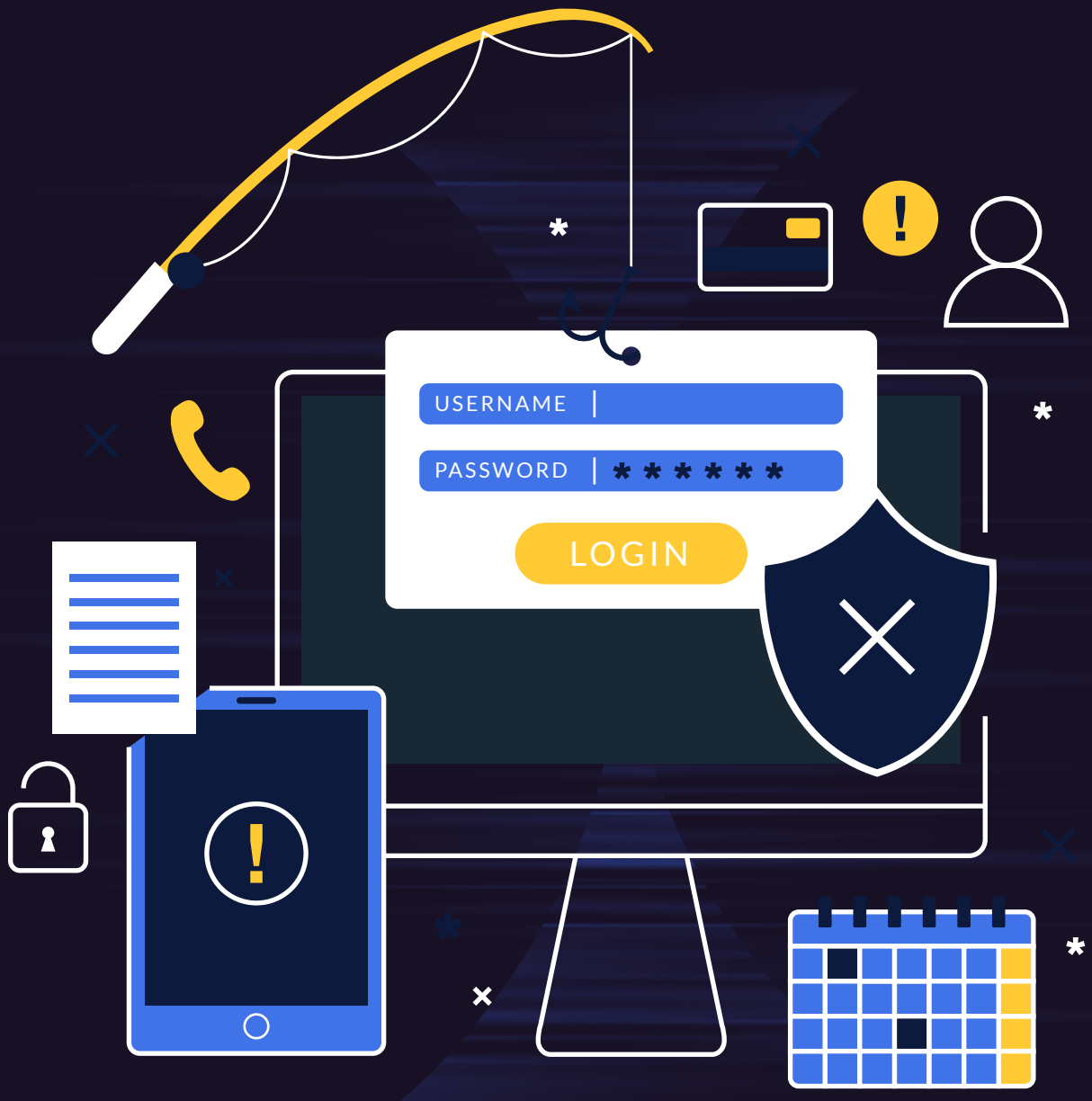
seclogic

CYBERQ ORO

Threat Awareness Platform

PRODUCT DATASHEET



CyberQ ORO (Organisation Risk Orchestration)

CyberQ ORO helps security leaders in enterprises measure, communicate and reduce human risk to keep their companies safe from cyber threats. One of the most challenging aspects of building a cybersecurity program is the human risk component.

CyberQ ORO provides a way to quantify this human risk across the entire organisation using security incident data, automated assessments & training. Quantifying human risk and analyzing it as part of an overall cyber risk framework provides unique insights to security teams & leaders.

CyberQ ORO evaluates employees risk posture through multiple unique threat determinants such as simulating multi-vector phishing attacks (delivered via Email, SMS, WhatsApp) training outcomes, situational awareness assessment, external threat exposure/learning user cyber behavior. By collating unique threat vectors determinants, a risk posture of all the users, departments, and overall organisation are calculated, and through automation techniques, well-defined educational content is triggered for users who demonstrate vulnerable posture.

Threat Evolution– Targeting Humans vs. Machines

There's a three-legged stool of security failures: faulty code, misconfiguration, and social engineering attacks. Phishing attacks, a social engineering technique, have been successfully used to compromise global organisations of all sizes across sectors. Statistics vary, but phishing has cost organisations billions of dollars via business email compromise scams alone, as well as the loss of reputation.

As technology becomes more advanced, the adversaries' TTP's are also becoming sophisticated, vectors such as Spear Phishing, Session Hijacking, Content Injection, Vishing, Smishing, Telegram, Link Manipulation,etc. are detected by various global security vendors.

In the wake of brute force targets, users must have knowledge of how the adversaries conduct frauds, understand their cyber exposure, and be aware of anti-phishing techniques to protect themselves from becoming victims.

KEY FEATURES

- SAAS Offering
- Risk Posture - Users,Departments & Organisation
- Continuous Emlpoyee Security Risk Assessment
- Multi-Vector Attack Simulations - Email, SMS*, WhatsApp*
- Automated/Targeted Training Campaigns
- Visibility into Multi-variate User Actions
- Cyber Threat Intelligence*
- Analytics & Reporting

APPROACH

Employee Assessment

Central repository of global phishing trends. Increase phishing detection through leveraging the power of employee reporting

Collaborate

Comparison of historical analysis with the global benchmark statistics

Profile

Analyze user cyber behavior, map weak & strong points, track their awareness level & generate reports

Train

Phishing simulation & awareness training for employees, contractors through engaging videos & gamified quizzes to reduce risk

PRODUCT FEATURES

Continuous Employee Assessment i.e. Multi-Vector Phishing Assessments

» **Organisation Cumulative Risk:**
Campaign-wise assessment for departmental groups, users and their actions, risk analysis & insights like OS & browser distributions

» **Risk Posture for Single/Multi-Vector Phishing Assessments:**
User and departmental group risk levels generated over multi-vector phishing campaigns via Email, SMS, or WhatsApp, etc

AI-Driven Automated Training Assignment

» Automatic assignment of user training based on user risk history and performance over recent campaigns*

Risk Management & Trending

» **Overall Risk Score:**
Comprehensive analysis of departmental groups and individual users on their phishing assessments and generated results based on classified risk levels

» **Overall Risk Prone%:**
A higher risk prone% indicates vulnerable users and groups for real-time phishing attacks. This provides an overall analysis of prone probability to train users who are more vulnerable to phishing attacks than other users

» **No. of Users and Departmental Groups at Extreme Risk:**
An umbrella view of the total number of users and user groups at extreme risk based on the five risk levels of CyberQ ORO i.e. extreme, severe, elevated, mild, and no risk

Historical Users, Departments, Trainings Analysis & Reporting

» **Top 5 High/Low-Risk Groups:**
A catalog of extreme risk user groups to focus on remedial training and to incentivize low-risk users for their real-time vigilance

» **Top 10 High-Risk & Low-Risk Users:**
Comprehensive listing of extreme risk users along with their risk levels, risk prone %, susceptible phishing vector

Just-in- Time Phishing Multi-Vector Templates

» **Template Library:**
Wide range of BEC and social phishing templates available

» **Landing Page Library:**
Precisely curated phishing landing pages for believable phishing simulation and to capture user actions over it

Extensive Cyber Training Video Library in Multiple Global Languages

» **Whiteboard Training:**
Get access to the performance and progress made by your users and groups on various training focusing on real-world phishing scenarios assigned to them

» **Multi-Language Support:**
Whiteboard training videos available in multiple global languages like English, Spanish, Arabic, French, and German

Comprehensive User Behavior Metrics & Global Benchmarking

» **Capturing User Actions & Attack Simulation:**
CyberQ ORO captures the user actions over the phishing campaigns like emails opened, clicked, replied, credentials entered, attachment downloaded, macro-enabled, etc. to analyze their preparedness and generate analytics for remediation

» **Global Benchmarking:**
An encapsulated overview of your organization's risk trends of users and groups and your organisation's posture compared with global benchmark

» **Reporting Features:**

- Risk Score Report
- Risk Prone % Report
- User Report Card
- Group Report Card
- Training Report Card

Automated Training Reminders

Automatic training registration & reminder notification feature - allows sending e-mail notifications, reminding all the participants about pending training courses they have yet to take. Sending bulk notifications is easy and can be done in a matter of minutes!

» **Automated**
Periodic reminders are sent automatically to the participants.

» **Manual**
Training reminders as well as training registration notifications can be sent to the intended participants by the Administrators.

Multi-Layer SaaS and Phishing Intelligence

» **Multiple SaaS Options:**
Availability for self-managed, partner-managed, and SecLogic-managed CyberQ ORO services

» **Phishing Intelligence:**
In house and third-party collaborations to build JIT phishing templates

Bring Your Own Content

» **Newsletters/Policies and Posters:**
BYOTC (Bring your own training content) as per InfoSec & compliance requirements

» **Track and Acknowledge:**
Assign posters, policies and newsletters and track user acknowledgement, enforce security culture

Alignment with NIST & SANS Frameworks

» **Phishing Templates:**
JIT (just-in-time) phishing templates that aligns with NIST Phish Scale Methodology

» **Training Library:**
Whiteboard user training videos aligned with NIST NICE Framework

» **SANS Framework:**
CyberQ ORO aligns with the SANS Security Awareness Maturity Model promoting good security practices and employee education

Subscription Available in Annual, Multi Year Plans

» Employee assessment as a service is available with the following subscription models:
- Annual
- Multi Year

TEMPLATE CATEGORIES

01 **Credentials Entry**
To Identify Users Vulnerable to Credential Harvesting

02 **Reply**
To Identify Users Vulnerable to Data Leakage or Causing Financial Loses

03 **Attachment**
To Identify Users Vulnerable to Downloading Malicious Attachments

TRAINING LIBRARY

Trainings can be assigned to the employees in the form of Video, Policy & Newsletters through the platform

- Security Awareness Overview
- Prevailing Common Threats
- Mobile Security Landscape
- Password Best Practices
- Deciphering Phishing
- Understanding Ransomware
- Insider Threat Overview
- Leadership Training
- New Employee Onboarding
- Work From Home Best Practice
- Avoiding Frauds
- Staying Secure Online
- Demystifying GDPR
- Delusive Social Engineering
- Data Privacy
- PCI-DSS
- OmniPresent Office 365
- Try Zooming In
- Ubiquitous Google Workspace
- Wobbly Webex Attacks
- The Boss is Always Right?
- MS Teams Trickery
- Look Out Linkedin
- Speculating Salesforce - Finance
- Speculating Salesforce - Sales
- Decoding Docusign
- Dropbox Email Faux

Training Video Languages Supported:

ABOUT SECLOGIC

SecLogic provides cloud security & cyber risk management solutions to aid any organization's journey towards achieving a secure digital landscape. We automatically analyze an organization's risk exposure across thousands of unique data points, using trusted qualitative and quantitative risk assessment methodologies, providing holistic risk insights across the threat landscape.

Our Flagship Products:

» **CyberQ Shield**
Next Generation Cloud Security Platform

» **CyberQ ORO**
Next Generation Organisation Risk Orchestration

SecLogic's ability to tailor solutions across quadrants is strengthened through delivery of seamless support services built on the customer first foundation.


https://seclogic.io/


connect@seclogic.io


SecLogic INC


HQ: 4th Floor, 90 Canal St, Boston, MA 02114, United States