## securonix

#### DATASHEET

# securonixeon

A New Era of AI-Reinforced CyberOps

#### Introduction

The cybersecurity threat landscape is no longer simply evolving; it has been hit by the perfect storm.

Securonix EON is a groundbreaking suite of AI-Reinforced capabilities to transform CyberOps in the face of new AIpowered attacks.



### The Pillars of Securonix AI-Reinforced CyberOps

The cornerstone of Securonix's innovative approach rests on three core pillars:

#### **AI-Reinforced Platform**

The platform leverages AI at all layers to make precise security decisions at high speed, focusing human intervention where most valuable.

#### **Cybersecurity Mesh**

Seamlessly and agnostically integrates with existing tools and technologies to create a unified defense architecture, maximizing the value of your security investments.

#### **Frictionless Security Experience**

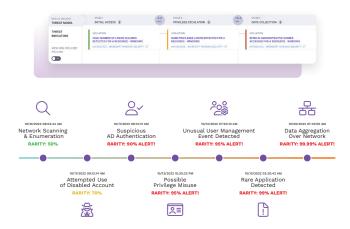
Delivers reduced noise, an intuitive user experience and targeted threat intelligence to empower teams to counter sophisticated threats. From these principles, Securonix EON extends the capabilities of the company's industry-leading Unified Defense SIEM.

EON is a groundbreaking suite of AI-Reinforced capabilities to transform CyberOps in the face of AIpowered threats.

#### **Insider Threat Psycholinguistics**

Our industry first Insider Threat Psycholinguistics feature employs AWS bedrock based, Large Language Models to accurately and efficiently discern the intent behind a user's language and behavior, identifying malicious activity and giving a TLDR summary of the user's actions.

Psy	cholin	guistics analy	ysis					
AI Fla	agged as	High Risk						
	accountrame	palicy	query		don don	nain	distance	LLMGrade
obfuscat violencel obfuscat								
legalAge	rements	6						
legalAgra	eementsWithInten							
flightRisk	k							
anxietyA	ndStress							
obfuscati	universite and							
	accountriame Silvia Holt	policy	query		doy 300	domain		+ distance
		compression or encryption of da		crypt and send business plans.		www.googi		
	Mark Plummer	compression or encryption of da	ata data encrys	t	300	www.bing.c	iom .	0.1

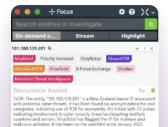


#### **Adaptive Threat Modeling**

Leveraging machine learning to develop dynamic adaptive threat models and automatic threat chaining of violations with anomaly detection, Securonix enhances investigations by enabling analysts and CyberOps teams to identify never before seen attack chains in near real-time.

#### InvestigateRX

Securonix Investigate automatically extracts context from internal and external data sources for investigations in flight. Security teams can share knowledge and collaborate within the investigation without pivoting to external tools like ticketing, email or messaging. InvestigateRX builds on this by converting retrieved personalized and objective content into a coherent and context-aware summary, analysts are empowered to make swift decisions and save approximately 15 minutes per incident.



The entity "101.100.139.201" is a New Zealand-based IP registered under MyRepublic Limited, specifically located in Auckland. The IP has been associated with sup such as "sideogene", "side'signed", and "isantis", and is hasted on several mereved parts including 21.25.33, 81.110.143 Mit.445, and 53 Truthermore, It has been found on anonymization/for exit categories, indicating attempts at maintaining anonymity.

This IP has been associated with 31 pulses, which are reports of threat intelligence, indicating its potential involvement in cyber security breaches. These breaches have targeted multiple countries, including the brief of the target of the security of the security breaches.



## Securoni× Your Partner in the CyberOps Era

Securonix, a 4x leader in Gartner's Magic Quadrant for SIEM, offers the experience and tools to enable CyberOps teams.

#### **(**P)

#### **Deep AI Expertise**

Over a decade of experience in AI-driven security underpins our solutions (UEBA, SOAR, etc.)

#### T

#### Future-Proof SIEM

The Securonix Unified Defense SIEM platform provides ultra fast 365 days of hot single-tiered search, BYO cloud, on-demand scalability and data enrichment.

#### Q

#### **Proven Accuracy & Detection**

Our solutions empower analysts with high-fidelity and targeted threat intelligence for confident decision-making.

#### 22

#### **Continuous Innovation**

We invest in threat research, advanced data science, AI capabilities, content as a service and seamless user experiences to stay ahead of threats.

