BLOCK SECURITY

BLOCK SECURITY ANNOUNCES THE WORLD'S FIRST HOLISTIC CYBERSECURITY BLOCKCHAIN-BASED ECOSYSTEM

THE INDUSTY AVERAGE of 240 DAYS to detect a cyber security breach is NOW down to SECONDS...!

BLOCK SECURITY

www.TheCurrency.Store

OFFICE LOCATIONS

The Shard,
Level 24,
32 London Bridge St,
London, SE1 9SG,
UNITED KINGDOM

Al Maqam Tower,
35th Floor, PO. Box 35665,
ADGM Square, Maryah Island,
Abu Dhabi,
United Arab Emirates

CONTACTS

Office number: +44 (0) 207 205 4848
24 hour Call Center: +44 (0) 845 366 9742
Email: info@theglobalcc.com
Web: www.BlockSecurityServices.com

BLOCK SECURITY SERVICES

Block Security is excited to announce that it is offering a new patented disruptive cyber security system developed by Naoris Limited. Block Security is powered by GCC Global Consortium Corporation – an international resource bank and investment platform that provides services to entrepreneurs and investors.

WHAT IS BLOCK SECURITY?

1. FROM START UPS TO HIGHLY REGULATED INDUSTRY

In many organisations, their approach to cybersecurity has barely changed in the last 35 years. However, the hackers, fraudsters and other criminals with the capability to deliver a cyberattack are becoming ever more sophisticated. Organisations now need to respond by overhauling their approach to cybersecurity. Naoris is the world's first holistic blockchain-based cybersecurity ecosystem. Organisations ranging from start-up companies to highly regulated industries, governments, the military and public bodies could all benefit hugely from embracing the radical new solutions offered by Naoris.

2. A REVOLUTION IN THE WAY IN WHICH CYBERSECURITY IS THOUGHT ABOUT AND DELIVERED

The Naoris SE (Security Ecosystem) leverages blockchain in a sustainable way to secure cyberspace. We are now experiencing the fourth industrial revolution - where disruptive technologies such as the Internet and artificial intelligence are changing everyday life and the way we work. Naoris recognises the need to future proof their technology. Public institutions, small and large companies across all business sectors, the military and national governments must all adapt to the rapidly changing world. In particular, a new radical approach to cybersecurity, which embraces new techniques and technologies, is required. In summary, Naoris SE aims to instigate innovation through disruption in the cybersecurity field.

WHY BLOCK SECURITY?

WHAT ARE THE CHALLENGES FOR CYBERSECURITY?

In spite of all the benefits provided by 21st century technological innovations, recent years have also produced an increase in cyber risks. The malware problem has reached epidemic levels, while cases of hacking and fraud have also risen dramatically.

SINGLE POINT OF FAILURE

For some time, a silo mind-set has been the standard approach in the field of device and network security, involving centralisation of data and processing. However, this is an extremely risky strategy, as it effectively means that every individual device is a potential entry point for a hacker, and a breach could potentially compromise the entire network.

STATIC INDUSTRY APPROACH FOR 35 YEARS

The value of the cybersecurity market will soon pass the $1 trillion mark, and with annual growth of 18% things won't stop there. If organisations continue to use a model that has remained largely unchanged for 35 years, while hackers and other criminals continue to innovate and develop new tactics, cyberattacks are projected to cause up to $6 trillion in annual damage by 2021 – the figure for 2015 was $3 trillion.

RAPID SPREAD OF THREATS AND SLOW DETECTION

Hacking is a virtually risk-free activity – if they are successful, they can cause considerable damage, but if they are unsuccessful, they simply move on to their next target. In contrast, businesses and other organisations operate in an environment of absolute liability, where any successful cyberattack can cause untold financial problems and other damage. The impact of a cyber incident can be magnified if the organisation fails to realise that they have been targeted. At present, the median average is 101 days – this covers the period from the initial breach to the time the organisation realises anything is amiss. Attacks can also spread throughout the organisation, just as any virus might be transmitted between humans - 32% of cyber breaches affect more than half of the targeted system. Organisations also need to be wary of the people they do business with, as 56% of organisations say they have experienced one or more breaches that were caused by one of their vendors.

WEAK AND COSTLY CYBERSECURITY COMPLIANCE AUDITS

Service level agreement (SLA), cybersecurity, and compliance standard audits are inefficient and opaque, checking only a small fraction of devices. Enterprise cybersecurity certifications offer a beacon of false hope that enables further breaches.

HOW DOES BLOCK SECURITY WORK ?

DISRUPTING THE STATUS QUO

1

DEVICE & O.S. AGNOSTIC SECURITY

As a DApp, Naoris SE can be used with most networked devices and their operating systems.

2

RE-BALANCING THE WORLD OF CYBER

Naoris SE allows organisations to catch up with the threats posed by hackers, fraudsters and other criminals, who have been honing their technique for the last 35 years while many companies and other organisations have stood still. Devices should now be seen as resilient consensus-based defenders instead of points of weakness which could allow unauthorised entry to an organisation's systems.

3

CYBERSECURITY EVOLVES INTO AN ECOSYSTEM

Naoris SE heralds a new era in cybersecurity, using Blockchain consensus technology as the focal point of its ecosystem. With Naoris SE , no single end-point, mobile device or terminal is independent of one another.

4

PREVENTATIVE SELF HEALING

Naoris SE provides valuable peace of mind to companies and organisations, and their directors and senior management. Instead of having to trust centralised tools and decision makers, Naoris SE allows them to rely on a decentralised consensus mechanism. This mechanism registers and responds to information in real time, reacting to threats and unexpected changes.

TECHNOLOGY

REAL-TI D.I.V.A & S.P.O.E

Together, the Decentralized Identity Validation Authority (DIVA) and Smart Proof of Existence (SPOE) provide blockchain technology that can leverage techniques in both cryptography and cybersecurity to tackle real world information. Their origin systems through uniquely traceable artifacts and the capacity to detect, react and recover from breaches of truth or trust with direct application today within a rule-based ecosystem.

N.H.C

Naoris Hybrid Chain (NHC) has been designed with both future proofing and resilience in mind. Concurrent snapshots of the Naoris chain will be 'backed up' on other blockchains for resilience, which will allow for extra resilience of nodes and services across the environment.

AN INNOVATIVE DISTRIBUTED CYBER-ECOSYSTEM FOR YOUR BUSINESS

Naoris DSE

Naoris Distributed Security Ecosystem (NaorisDSE) is a world-class technology information in all types of businesses and environments, like intellectual property, sensitive files, core databases, critical processes and applications.

Naoris DC

Naoris Distributed Core or Naoris DC for short is a dynamic application security and cloud security technology. The Naoris DC command and control systems allow the user to set permissions, manage governance and monitor access and use of critical business applications on servers or in cloud environments.
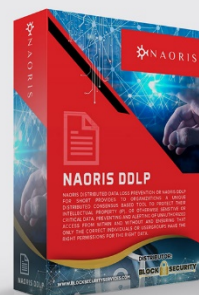
Naoris Legion

Naoris Legion is Naoris`s revolutionary distributed approach to next-gen end point security. Naoris Legion can stop millions of traditionally undetectable attacks before they result in a costly breach, including zero day attacks and fully undetectable malware.

Naoris DOT

Naoris DOT is a specialized version of Naoris protecting SCADA Systems, Industrial Control Systems (ICS), Industrial Internet of Things (IIOT) and smart sensors commonly found in Smart Cities or large IOT infrastructures.

Naoris DDLP

Naoris Distributed Data Loss Prevention or Naoris DDLP for short provides to organisations a unique distributed consensus based tool to protect their intellectual property (IP), or otherwise sensitive or critical data, preventing and alerting of unauthorized access from within and without and ensuring that only the correct individuals or user-groups have the right permissions for the right data.

Managed Solution

For clients wanting to outsource their Cyber Security monitoring contact us about our BLOCK SECURITY MANAGED SOLUTION.

REDUCE COST, RISKS AND POTENTIAL DATA BREACH FINES...

The previous industry average of **240 days** to detect a breach has now been reduced to a matter of seconds

OFFICE LOCATIONS

The Shard,
Level 24,
32 London Bridge St,
London, SE1 9SG,
UNITED KINGDOM

Al Maqam Tower,
35th Floor, PO. Box 35665,
ADGM Square, Maryah Island,
Abu Dhabi,
UNITED ARAB EMIRATES

CONTACTS

Office number: +44 (0) 207 205 4848
24 hour Call Center: +44 (0) 845 366 9742
Email: info@theglobalcc.com
Web: www.BlockSecurityServices.com

THANK YOU