People Security Management
Strengthening the Weakest Link in Cybersecurity

ASSESS | AWARE | PROTECT | EMPOWER

www.threatcop.com
Threatcop is a pioneer in People Security Management (PSM), empowering your workforce as the vanguard of defense. With a track record serving 200+ global enterprises, we specialize in protecting organizations against evolving cyber threats, focusing on social engineering and email attacks.

Why People Security Management?

PEOPLE SECURITY MANAGEMENT
The Power of 360 Degree Cybersecurity Awareness & Protection

Phishing
Smishing
Vishing
Whatsapp Phishing
Ransomware

Compliance Regulation
Flagging Threat
Cyber Vigilance
Strengthening Workforce
Peace Of Mind

Attack Vectors
Process
Outcome
Quadral Approach to People Security and Securing Organizations

We assess the weakest links; raise awareness, provide robust protection; and empower employees to defend against cyber threats. Our exclusive AAPE Model safeguards your human assets by creating a culture of security awareness and equipping individuals with the knowledge, skills, and tools to actively participate in the defense against cyber threats.

To ensure that humans become the strongest defense between you and threats, we embrace the exclusive AAPE Framework.

<table>
<thead>
<tr>
<th>TSAT</th>
<th>TLMS</th>
<th>TDMARC</th>
<th>TPIR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Spear Security Awareness Training</td>
<td>Threat Learning Management System</td>
<td>Tactical Domain Message Authentication, Reporting, and Conformance (DMARC)</td>
<td>Threat Planning Incident Response (TPIR)</td>
</tr>
<tr>
<td>TSAT helps you assess the awareness level of your employees by running cyber attack simulations and evaluating their vulnerabilities.</td>
<td>TLMS helps you educate and train your employees about the latest threats through interactive quizzes, cyber comics, infographics, etc.</td>
<td>TDMARC helps you secure your domain and outbound email, ensuring domain reputation and email deliverability.</td>
<td>TPIR provides a one-tap methodology for threat reporting that not only evaluates employees cyber awareness but also prevents potential breaches.</td>
</tr>
</tbody>
</table>
Secure Your People with TSAT in 3 Easy Steps

1. Cyber Attack Simulation
2. Knowledge Imparting Sessions
3. Enhanced Assessment & Analysis

Benefits
- Eliminates employee negligence
- Reduces up to 90% cyber risks
- Makes employees cyber aware
- Creates cyber resilient work culture
Exclusive Features of TSAT

- AI Template Generation
- Unlimited Security Attack Simulations
- Employee Vulnerability Score
- Fully Customizable Campaigns
- Real-Time Dashboard
- Executive Simulation Report

Advantages of Choosing TSAT

- Comprehensive reporting inclusive of employee vulnerability score
- An affordable and scalable solution for organizations of all sizes
- Fully customizable phishing templates
- Latest attack vectors including WhatsApp phishing and smishing
- Real-time employees' vulnerability tracking

TSAT's Competence

- 2.3 Million People Assessed
- 40% to 5% Phish Risk Rate Reduced
- 150+ Enterprises Secured
- 700+ SMEs Safeguarded
Threatcop Learning Management System
Empower Your Employees as the Strongest Defense with TLMS

Interactive and Effective Cyber Awareness

Are you tired of boring cybersecurity training? Look no further than Threatcop’s Learning Management System! Our tool incorporates fun and creative content to help you stay aware of potential cyber risks and threats.

Shortfall in Employee Training Completion Rate

- *Infosec Institute*
  - 97% of employees globally cannot identify phishing emails and 25% of them end up clicking on it.

- In a cybersecurity breaches survey, only 20% of the 1500 respondents found that employees take cybersecurity training.

- *E&Y survey:* only 8% find provided cybersecurity awareness material sufficient.

Improve Training with Highly Engaging Content

1. Multiple Content Categories with Customization
2. Interactive Cybersecurity Awareness Sessions
3. Effective & Engaging Training

Benefits

- Improves Employees’ Training Completion Rate
- Offers employees a diverse content library
- Comprehensive User Analytics
- Improve Compliance & Standard Regulations
Exclusive Features of TLMS

- Co-Branding of Awareness Content
- Unlimited Reminder Scheduling
- Customized DIY Certification
- Auto Department Creation
- Team Progress Reports

Advantages of Choosing TLMS

- Multi-lingual, making it suitable for organizations with a global presence
- Includes 10+ cybersecurity awareness content categories
- Entertaining and interactive assessments, quizzes, and games
- Creates an environment of reinforcement and motivation

TLMS's Competence

- 1 Million+ People Trained Under PSM
- 1000+ Awareness Content in Library
- Upto 99% Engagement of Awareness Content
- 200+ Topics in 15+ Categories
**Email Authentication and Domain Security**

TDMARC is an anti-spoofing and email authentication solution that helps organizations secure their outbound email flow and prevent the misuse of their email domain while boosting email deliverability and engagement rates.

---

**Unsecured Domains Leads to Spoofing Attack**

- $1.8 billion adjusted losses due to BEC reported in 2020.  — FBI
- 3.1 billion emails are sent from spoofed domains every day.  — Forbes
- $12.5 billion is the annual cost of BEC attacks globally.  — FBI

---

**Secure Your Email Domain Against Spoofers**

- Spoofed emails + Legitimate Emails
- Filtering out of spoofed emails
- Legitimate emails safely landing in inbox

---

**Benefits**

- Spoofing attempt monitoring for domains
- Increased visibility of email marketing campaigns
- Effortless monitoring of multiple email domains
- Setting up BIMI record for better brand reputation
Advantages of Choosing TDMARC

- Anti-spoofing protection
- Enhanced email deliverability
- Boosts email engagement rates
- Safeguards brand reputation
- Access to email domain threat summary for any specified period
- Setting up BIMI record for better brand reputation

TDMARC’s Competence

- 2500+ Domains with SPF Implementation
- 3100+ Domains with DMARC Protection
- Over 95% Emails are DMARC Compliant
- 10+ BIMI Implemented for Brand Protection
Empower Your Employees in 4 Easy Steps

Benefits
- Evaluates security awareness training
- Reduces the risk of phishing
- Identifies email threats on time
- Avoids data breaches

Your People are Prime Targets of Email Phishing

- **2 million** malicious emails bypassed secure email defenses over 12 months in 2020.  
  [Helpnet Security](#)
- **14** malicious emails per year are received by a single employee on average.  
  [Forbes](#)
- **91%** of all cyber attacks begin with a phishing email.  
  [Deloitte](#)

Empower Your Employees in 4 Easy Steps

1. Click the TPIR button to analyze Email’s Threat-Level
2. Use the TPIR reporting button to report suspicious emails
3. The reported email is forwarded to the Security Team for further analysis
4. If the email is genuine, it comes back to the user’s inbox, otherwise, it is permanently deleted

TPIR is an email threat checker and a phishing incident response solution that empowers your employees to proactively detect and report suspicious emails, reducing the risk of email-based cyber threats.
**Exclusive Features of TPIR**

- **Header & Malware Analysis**
- **Suspicious Email Reporting System**
- **Email Alert to SOC Team for threat reports**
- **Sender Domain Reputation Check**
- **Advanced Attachment and URL/Link protection**
- **Keyword and Language-Based Mail Traffic Control**

**Advantages of Choosing TPIR**

- Transform your employees into strongest defense
- Header analysis and language-based mail traffic control
- Comprehensive sender reputation report
- Empower your employees to identify phishing attempts
- Helps your security team to prevent cyber attack

**TPIR’s Competence**

- **50,000+** People Empowered
- **2 Million** Emails Reported by Employees
- **20 Million+** IOCs Recorded in GCTx Database
- **2000+** Malicious IPs Blocked
AI-Powered Phishing Simulation: Stay Ahead of the Curve

"AI-generated phishing templates were 30% more likely to be successful than human-generated phishing templates. – University of Washington"

Hackers are upgrading their attack systems with the help of AI.
Let’s beat them with the intelligent and sophisticated use of AI.

AI Phishing Template Generation with TSAT

Step 1: Enter Your Prompt

Step 2: Mention Your URL

Step 3: Your Company Logo

AI Generated Phishing Template

We are pleased to inform you that you have been selected to receive an Amazon gift voucher worth $100 as a token of appreciation for your hard work and dedication.

This voucher can be used to purchase any item of your choice from the Amazon website.

Please note that this offer is valid for a limited time only, so we encourage you to redeem your voucher as soon as possible.

To claim your voucher, please click on the button below:

Claim Voucher

If you have any questions or need further assistance, please do not hesitate to contact our HR department.

Thank you once again for your hard work and dedication.

Best regards,

Your Company Name

© 2023 All rights reserved
WhatsApp Phishing: Rising Threat to Business and Employees

89.6% of detected malicious links were sent via WhatsApp. The largest number of malicious links were detected in Russia (56%), India (6%), and Turkey (4%). – The News Minute

WhatsApp is a new operational ground for hackers to target businesses. Employees must know how to safeguard their personal communications.

WhatsApp Phishing Simulation from Threatcop

Step 1: Create WhatsApp Campaign

Step 2: Create Template: Using AI
People-centric cybersecurity is becoming a major concern these days, being associated with Threatcop has really put our security concerns at ease. **TSAT**’s features and expertise is quite comforting and their post-sale support is impeccable.

*CISO, Pharma Company*

**TDMARC** was the most easy to use, with a good and knowledgeable team to guide in case of overwhelming data available out there regarding email security. We have had a very good experience with Threatcop solutions and services.

*CISO, Financial Services Company*

**TPIR** has been a great addition to our cybersecurity arsenal. In fact, it has helped our workforce realize the extent of their ignorance in dealing with social engineering threats and improve by working on it.

*CISO, Ed-Tech Industry*

---

### Recognitions and Ratings

![G2](#) 5/5

![crozdesk](#) 4.9/5

![Gartner Peer Insights](#) 5/5

![Top Performer Winter 2022](#)

![Quality Choice India 2022](#)

![IFSEC India](#)

![Happiest Users 2021](#)
Threatcop’s Industry-Wise Customers

- BFSI: 26.8%
- NBFC: 18.3%
- Consumer Internet: 15.5%
- Manufacturing: 9.9%
- Healthcare & Pharma: 9.9%
- IT Services: 9.9%
- Oil & Energy: 2.7%
- Others: 7%

Brands You Trust, Trust Us

- Airtel Payments Bank
- AngelOne
- NPCI
- Kotak Life
- Axis Bank
- Bharti AXA
- Ageas Federal Life Insurance
- Juspay
- Pine Labs
- KreditBee
About Us

In today’s cybersecurity landscape, where companies are putting all their resources into protecting their systems and IT infrastructure, Threatcop is focused on keeping your people safe against the evolving cyber threats. Cybercriminals leave no stone unturned to breach your organization by exploiting your people. We strive to make sure they fail! With the help of our 4 people-centric security solutions – TSAT, TLMS, TDMARC, and TPIR, we make your employees resilient against social engineering and email-based attacks, making your organization safer.

Get In Touch

LOCATIONS

UNITED STATES
400 W Peachtree St NW Atlanta, GA, 30308
(+1) 323 287 9435

INDIA
B–70, Block B, Sector 67, Noida, Uttar Pradesh 201301
+91 7428092413, +91 9717792410

Dubai, Abu Dhabi, Mumbai, Bangalore, Hyderabad, & Riyadh

FOR SALES
sales@threatcop.com

VISIT OUR WEBSITE
www.threatcop.com