AUDIT • ADVISORY • TAX

BDO CYBER LAB TECHNOLOGY SOLUTIONS CATALOGUE

Helping organisations protect their IT and OT estates against cyber threats and implement measures to achieve and maintain cyber resilience.

List of OEM Partners:

1. AXIO
2. TERRANOVA
3. DARKTRACE
4. FORTINET
5. CHECK POINT
6. WATCHGUARD
7. EGRESS
8. TESSIAN
9. CYMULATE
10. CEQUENCE
11. CHECK POINT

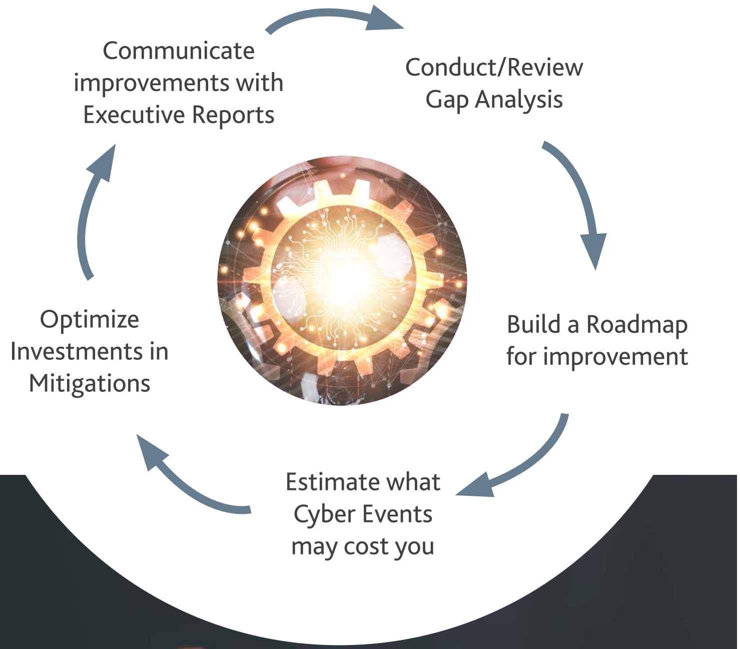
1. CYBER RISK MANAGEMENT WITH AXIO (DIGITAL RISK TRANSFORMATION)

The BDO Cyber Lab adopted an approach to conduct risk assessments that ensure our clients enjoy the benefit of viewing the complete "before" picture and the gap that exists from the desired state stipulated by compliance standards or frameworks. Consequently, we are in a good position to advise clients on the necessary controls and measures that will reduce that gap over time, while measuring their progress. With Axio, we can assess more than 300 security controls based on NIST and ISO standards and help to manage remediation processes. Additionally, we can perform risk quantification and assist the client with a baseline for securing cyber insurance, including stress testing the cyber insurance cover.

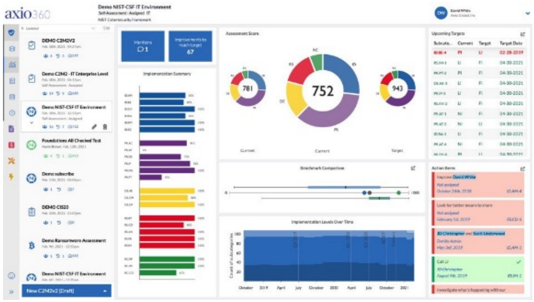
Axio 360 Ecosystem

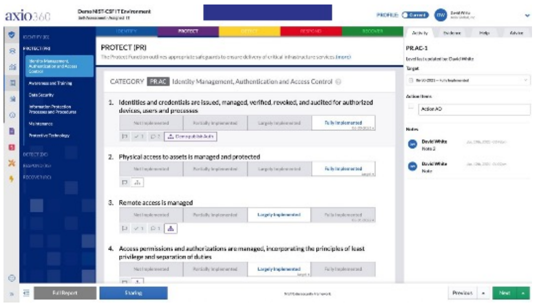
Smarter Cybersecurity Decisions Made Faster

- Assessments can be completed 70% faster – allowing time to focus on subsequent improvement projects.
- A single source of truth for client program improvements.
- Risk Quantification method that can provide business aligned analysis in under a week.
- Model various controls against the quantified cyber events to gain support from Executives.
- Model the risk if controls were reduced
- A tool that supports continuous program management.



Communicate improvements with Executive Reports
Conduct/Review Gap Analysis
Build a Roadmap for improvement
Estimate what Cyber Events may cost you
Optimize Investments in Mitigations

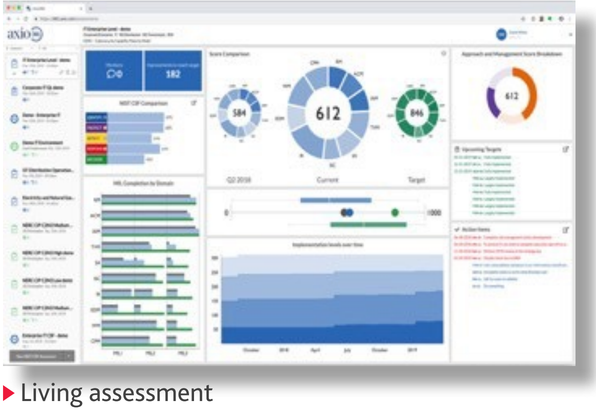




axio360
Demo NIST-CSF IT Environment
PROTECT (PR)
CATEGORY PR.AC Identity Management, Authentication and Access Control
1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
2. Physical access to assets is managed and protected
3. Remote access is managed
4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

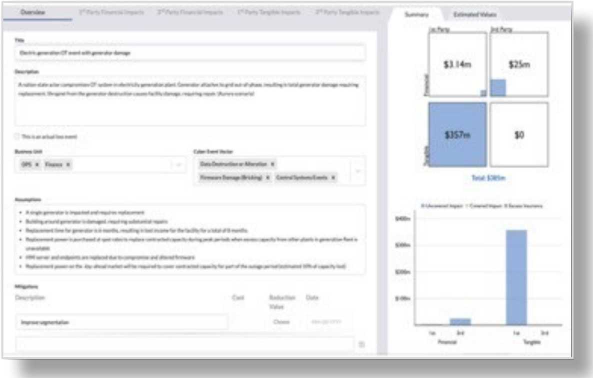
BDO HELPS YOU GAIN CONTROL OF CYBERSECURITY RISK MANAGEMENT IN YOUR ORGANISATION

1 *Is my cyber program maturing as needed?* Cybersecurity Planning & Management



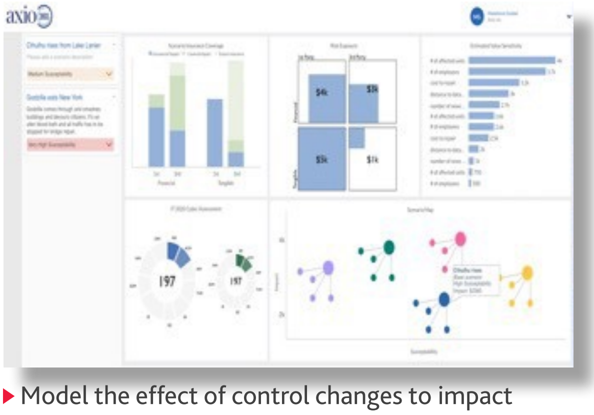
- Living assessment
- Benchmarking
- Improvement planning and tracking
- Executive reporting

2 *What's my exposure in financial terms?* Cyber Risk Quantification



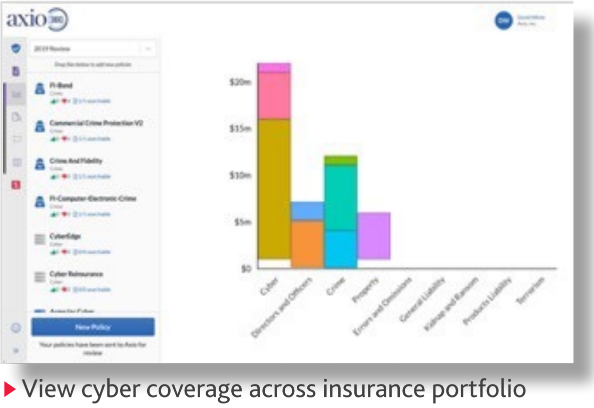
- Transparent, collaborative risk modelling
- Defensible impacts
- Accurately quantify risk in hours, not months
- Executive reporting

3 *Where should I invest to reduce risk?* Control Initiatives



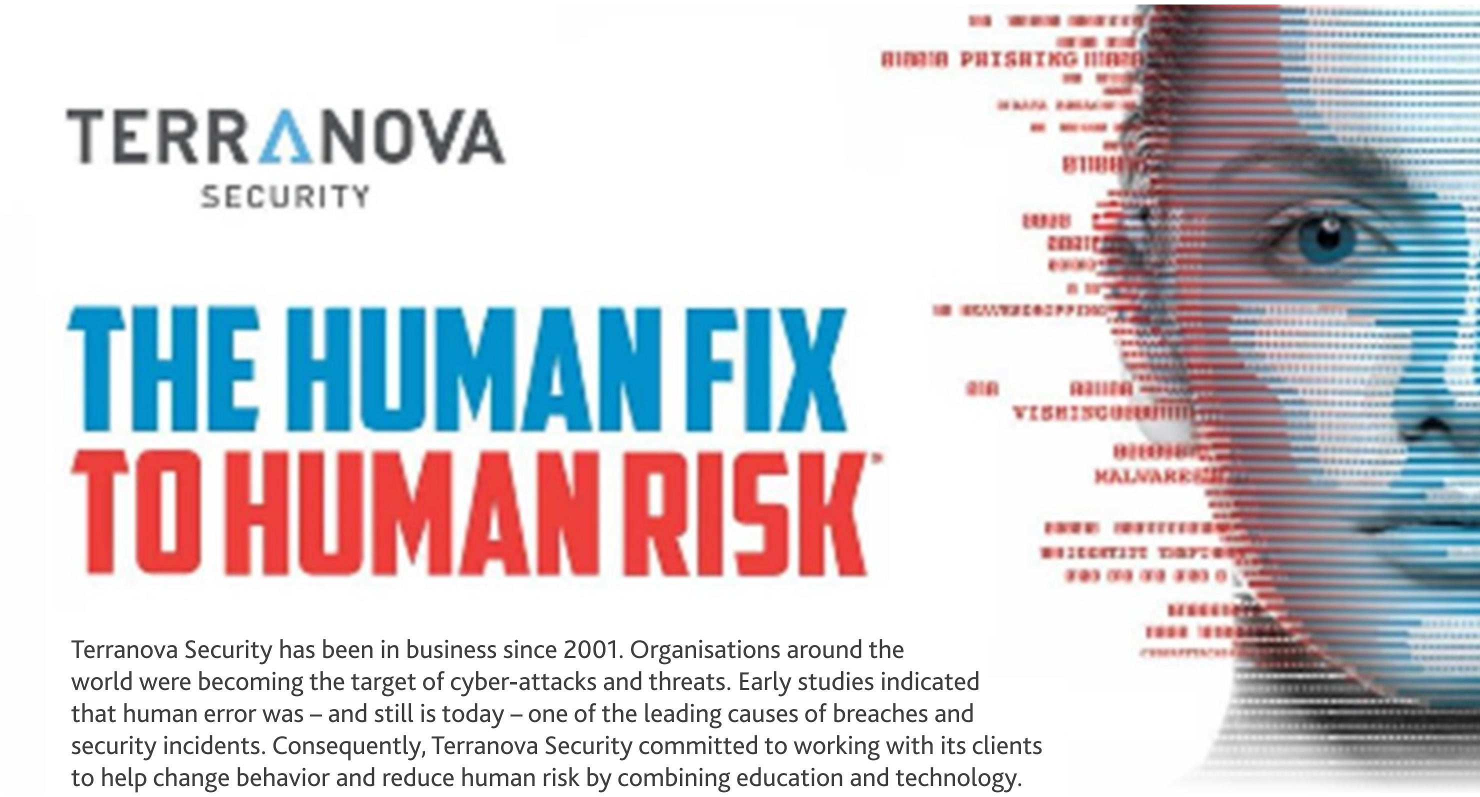
- Model the effect of control changes to impact and susceptibility
- Compare controls to optimise selection
- Track risk reductions

4 *Do I have the financial ability to recover?* Insurance Stress Testing



- View cyber coverage across insurance portfolio
- Evaluate coverage limits and triggers
- Identify exclusions and gaps

2. MANAGING THE HUMAN RISK (TERRANOVA)



Terranova Security has been in business since 2001. Organisations around the world were becoming the target of cyber-attacks and threats. Early studies indicated that human error was – and still is today – one of the leading causes of breaches and security incidents. Consequently, Terranova Security committed to working with its clients to help change behavior and reduce human risk by combining education and technology. Below are recent major milestones:

- March 2020: Terranova Security partners with tech giant Microsoft to bring the best in security awareness content to users, globally. All content and phishing simulations are based on real-life threats, on real-time intelligence provided by Microsoft.
- July 2020: Cyber Security Hub is launched with engaging, shareable cyber security awareness content to help supplement communication and reinforcement tools.
- October 2020: Gone Phishing Tournament (sponsored by Microsoft) launched as global phishing simulation event to help security leaders compare their click rate with peers by industry, geo and segment. The Global Phishing Benchmark report continues to be leveraged by organisations globally to benchmark their security awareness program.
- May 2021: New partnership to be announced with Security Innovation that will augment the content library with training for software developers.

Terranova Security is:

- Recognised as a representative vendor in 2020 Market Guide for Security Awareness Computer- Based Training
- Recognised as a global leader in Gartner's Magic Quadrant for Security Awareness Computer- Based training in 2019, 2018, 2017, 2016 and 2015.
- Gartner Peer Insights Region - Customer's Choice 2021.
- Awarded the Customers' Choice in 2020 and 2019 for Security Awareness by Gartner Peer Insight.

20+ Years Expertise 1000+ Security Awareness and Phishing Simulation Campaigns	10M+ Cyber Heroes Users Trained Globally	200+ Countries Global Customer Base	90% Renewal Rate Driven By Customer Excellence Core Value	150+ E-learning Courses 40+ Languages	Leader inSecurity Awareness Recognized by Gartner Peer Insight Customers Choice

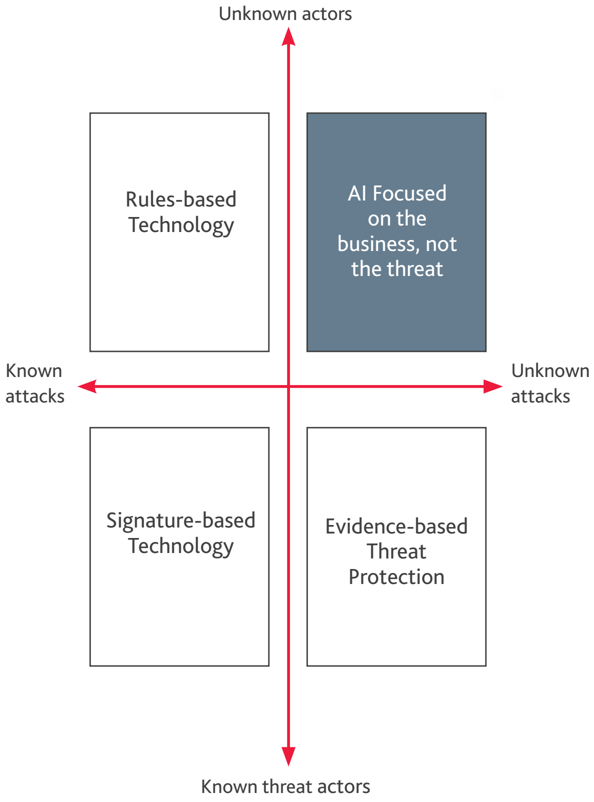
3. DARKTRACE ADVANCED AI SOLUTION FOR NETWORK AND EMAIL SECURITY

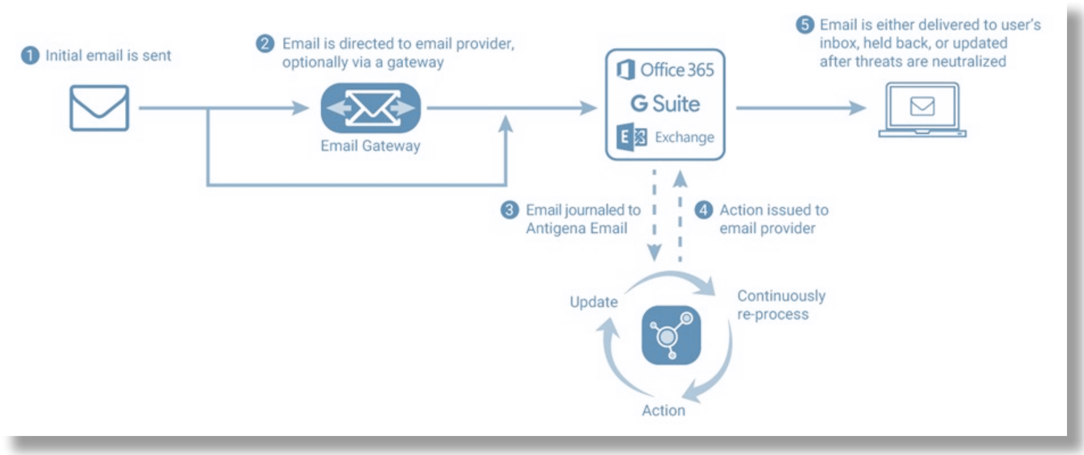
Darktrace is the world's leading machine learning company for cyber security. Created by mathematicians from the University of Cambridge, the Enterprise Immune System uses AI algorithms to autonomously detect cyber-threats. Darktrace's technology has been deployed over 10,000 times across six continents, and the company has over 1500 employees across 44 global offices, with dual headquarters in San Francisco and Cambridge, UK. Darktrace's team combines unique expertise across the fields of mathematics, software, and government intelligence.

Traditional approaches to security assume it is possible to keep threats outside of a network by strengthening the enterprise's external boundaries. As networks have grown more complex and threats have become more sophisticated and rapid, traditional approaches have become insufficient to defend enterprise networks.

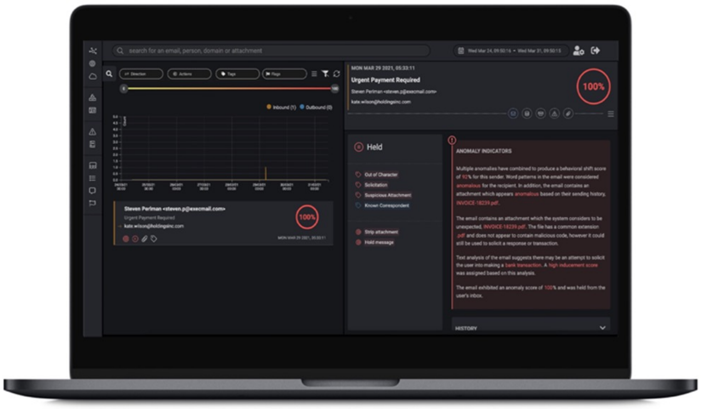
Darktrace's Cyber AI Platform delivers an 'immune system' style of defence to enterprises for the first time. Based on proprietary AI algorithms, unsupervised machine learning, and probabilistic mathematics, Enterprise Immune System technology learns a sense of 'self' for an organisation, its users and its devices. As such, it has become the only technology capable of defending against novel threats, including trusted insiders that start behaving in an abnormal manner.

Darktrace's artificial intelligence stops even the most advanced email threats. It works fundamentally differently by 'understanding the human' behind the email address, learning what employees do, who they interact with, how they write, and the substance of their typical conversations. The Darktrace AI looks at 750 metrics on every single email-inbound, outbound, and lateral - to form this mathematical understanding.


Unknown actors
Rules-based Technology
AI Focused on the business, not the threat
Known attacks
Unknown attacks
Signature-based Technology
Evidence-based Threat Protection
Known threat actors


1 Initial email is sent
2 Email is directed to email provider, optionally via a gateway
Email Gateway
Office 365
G Suite
Exchange
5 Email is either delivered to user's inbox, held back, or updated after threats are neutralized
3 Email journaled to Antigena Email
4 Action issued to email provider
Update
Continuously re-process
Action

Darktrace Antigena represents a critical step toward a fully autonomous cyber security system, empowering the Enterprise Immune System to act against cyber-threats for the first time. Based on the 'pattern of life' understood by the Enterprise Immune System, Darktrace Antigena acts as a 'digital antibody', neutralizing threats in the network automatically.


search for an email, person, domain or attachment
Wed Mar 24, 09:50:16 • Wed Mar 31, 09:50:15
Direction
Actions
Tags
Flags
Inbound (1)
Outbound (0)
Steven Perlman <steven.p@execmail.com>
Urgent Payment Required
kate.wilson@holdingsinc.com
100%
MON MAR 29 2021, 05:33:11
MON MAR 29 2021, 05:33:11
Urgent Payment Required
Steven Perlman <steven.p@execmail.com>
kate.wilson@holdingsinc.com
100%
Held
Out of Character
Solicitation
Suspicious Attachment
Known Correspondent
Strip attachment
Hold message
ANOMALY INDICATORS
HISTORY

Multiple anomalies have combined to produce a behavioral shift score of 92% for this sender. Word patterns in the email were considered anomalous for the recipient. In addition, the email contains an attachment which appears anomalous based on their sending history, INVOICE-18239.pdf.

The email contains an attachment which the system considers to be unexpected, INVOICE-18239.pdf. The file has a common extension .pdf and does not appear to contain malicious code, however it could still be used to solicit a response or transaction.

Text analysis of the email suggests there may be an attempt to solicit the user into making a bank transaction. A high inducement score was assigned based on this analysis.

The email exhibited an anomaly score of 100% and was held from the user's inbox.

4. DELIVERING ADVANCED END POINT, NETWORK AND CLOUD SECURITY PROTECTION

BDO has established partnerships with Fortinet, IBM, Watchguard and Check Point to provide end-to-end cybersecurity solutions for the enterprises, irrespective of size or industry. BDO has inhouse technical expertise to install, implement, configure and support product solutions from user & access security, network security, security operations, to cloud security.

FORTINET

IBM

WatchGuard

Check Point SOFTWARE TECHNOLOGIES LTD

5. DELIVERING ADVANCED EMAIL SECURITY FOR EFFECTIVE PROTECTION AND DATA LOSS PREVENTION

Egress and Tessian provide a Human Layer Security platform to secure people using email. Employees spend 40% of their time at work in email and the combination of human vulnerabilities (people make mistakes, people break the rules and people can be hacked) with the insecure nature of email (open by design, decentralised) means that a large number of security breaches originate with an employee doing something wrong when using email. These solutions provide the capability to:

- Automatically prevent spear phishing, Business Email Compromise and impersonation attacks impossible to detect with Secure Email Gateways and legacy email security controls.
- Automatically prevent accidental data loss due to misdirected emails.
- Automatically prevent data loss and insider threat caused by data exfiltration on email.
- Design and deploy customised policies to ensure employee email activity is compliant and secure.

TESSIAN

egress

6. VISIBILITY OF API'S AND END-TO END SECURITY (CEQUENCE)

Cequence Security: The Only Unified API Protection Solution

Eliminate API risk at every phase of your API protection lifecycle by improving discovery, detection and defense while reducing cost, minimising non-compliance, fraud, business abuse and data losses. Achieve API security through the following Cequence capabilities:

API SPYDER

Proactively discover what attackers see and categorise based on risk – all without deploying any software or traffic flow modifications. Prioritise remediation efforts based on severity.

API SENTINEL

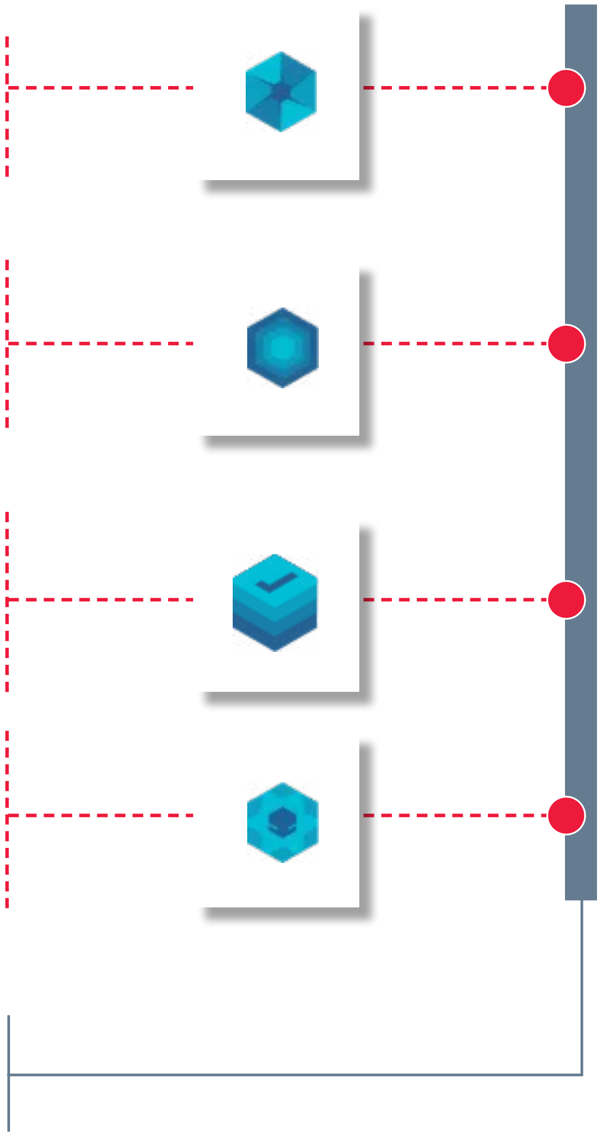
Create an up-to-date API catalogue with continuous API discovery, inventory tracking and threat detection. Assess and remediate sensitive data handling and authentication errors during development.

API TESTING

Discover and remediate API vulnerabilities using a combination of development and security focused test scenarios.

API SPARTAN

Prevent automated API attacks and business logic abuse with unmatched efficacy rates using behavioural fingerprinting that tracks attackers regardless of how rapidly they retool.



CEQUENCE®
SECURITY

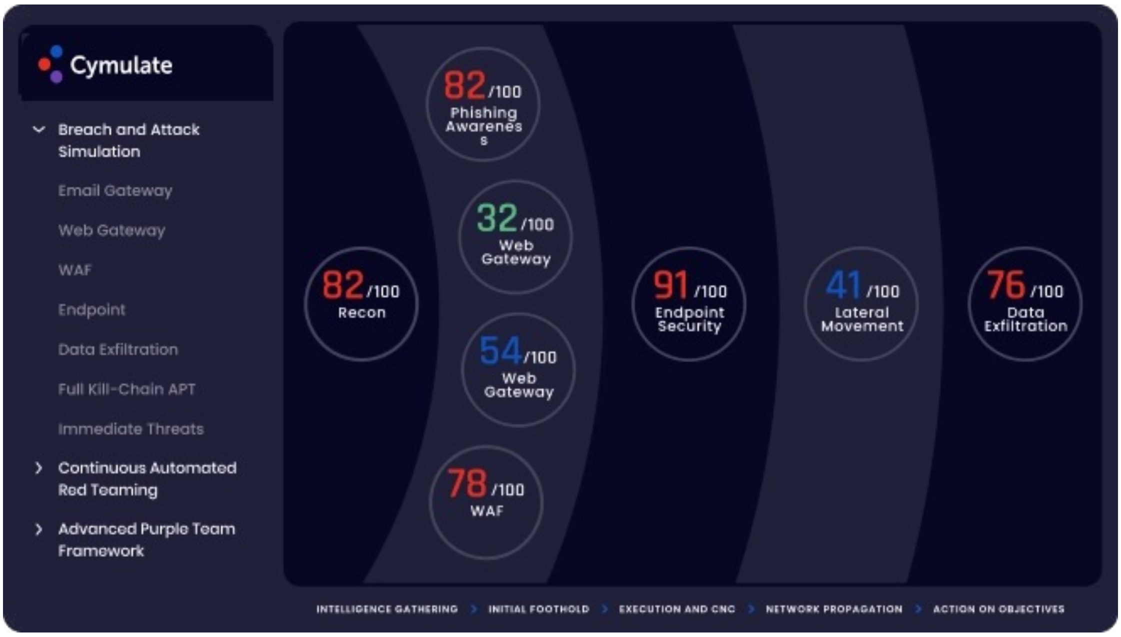
7. AUTOMATED BREACH AND ATTACK SIMULATION (CYMULATE)

With the broadest coverage in the industry, Cymulate Continuous Security Validation helps to manage the cybersecurity posture across the entire organisation. It takes a proactive approach by launching red team campaigns and purple team scenarios in a continuous and automated fashion. Executive reports highlight high-risk security deficiencies and quantifies risk based on a consistent standards-based risk scoring methodology across all the most important cybersecurity domains:

- Attack Surface Management
- xDR/SIEM/SOC Validation
- Security Control Validation
- Cloud Security Validation
- Vulnerability Management
- Employee Security Awareness

Automation of the security assurance process enables you to establish an enterprise-wide security baseline and continuously maximise your security posture, assure improved effectiveness, and prevent security drift.

Cymulate provides visibility across the full skill chain and automatically validates that security programs are effective, continuously optimises remediation efforts, and rationalises requests for additional budget or headcount.



Cymulate

FOR A CLEAR PERSPECTIVE, PLEASE CONTACT US:

GILCHRIST MUSHWANA
Director and Head of Cybersecurity
gmushwana@bdo.co.za

/BDOSouthAfrica

/bdoafrica

/bdo_sa

/bdosouthafrica

/company/bdo-south-africa

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO to discuss these matters in the context of your particular circumstances. BDO, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of BDO South Africa Services (Pty) Ltd. The opinions expressed are in good faith and while every care has been taken in preparing these documents, BDO South Africa Services (Pty) Ltd makes no representations and gives no warranties of whatever nature in respect of these documents, including but not limited to the accuracy or completeness of any information, facts and/or opinions contained therein. BDO South Africa Services (Pty) Ltd, its subsidiaries, the directors, employees and agents cannot be held liable for the use of and reliance of the opinions, estimates, forecasts and findings in these documents.