CyberAntix

CYBERANTIX SOCAAS

Achieve improved cyber defence and response for your business with the CyberAntix Security Operations Center as-a-Service (SOCaaS).

CyberAntix

Premium cybersecurity for your business using advanced Service Operations Center (SOC) technology and process platforms, built using cutting-edge automation (SOAR) technologies and reinforced by a steadfast and expert SOC team.

Bolster your IT department's efforts and proactively counteract cyber risks and attacks through dedicated monitoring, detection and response to modern cybersecurity needs.

History of Cyber Threats

You have often heard that "threats are constantly evolving, and you need to keep on running to stay on top of them". This expression is often used to sell cyber-defence products that need constant updates, such as network IPS, or signature-based anti-malware solutions.

Our observations have revealed that:

- Current threats are slight evolutions or mutations of techniques developed decades ago, but still manage to slip through defenses at a great cost to businesses.
- Capabilities of "modern" malware (such as the latest ransomware threats) differ slightly from initial computer worms decades ago in their technical execution.

History

Deploy the CyberAntix SOCaaS service to achieve:

- **Faster prevention and restricted business loss**
  Through significant threat coverage and detection reliability, the CyberAntix SOCaaS service acts swiftly to prevent both regular and catastrophic business loss.

- **Visibility, prevention, and deterrence with special access**
  Mitigate sensitive scenarios where prevention is typically not possible, such as external vendors and partner access, or IT administrator auditing.

- **Regulatory or industry compliance**
  Fulfil your compliance requirements through activity monitoring, incident detection, proactive investigation and incident response as stipulated in compliance frameworks, industry or local legal requirements.

Achieve

Minimise cyber risks with CyberAntix START-UP designed to proactively detect and monitor cyber threats.

Combine endpoint detection and response with leading next generation anti-virus and expert monitoring and response.

Two factor authentication

Verifies the identity of all users before granting access to corporate applications.

- **Reduce Security & Compliance Risk**
  Improve enterprise security and risk posture while ensuring regulatory compliance.

- **Improve End User Productivity & Experience**
  Effective, scalable security that is easy to use, easy to deploy and easy to manage.

- **Reduce Total Cost of Ownership**
  Efficient and affordable security with lower investment and management overheads.

- **Enable Organisational Agility**
  Deliver modern security solutions that support evolving enterprise needs, at scale.

DNS Protection

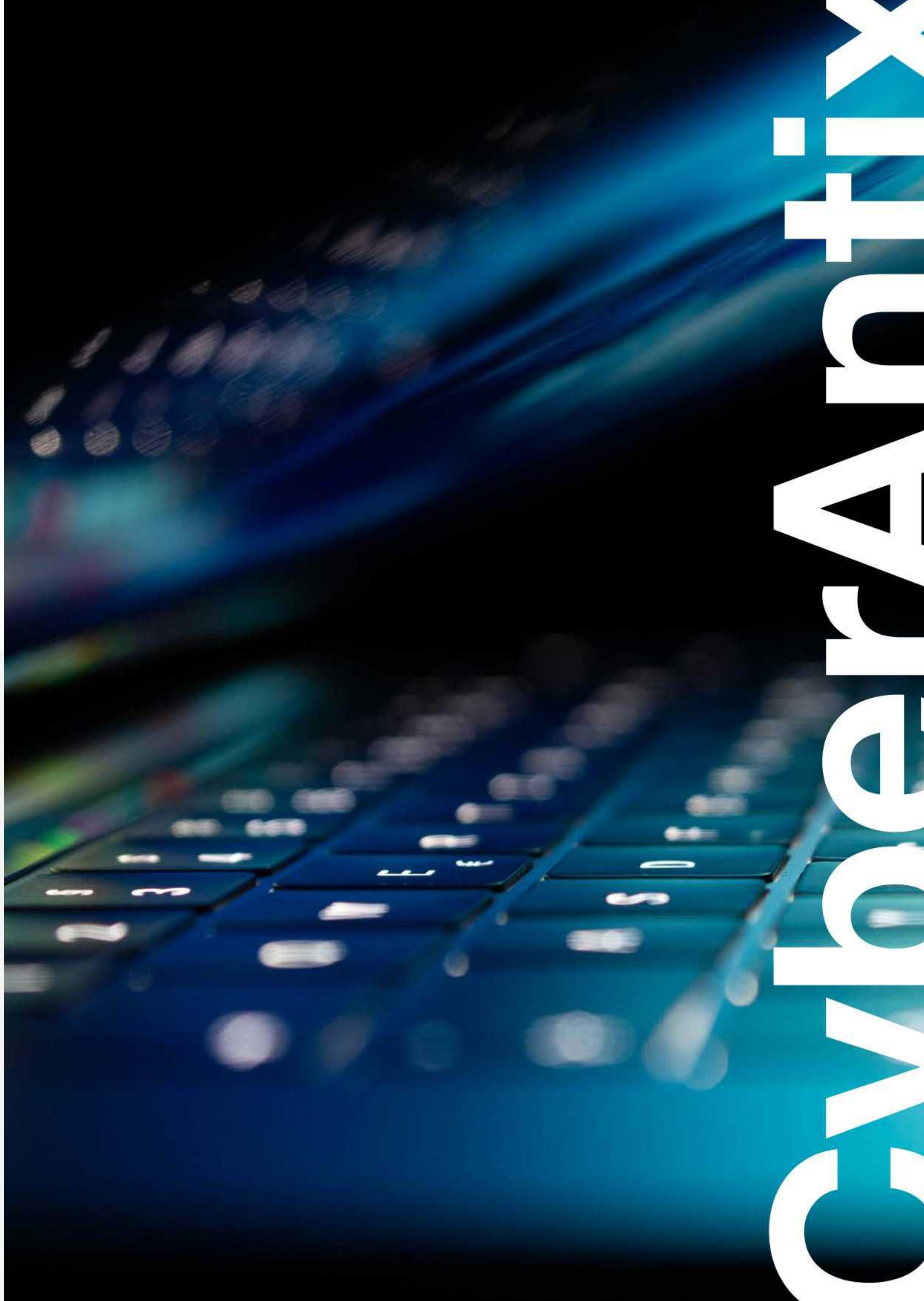
Provides first line defence against threats.
Multiple security functions in a single cloud security service.

- SND layer security
- Secure web gateway
- Cloud-delivered firewall
- Cloud access security broker (CASB)
- Interactive threat intel

CyberAntix Advanced End Point Detection and Response (EDR)

Provides first line defence against threats.
Multiple security functions in a single cloud security service.

- SND layer security
- Secure web gateway
- Cloud-delivered firewall
- Cloud access security broker (CASB)
- Interactive threat intel



CyberAntix SOC offers solutions for your business as it grows. We also provide bundled solutions tailored for a comprehensive approach.

Security Operations

- Real-time monitoring and investigation
- Data source tuning
- Customer communications
- Monthly reporting

Incident Response

- **Level 1:** Incident containment creation
- **Level 2:** Level 1 + remote or on-site incident remediation

Proactive Detection Expansion

- Threat hunting
- Vulnerability assessment and management
- Threat intelligence sharing
- Penetration testing
- Code review
- Deception and honeypots

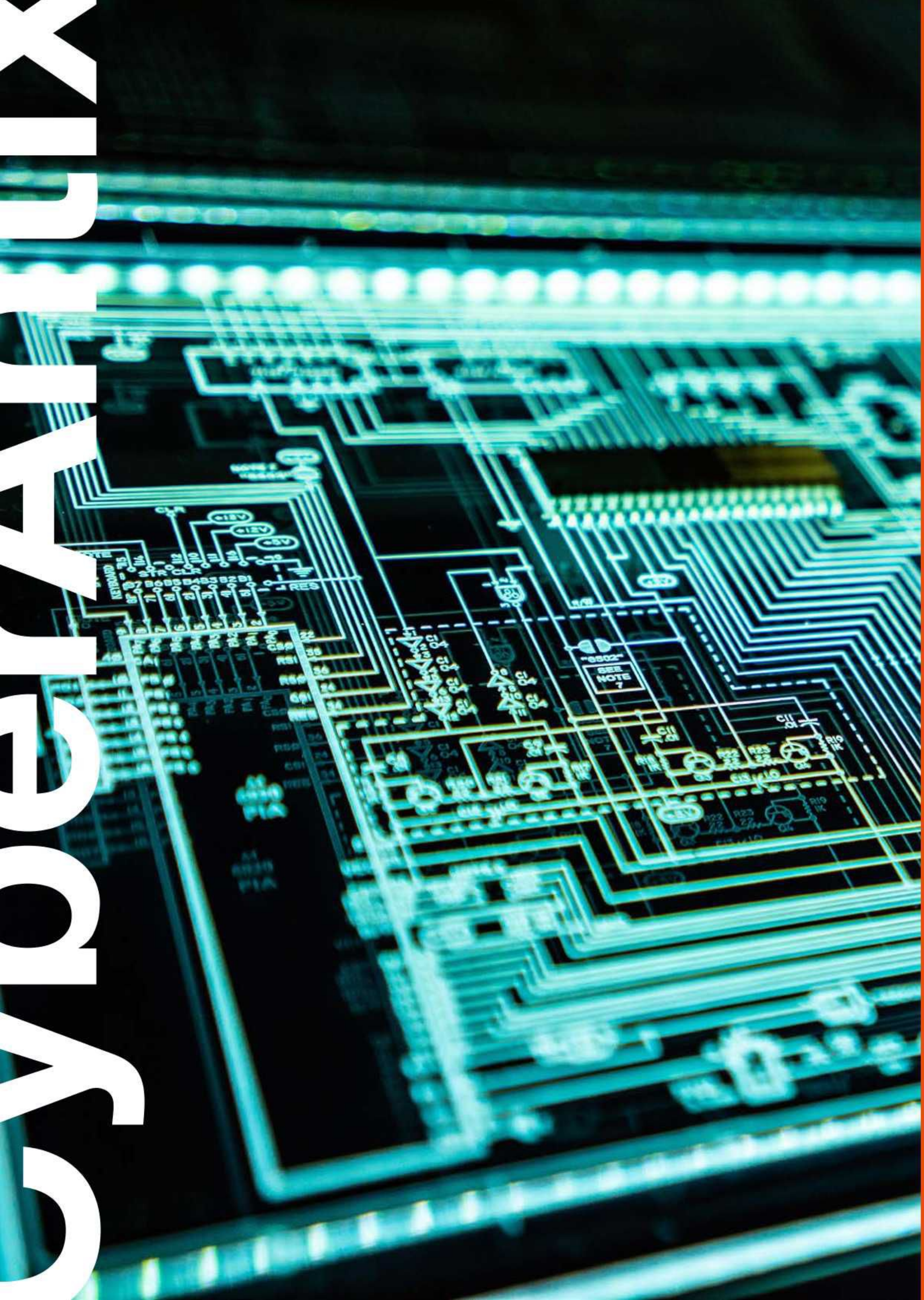
Lifecycle Consulting

- In-depth report interpretation
- In-depth risk analysis
- Security roadmap
- Security maturity improvement

Security Engineering

- Gap analysis
- Security architecture services
- Complex event source handling
- SEM deployment and tuning
- EDR deployment
- NTD/ IPS deployment

Security



Today’s malware attacks combine multiple advanced techniques with realtime hacking. To minimise your risk, you need advanced prevention, detection and monitoring to secure the whole attack chain.

Next Generation Firewall (optional)

- Stops data-stealing attacks with Synchronised Security.
- Automatic analysis and isolation of compromised systems to reinforce endpoint protection.
- Sharing of important wealth, status and telemetry information between Firewall and EDR, Synchronised Security can see, stop and secure it—before these threats can cause any damage.

Back up as a service (BaaS) (optional)

Protect personal or business data and information from the risk of loss associated with user error, hacking, or other technological hazards. CyberAntix Back up as a service encompasses:

- Online backup service to a remote secure cloud-based data repository over a network connection.
- Regular backup to an offsite data storage facility for files, folders, or hard drive contents by a service vendor.

Service Parameters and Service Level Agreements (SLAs)*

SLA Parameter	Basic	Continuous
Monitoring service availability. SOC analysts provide incident detection and triage during this timeframe.	24x7 (continuous)	24x7 (continuous)
Incident response service availability. SOC incident responders offer remote or optionally, on-site assistance with confirmed incidents.	24x7 (continuous)	24x7 (continuous)

*custom timeframes are available upon request.

CyberAntix SOC provides guarantees of response times as part of the service contract. There are two core SLA parameters:

First Expert Verdict (FEV): The amount of time, from when the potential incident has been logged by the SOC technical systems, until the time the initial triage is completed and an expert verdict is delivered for the suspicious activity. This encompasses factors like the likelihood of the incident and initial severity. This time is contractually set to 60 minutes but can be customised.

Time-to-IR: The amount of time, from when a potential incident has been determined to require incident response procedures, and the initiation of the IR process with dedicated incident responders. This time is contractually set to 60 minutes and can also be customised.

Parameters

SLA Parameter	
SOAR Automation	CyberAntix SOC automates alert investigations through detailed and up to date playbooks.
SIEM	Management of your MDR and IR if you have already invested in an approved SIEM.
International Back-Up	Access to international reinforcements for Incident Response based on the award-winning NIL SOC in Europe.
Local presence	Through the Sizwe footprint we have nationwide geographical reach.
SOCaas	As you increase your cyber security, you can progress to being a complete SOC customer.

CyberAntix

Contact your cybersecurity expert on

012 6575300 or email Info@cyberantix.co.za