SHELT

YOUR CYBERSECURITY
AS-A-SERVICE PARTNER

Who

Are we?

SHELT is a European Cybersecurity enterprise for the new digital world, with presence in Europe, Middle East and on the African Continent.

A culmination of years of experience from several partners that are all leaders in their respective fields; ranging from Telecommunication Network providers, Managed Services to Cyber Security service providers.

Information Security Management
ISO
27001
Certified

GDPR
Certified

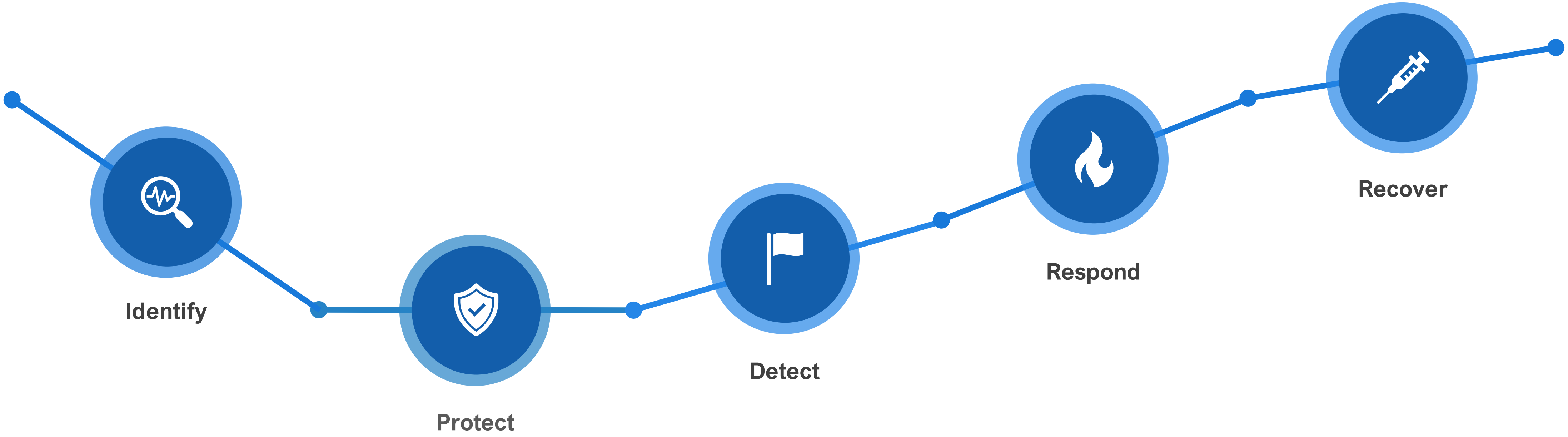
SHELT

Secure

Services

SHELT protects your business by providing a 24/7 Managed Security Services with centralized dedicated security consultants .

By observing data feeds across your enterprise, we will



from any potential security breach in your organization.

Cybersecurity

Maturity

Increase in cybersecurity maturity

From Reactive to Proactive

Level 0 - Unprepared

- Lack of people, processes and technologies to deal with cybersecurity threats
- No dedicated Cybersecurity personel

Level 1 – Reactive

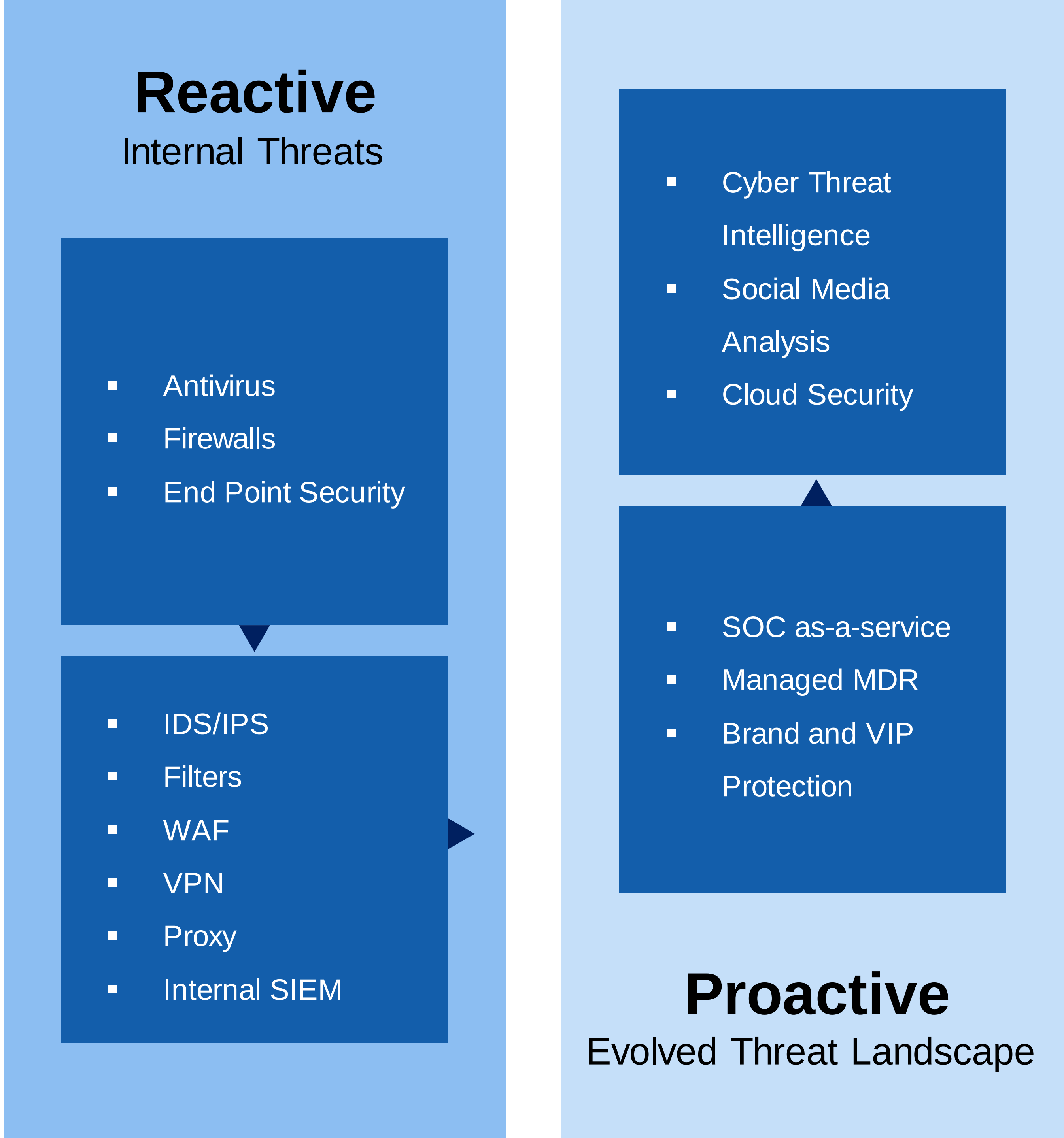
- People and some processes and technologies are in place to manage attacks when they occur
- No visibility against latest threats.
- Unmanaged & Siloed Security tools.
- No incident response plans

Level 2 – Proactive

- People, processes and technologies are orchestrated to protect against foreseeable threats from known and unknown sources.
- Security is aligned with the needs of the Enterprise
- Risk-based, defence in-depth approach
- Proactivity in threat hunting
- Cybersecurity Mesh Architecture
- Automation

Cybersecurity

Evolution



Reactive

Internal Threats

- Antivirus
- Firewalls
- End Point Security

- IDS/IPS
- Filters
- WAF
- VPN
- Proxy
- Internal SIEM

- SOC as-a-service
- Managed MDR
- Brand and VIP Protection

- Cyber Threat Intelligence
- Social Media Analysis
- Cloud Security

Proactive

Evolved Threat Landscape

Defense-in-Action Program

Proven program and methodology trusted by all our customers with 100% satisfied clients

24x7x365
SECURITY OPERATION CENTER

reva

24x7x365
BRAND & VIP
PROTECTION

GENECYS
POWERED BY SHELT

EXTENDED
DETECTION & RESPONSE

FORTINET
securonix
Gartner
Magic Quadrant

SIEM
AS A SERVICE

CEQUENCE
SECURITY

24x7x365
API SECURITY MONITORING

BLACK KITE

Digital RISK MAPPING
(Technical, Financial, Compliance)

MATRIX42

IT ASSET MANAGEMENT
(ITSM, ITAM, EDP, …)

SOTI

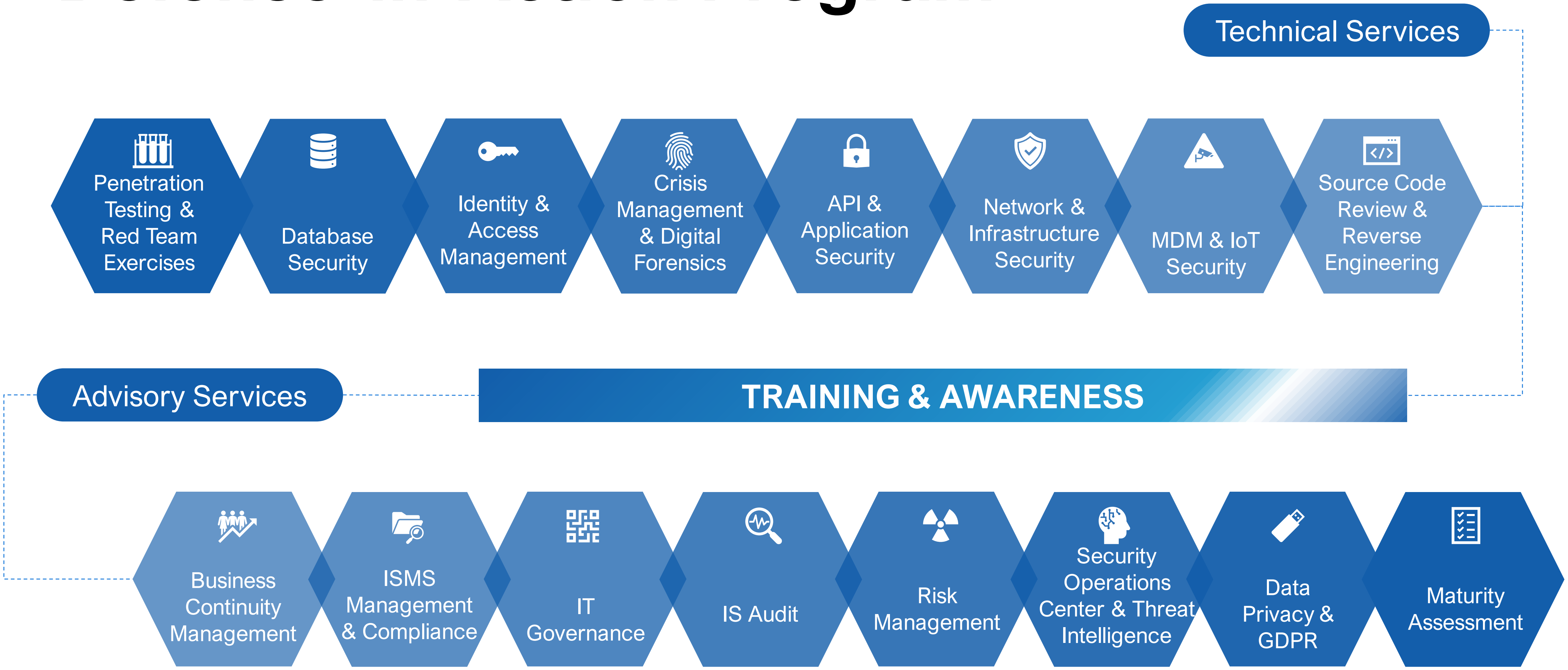
MOBILE DEVICE
MANAGEMENT

WIZ

CLOUD SECURITY

Our Cybersecurity Services

Defense-in-Action Program



Technical Services

- Penetration Testing & Red Team Exercises
- Database Security
- Identity & Access Management
- Crisis Management & Digital Forensics
- API & Application Security
- Network & Infrastructure Security
- MDM & IoT Security
- Source Code Review & Reverse Engineering

TRAINING & AWARENESS

Advisory Services

- Business Continuity Management
- ISMS Management & Compliance
- IT Governance
- IS Audit
- Risk Management
- Security Operations Center & Threat Intelligence
- Data Privacy & GDPR
- Maturity Assessment

SHELT

Next Generation

Adaptive Cyber Security Architecture

PREDICT

Risk exposure assessment

Anticipate threats

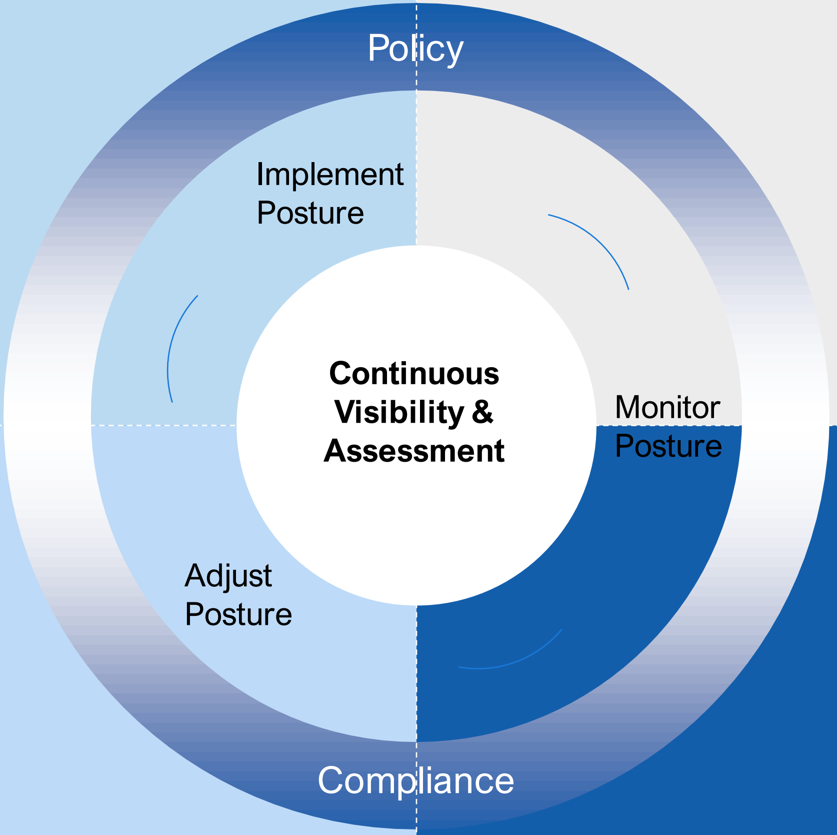
Baseline security posture

PREVENT

Harden Systems

Isolate Systems

Prevent attacks



Policy

Implement Posture

Monitor Posture

Compliance

Adjust Posture

Continuous Visibility & Assessment

Detect incidents

Confirm and prioritize risk

Contain Incidents

DETECT

Remediate

Review policy change

Investigate incidents

RESPOND

SHELT

24/7/365 NEXT GEN SECURITY OPERATION CENTER

Predict / Anticipate Threats

Discover Requirements

Vulnerability Mgt

Cyberspace Monitoring

reva

Digital Risks

BLACK KITE

Prevent Attacks

Adaptive Access / Defense Posture

VAPT & Red Team

Vulnerability Assessment & Penetration Testing

Security Controls

EDR IDS NAC NGFW

API Security MDM

CEQUENCE SECURITY SOTI

EDP

MATRIX42

Detect Incidents

Continuously monitor; Access Risk & Trust

Next Gen SIEM

FORTINET securonix TACIVOAR

API Security MDM

CEQUENCE SECURITY SOTI

Cloud Security EDP

WIZ MATRIX42

Brand Protection

reva

Respond to Incidents

Enable adaptive response

Digital Forensic Lab

Incident Response

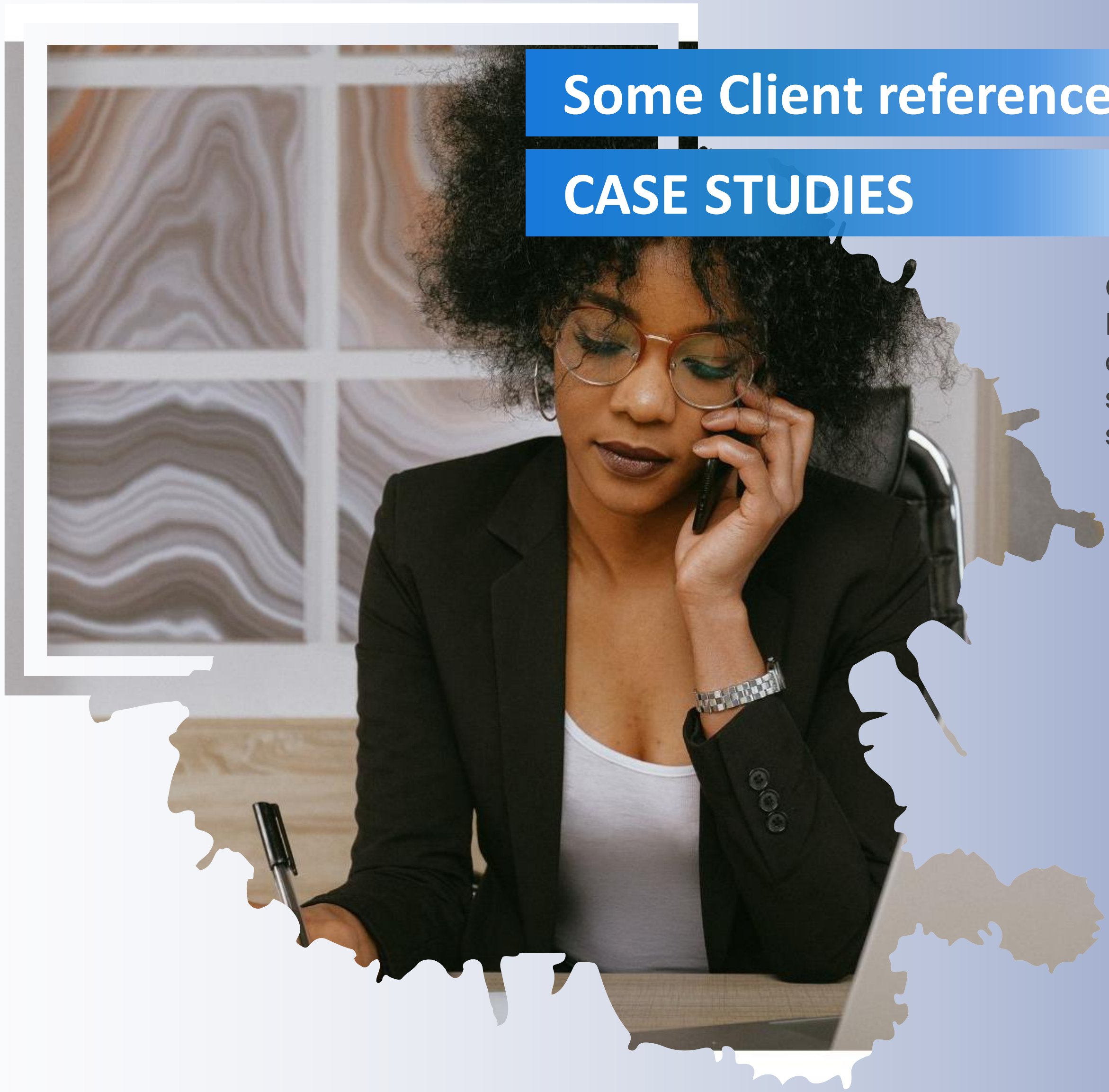
SOAR

FORTINET

ITSM & ITAM

MATRIX42

SHELT



Some Client referenced

CASE STUDIES

Our successful delivery of services to prestigious organizations in he EMEA region, enables us to better understand the requirements of our clients. We leverage on our knowledge and experience obtained from similar engagements and plan to provide seamless quality professional services to our clients.

Inside…

- ✓ Large European Bank
- ✓ Large Pan African Mobile Operator
- ✓ Large Pan African Investment Bank
- ✓ Global Cloud Content Security Provider
- ✓ Multi Regional Bank

Security Operations Center Implementation and Cyber Security Advisory Services

Large Pan African Mobile Operator

01 Challenge

- The client is a Pan African Mobile Network Operator with several presence in different African countries.
- The client engaged SHELT in order to enhance the security of its information system by adopting a proactive approach
- The client was concerned about cyber threat that is becoming more and more complex and the need to develop their information security capabilities in order to respond faster, work more efficiently and protect their core business.
- The Client lacked internal capabilities to face these challenges and thus wanted to outsource the Cyber Security Function to a competent firm

02 Solution

- We performed an initial assessment to determine the current capabilities and prioritize the different components and created a Gap assessment on internal client capabilities
- We carried out the implementation of the SIEM technology and defined the different security use cases and related reports and alerts
- We assisted the client in developing full incident and change management policies, procedures and processes
- We performed full Vulnerability assessment on its network components to determine the need for improvement
- We implemented several enhancements capable of detecting intrusions and vulnerabilities

03 Added Value

- We helped the client fix most of its present vulnerabilities (”known knowns”)
- We helped in the continuous monitoring of the environment
- We improved the detection time of attacks and therefore the security posture the Operator’s environment
- We detected several incidents and helped in their swift resolution
- We allowed the proper management of the different generated and collected log events
- We established an information security officer checklist in order to view and evaluate all changes and developed an operational playbook to be used during incidents

SHELT

Security Operations Center Implementation and Management

Large Pan African Investment Bank

01 Challenge

- The client is an international bank with several branches in different countries.
- The client engaged SHELT in order to enhance the security of its information system by adopting a proactive approach
- The client was concerned about cyber threat that is becoming more and more complex and the need to develop their information security capabilities in order to respond faster, work more efficiently and protect their core business.

02 Solution

- We performed an initial assessment to determine the current capabilities and prioritize the different components
- We carried out the implementation of the SIEM technology and defined the different security use cases and related reports and alerts
- We assisted the client in developing SOC related incident and change management policies, procedures and processes
- We implemented several network enhancements capable of detecting intrusions and vulnerabilities
- We defined a monitoring and improvement framework in order proactively detect and respond to potential threats

03 Added Value

- We helped in the continuous monitoring of the environment
- We improved the detection time of attacks and therefore the security posture the bank's environment
- We detected several incidents and helped in their swift resolution
- We allowed the proper management of the different generated and collected log events
- We established an information security officer checklist in order to view and evaluate all changes
- We developed an operational playbook to be used during incidents

SHELT

ADVANCED DETECTION AND RESPONSE CLOUD SETUP & INTEGRATION

GLOBAL CLOUD CONTENT PROVIDER

01 Challenge

- The client is a public listed Australian-headquartered global cybersecurity company, which has been delivering cybersecurity-as-a-service solutions to the market since 2004 and with a Global presence in five continents.

- The Client owns and host a global Cloud platform that enables service provider partners to deliver a comprehensive range of security services to their customers from a single platform 'as-a-Service'.

- The Client engaged SHELT in order to implement a customized solution to and automate threat detection and Automatically uncover and stop elusive threats with agility and precision that are not detected by even global security vendors.

02 Solution

- We performed an initial assessment to determine the current security capabilities of underneath technologies and provided along with the customer the right scenarios and built in solution algorithms for advanced detection of concealed threats .

- We carried out the integration over the cloud of our SIEM technology and enabled massive log ingestion, aggregation and message queuing, with central correlation of logs for the multitenant/multivendor platform
- We offered a single sign on seemless experience between the Client platform and our SIEM technology.

- We enabled alerting of advanced threats with a risk scoring algorithm into a single dashboard and integrated automated response within the solution.

03 Added Value

- We have provided a solution for continuous real-time monitoring of security services and automated threat visibility, detection, alerts and response.

- We have enabled through our solution Dark web monitoring services to report leakage of domains and user credentials from data breaches that present an increased attack surface and cyber risk to the client customers .

- We have enabled Continuous threat hunting via retrospective analysis of URL/Links and attachments in delivered emails.

- Our solution Provide in-built advanced protection against targeted phishing and impersonation attacks with a complete and detailed dashboards depicting the threat landscape.

SHELT

Digital Risk Protection with Brand & C-Level Online Identities Protection Service

Multi-Regional Bank

01 Challenge

- The client is a large Multiregional Bank who was targeted by hackers collecting leaked information on the web and targeting him by trying to exploit these information or impersonating his brand and C – Level executives.
- The client wanted a solution to monitor external internet activities and execute continuous proactive threat hunting on the cyberspace in order not only to detect threats but to predict and prevent any potential cyber attack and criminal activity being prepared.
- The Client engaged SHELT in order to implement REVA solution to and automate threat detection and stop these elusive threats.

02 Solution

- To further strengthen the security of its information system we took a proactive approach and implemented REVA for the client Digital Risk Protection
- We assisted the client by providing a real time platform that:
    - Scraps links on surface, deep and dark webs
    - Searches for information disclosed in the cyberspace
    - Identifies advanced threats and profile data vendors
    - Detect Brand and C-Level impersonation on the internet including social media sites
    - Provide cyber threat intelligence service
    - We also provided a 24x7 service for unlimited and continuous remediation of these threats.

03 Added Value

- Assisted the client in continously **detecting** and **taking down** more than
    - ✓ 7000+ pages of Facebook impersonations
    - ✓ 1500+ Instagram and Twitter imposters.
    - ✓ 1500+ phishing and malicious sites
    - ✓ 25+ Rogued Mobile App
    - ✓ 3000+ Email breaches
    - ✓ 2500+ Credit Cards leaks
- We reduced Attack surface by detecting weaknesses and vulnerabilities
- Presented weekly and monthly reports, with quantitative cyber threat and risk assessment..
- We have provided the company with remediation plans as well as our effective and operational assistance to enhance cybersecurity posture

SHELT

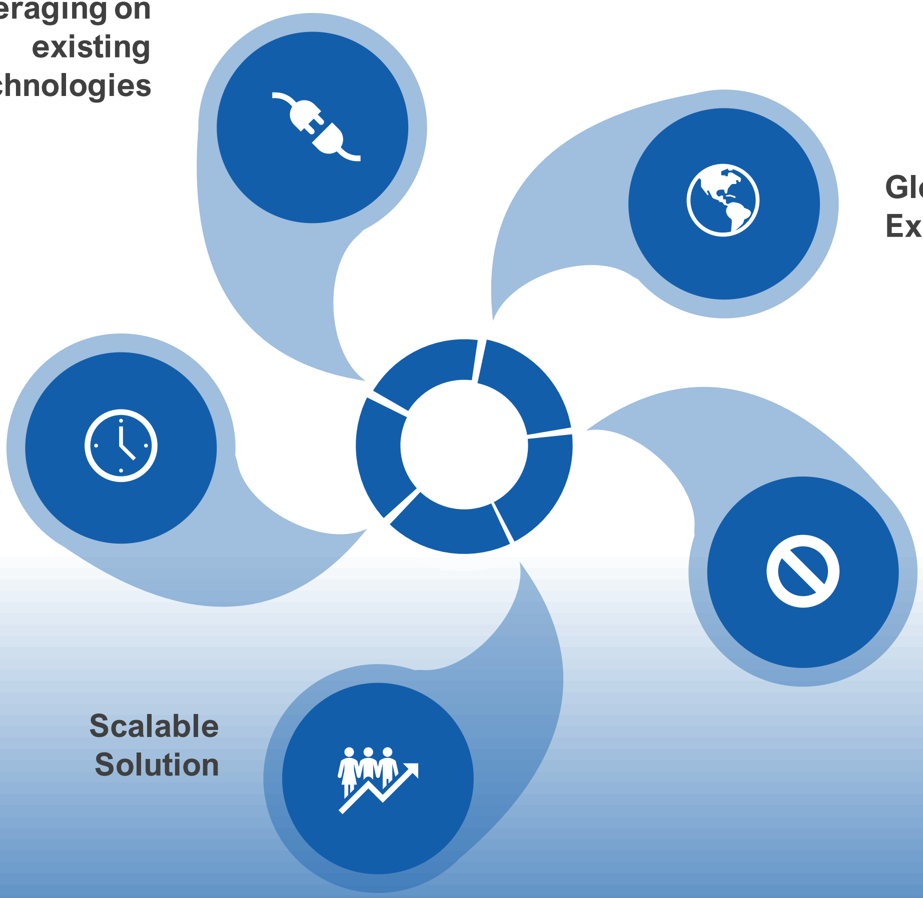
Adaptive Architecture

Advantages

Improve Your Security Posture

Minimize Your Operating Cost

Eliminate Your Security Risks



Leveraging on existing Technologies

Global Experience

24/7 Managed Services

Zero Initial Investment

Scalable Solution

SHELT

TOP CYBER SECURITY SOLUTIONS PROVIDER IN MENA 2024
SHELT
Awarded by CIOReview
SHELT
TOP MANAGED SECURITY SERVICES IN EUROPE 2021
Recognized by
SECURITY

Contact Us

+357-22503177 - info@shelt.com
www.shelt.com