaviour seen with alerts continuing to reduce

ShadowSight Features

- Evolution – Evolves dynamically with the business
- Very low false positives (Typically less than 1%)
- Rapidly improve the security culture of the organisation
- Rapidly identify high-risk behaviour by staff
- Historic, reactive and investigative reviews of employee activity
- Process large volumes of events with automated rules
- Reduce the intensive resource requirements on security teams
- Rapid notifications using the workflow feature

ShadowSight – How is it different?

- ShadowSight dramatically reduces alerts through a process which involves;
  - Correlation of contextual information and staff activity
  - Analysis of staff activity using the ShadowSight proprietary risk rules
  - Dynamic tuning of detection rules
- Changes the Insider Threat strategy from reactive to proactive
- No ongoing professional services – Rules are tuned dynamically
- Risk rated alerts based on actual business context and staff activity

- Maximises the benefits of your existing detection technologies implemented
- No endpoint agent required – API's utilised
- Rapid deployment – Hours and not weeks
- Augments resource poor Security Teams
- Integrates throughout the entire business
- Very low false positives (Less than 1%)
- Creates a rapid change to the organisational culture
- Results and ROI in days and not weeks or months
- Predictable reduction of alerts

ShadowSight – Value Proposition

- You need to implement an Insider Threat program but don't know where to start
- Your internal Security Team cannot manage the large volume of alerts being generated through your Insider Threat program
- Your Insider Threat program was set up with some professional services but three months along and the business how now changed
- Resourcing restraints mean your Security Team have had to detune your Insider Threat detections and you are concerned you have lost visibility of your risk
- You are not getting return on your investment from your Insider Threat program
- You have no visibility of staff activity and do not understand your Insider Threat risk
- Many of your security incidents have been as a result of inadvertent staff errors or simply lack of awareness. How do you help guide staff and improve the security culture?
- You want to ensure your sensitive customer and company information is protected. How do you gain an understanding of what staff are doing with this information?
- You want to make your security awareness campaigns more effective.