FOREGENIX

Making Cyberspace Safe for Everyone

From first contact to final delivery, we commit to providing a strong cybersecurity posture well beyond compliance

WHY FOREGENIX

Experience

Cybersecurity experts with extensive hands-on experience and no less than 15 years operating in the field. Qualified, recognised and certified professionals.

Sense of Duty

Real commitment to help simplify complex topics and protect business continuity.

Research and Development

Passionate about Cybersecurity and its continual challenges. Consistently learning and researching to stay ahead of the curve by developing skills, tools and methodologies.

Global, but Local

We have active analysts, consultants and investigators in every continent. We source and nurture talent where our customers are.

WHAT WE DO

COMPLIANCE & CONSULTING

- Effective methodology for cyber risk management, improve clients security stance and achieve compliance with several cybersecurity programs.
- Security programs such as PCI, CMMC, DFARS, HIPAA, SWIFT, ISO 27001, and more.
- Cybersecurity Consulting, Due Diligence, Risk Assessments, Virtual CISO and Training.

OFFENSIVE OPERATIONS

- Services tailored to test your defences and detect weaknesses before attackers do, delivering effective security bleeding-edge techniques, methodologies & effective development and implementation of a range of Adversarial and Assurance services.
- Penetration Testing, Attack Simulation, Red & Purple teaming, social engineering, Hardware OT/ IoT Testing.

DIGITAL FORENSICS & INCIDENT RESPONSE

- Top 4 leading PCI forensic team globally.
- PCI PFI Forensic Investigations, PFI Lite, DFIR, Proactive IR, Blue team Extension and Training.

CYBERSECURITY SOLUTIONS

- Managed Website Security Monitoring and e-commerce Portfolio Scanning.
- Managed Threat Detection and Response (MDR)
- End-Point Protection and Threat Intel Group (TIG), 24x7 Operation.

COMPLIANCE & CONSULTING

As a global security leader within the PAYMENT CARD INDUSTRY, Foregenix works with some of the largest and most complex payment environments globally providing information security advisory, strategy development and compliance support.

We offer a complete portfolio of services for the **payment industry**:

PCI DSS | SSF | P2PE | PIN | 3DS | CPSA

Foregenix offers a focused and well-supported methodology to achieving compliance, specifically customised around each of our clients' individual requirements. With years of experience, we offer our clients design, assessment and compliance services, and a well-supported path towards acquiring a strong security posture and staying compliant.
Our standard methodology includes:

- Programs Transitioning Workshops
- Pre-Compliance/Gap Analysis Service
- Penetration Testing
- Compliance Assessment Service (CAS)
- Delta Assessment
- General Consultancy

PAYMENT APPLICATION QUALIFIED SECURITY ASSESSOR

QUALIFIED PIN ASSESSOR (QPA) PROGRAM

QUALIFIED SECURITY ASSESSOR

POINT-TO-POINT ENCRYPTION

SECURE SOFTWARE ASSESSOR

3DS ASSESSOR

SECURE SLC ASSESSOR

PCI FORENSIC INVESTIGATOR

COMPLIANCE & CONSULTING

PCI P2PE - Point-To-Point Encryption

Our consultants help customers in the goal of reducing the risk of Cardholder Data compromise within different environments (solution/application/component) by setting security controls based on security best practices, defining the requirements for Point-to-Point Encryption (P2PE) solutions assessments for merchants.

PCI PIN Security

We provide design, assessment, and remediation services from our world-recognised experts in PCI PIN and general crypto key management challenges.

PCI 3DS Core Security Assessment

Foregenix offers a structured methodology, customised to assist the client to achieve and maintain the approval and activation process for 3-D Secure Enrolment Server/Access Control Server Service Provider and to present the security requirements for 3-D Secure ES/ACS hosting.

PCI Card Production (CPSA)

We assist business covering the following card production activities:
Card Manufacturing, Data Preparation, Pre-Personalisation, Fulfilment, Packaging, Storage, Chip Embedding, Card Personalisation, Chip Personalisation, Mailing, Shipping, PIN Printing and Mail (personalized, credit or debit), PIN Printing (non-personalised pre-paid cards) and Electronic PIN Distribution.

VISA Ready Site Security

We help high-growth businesses to manage risk and compliance at scale, with minimal friction.

COMPLIANCE & CONSULTING

CYBERSECURITY COMPLIANCE

Foregenix is leveraging decades of experience in NIST, FIPS and ISO to bring to market expertise in supporting clients with securing Controlled Unclassified Information (CUI).

More than just security and compliance, Foregenix leads the industry in designing robust security solutions to support a multi-disciplined environment with our Shared Services Architecture (SSA).

Our SSA consulting practice works with clients to implement a unified security platform, supporting many compliance disciplines simultaneously, including:

- PCI DSS
- CMMC/DFARS
- ISO 27001
- HIPAA
- SWIFT and more

As organizations wrestle with the adoption of the new CMMC standard for CUI, Foregenix stands ready to help integrate new regulations into brand new or existing environments while leveraging concepts of the SSA to minimize overall cost and administration.

COMPLIANCE & CONSULTING

CONSULTING & TRAINING

Cybersecurity Due Diligence
Cybersecurity Risk Assessments
PCI DSS Technical Training Course

Virtual CISO

By selecting a Virtual CISO from Foregenix to help mitigate your organisation's cyber security risk, your team and organization will benefit from an independent expert familiar with the challenges of managing information security across industries.

Foregenix VCISO service is designed to assist with:

- Review of Information Security strategy including 3rd party services
- Review and development of Security Policies and Procedures with relevant business owners.
- Achieving compliance with industry standards such as the ISO27000 and PCI DSS.
- Planning security testing, assessments and reviews through Compliance function/internal audit and as part of the vCISO service.
- Developing and implementing threat management strategy.
- Procuring security products and services.
- Recruiting and training IT engineers and security personnel.

OFFENSIVE OPERATIONS

TEAM OrionX

Introducing Foregenix's Elite Offensive Operations arm, OrionX. A highly skilled and diverse team of carefully selected and passionate cybersecurity experts solely focused on offensive operations. OrionX members have been with Foregenix for many years performing offensive operations, delivering excellence with speed to outrun threat actors in the race to find security weaknesses.

PENETRATION TESTING

Source Code Review | Static Application Testing

Static Application Security Testing (SAST) is a service that is applied in the source code of an application. Your application is analysed, all possible input and output points are identified along with the code paths that connect them. The resulting model is scrutinised against our comprehensive library of defect patterns, resulting in identifying the application's vulnerabilities.

Web Application Penetration Testing

OrionX assumes the role of an organised force targeting your web applications and APIs. The service not only identifies basic vulnerabilities such as SQL injection and cross site scripting, but also performs manual checks to business logic and rules, running authenticated and unauthenticated tests, application crawling, identifying application components and technologies across the application code as well as 3rd-party frameworks, libraries and other components.

OFFENSIVE OPERATIONS

External | Internal Network Penetration Testing

In this service offering, OrionX attacks the targets from a vantage point emulating either an external or internal attacker, depending on the assessment requirements. Our team follows a largely similar methodology when performing this type of penetration testing including reconnaissance, target identification, vulnerability assessment and exploitation but customises each step depending on the overall context, the placement of the attacker and the nature of the target.

Mobile Application Penetration Testing

Engineered towards identifying vulnerabilities in Mobile Applications (native, cross-platforms, WebView oriented, etc.). This service is customised specifically for your application and can include the server-side components as well (APIs) the mobile application communicates with in order to provide a holistic view as the application is looked at as a complete entity rather than a compartmentalised perspective.

Wireless Network Penetration Testing

Wireless penetration testing is a service designed to identify weaknesses in a client's wireless deployment. It is designed from the ground up to provide an overall view of your company's wireless deployment starting with site survey and coverage analysis and moving on to attacking the implementation parameters (keys, algorithms, etc.). In its full capacity it is a service designed to be performed on-site, however OrionX offers alternatives that can be run remotely and is solely focused on attacking the implementation.

OFFENSIVE OPERATIONS

ATTACK SIMULATION

Red Teaming

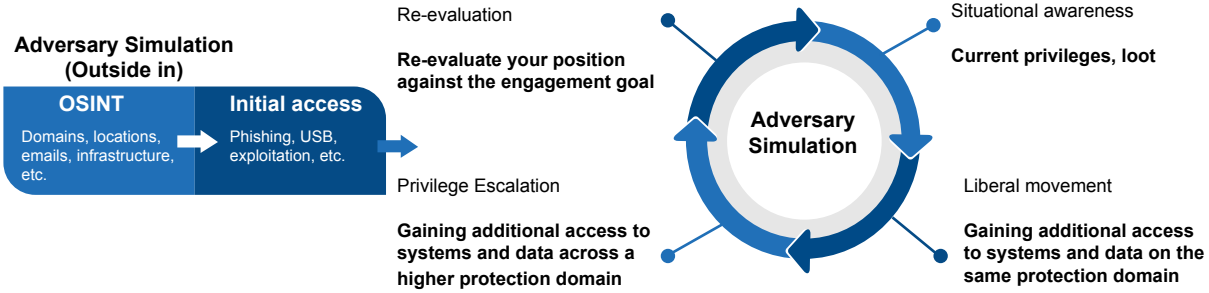
Adversarial simulation is a goal-oriented test designed to target your organisation's people, processes and technology. OrionX's most senior consultants target mature environments using advanced tactics, techniques and procedures used by real life threat actors. It is a covert exercise with a very specific objective without being caught; so all actions are evaluated against a Risk vs Reward formula.

Purple Teaming

Using real-world cases and threat intelligence data, OrionX simulates the actions of a threat actor/hacking group inside your organization's network with your blue team members (defensive) monitoring and logging our activities in a collaborative manner. It is a team working to address these shortcomings in the most effective manner to adopt defensive practices and improve their capabilities.

Social Engineering

It is the psychological manipulation of people into performing actions or divulging confidential information. OrionX offers a specialist service to test the People aspect of Cybersecurity using a selection of techniques such as Phishing, USB drops and Vishing to cater for specific use cases.



OFFENSIVE OPERATIONS

IoT / OT / ATMs / CUSTOM HARDWARE

Embedded Application | IoT Penetration Testing

Embedded systems exist in many shapes and forms and influence our lives in a variety of ways. In the vast majority of cases the closed nature and embedded nature of these systems is relied upon in a security through obscurity manner. Foregenix has developed a methodology that analyses these types of systems at the hardware and software level, learns about its input and output mechanisms and probes them for vulnerabilities.

ATMs | Unattended Kiosks | Payment Terminals

ATM's implementations are heavily customized depending on the brand, hardware, software, management configurations and security controls. However, there are common risks that these devices should face since devices are exposed to attacks from a logical and a physical point of view. OrionX has developed a methodology that allows for a holistic assessment of an ATM implementation that includes testing of architectural, physical, network and application security controls in order to identify potential vulnerabilities. OrionX can perform its assessments either in a test or pre-production environment or in a live production environment, in coordination of the systems custodians.

Operational Technology (OT)

As one would expect, the process of conducting a security assessment or penetration test on Industrial Control Systems (ICS) is a tedious operation that should not be taken lightly. OrionX's unique methodology allows for a structured and safe assessment of the overall architecture of Industrial Control Systems (ICS) while taking under consideration the sensitive nature and operational constraints of the components under scrutiny.

CYBERSECURITY SOLUTIONS

ONLINE

Managed Website Security Monitoring

Monitoring, protection and rapid incident reaction to security situations (depending on when Foregenix is introduced) is provided to thousands of e-commerce websites around the world.

Leveraging bespoke technologies and supported 24/7 by security professionals, our solution is continually fed threat intelligence from the team's own efforts, online research and substantially from our global Digital Forensic investigations.

e-commerce Portfolio Scanning

Foregenix constantly monitors in excess of 11 million websites and has been collecting security statistics and insights on these entities for several years. The intelligence provides acquiring partners valuable insight into the security stance and associated risk posture of their merchant portfolio.

CYBERSECURITY SOLUTIONS

BRICK & MORTAR

Managed Threat Detection & Response

Our team of Threat Intelligence Analysts monitor our client base around the clock, with the platform continuously monitoring for behavioural and system interaction indicators, memory only attacks and suspicious system activity.

Dealing with threats and incidents as they arise, our analysts can swiftly react from response through containment to resolution.

Managed Proactive Security

Foregenix Proactive Security pivots around our proprietary technology platform, to combine robust modern threat detection capabilities with remote enterprise-scale incident response, incident management and deep investigative abilities - all bundled into a rapid forensic process.

Depending on the timing of our engagement (before, during or after an incident) the platform and analysts, backed by our exceptionally experienced forensic investigators can operate rapidly to identify, understand and contain the incident.

DIGITAL FORENSICS & INCIDENT RESPONSE

PAYMENT INDUSTRY

PCI Forensic Investigations & PFI Lite

If an organisation is suspected to have suffered a data breach and had customer payment card data stolen, the business may be instructed by their acquiring bank to undertake a PCI Forensic investigation (PFI).

The goal of the investigation is to reach containment as soon as possible (stop the attackers), to attempt to determine the source of a breach and to find out when and how it was caused, and how much data was stolen. Through a combination of experience and skills, and in-house developed technology, Foregenix can offer unparalleled detection and containment speed.

Our team of expert Forensic Analysts will provide:

- Frequent updates and coordination support
- Critical guidance and technical details about the compromise
- A quick, discreet and minimally-intrusive investigation
- Rapid analysis and on-going monitoring to ensure that all regulatory requirements are met

If you operate a small e-commerce business based in Europe, you may be eligible for a **PFI Lite** investigations: PFI Lites are a Visa Europe initiative designed for small businesses with online presence who may have been hacked and lost cardholder data. This is a scaled-down PFI Investigation designed to provide a remediation service specifically for smaller e-commerce merchants.

DIGITAL FORENSICS & INCIDENT RESPONSE

NON-PAYMENT DFIR

Digital Forensics & Incident Response

When your business is compromised, time is of the essence. Foregenix Incident Response Service makes us an extension of your security team – we help you prepare for and enable rapid response and incident containment.
Our incident response service is quick and discreet, and we can get into action with minimal disruption to your business.

Proactive Incident Response

We provide guidance to organisations on how to structure and test their incident response plans. We help to write the plans, test them and ensure that the client has the best possible plan ready for action, if the need arises.

We develop in-house solutions to detect and mitigate active, advanced and previously unknown threats. Our technology and our team work in tandem to provide you with rapid threat hunting, instant analysis and ongoing protection of your systems: Foregenix Threat Intelligence, 24/7.

Blue Team Extension Services

Our Threat Intel team becomes your Blue Team to monitor and hunt threats inside your corporate infrastructure. The team analyses events as they are collected from different endpoints and network devices. They then correlate them and try to piece together the red teams – or actual attackers' actions, with the ultimate goal to clean up, reclaim and harden client assets.

SOME CLIENTS WE PROUDLY SERVE

Get In Touch With Us

Email Address

sales@foregenix.com

United Kingdom (HQ)

Foregenix Ltd.
8 9 High Street,
Marlborough
SN8 1AA

+44 845 309 6232

North America

Foregenix Inc
75 State Street, 1st Floor
Boston, MA, 02109
USA

+1 877 418 4774

Europe

Foregenix Germany GMbH.
Betzelsstrabe 27, 55116
Mainz, Germany

+49 6131 2188747

MEA

Foregenix (Pty) Ltd.
Sec H, Blg E, Coachman's Crossing Office Park 4
Brian Street, Lyme Park,
Sandton, South Africa

+27 860 44 4461

APAC

Foregenix (Pty) Ltd.
1 Market Street, Sydney
NSW 2000
Australia

+61 420 904 914

LATAM

Foregenix do Brasil
São Paulo
Brazil

+55 (11) 98781-4241

FOREGENIX