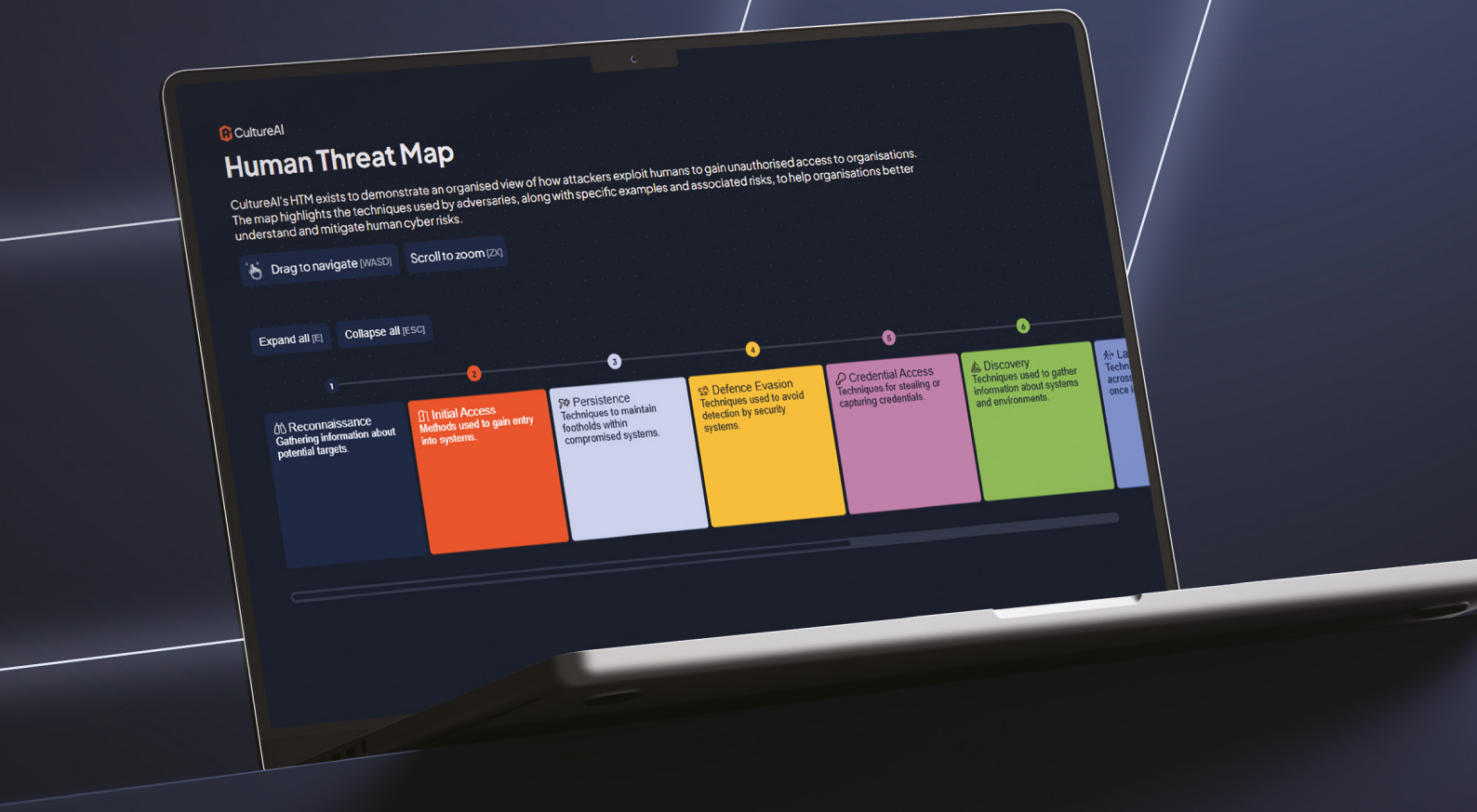
CultureAI



Whitepaper

New Risks, New Rules: Using HTM to Navigate the Modern Threat Landscape

A practical guide to understanding and mitigating human-centric cyber risks

The New Rules of Cyber Defence

It's 2025, and the cyber security playbook has changed.

Despite years of investment in security awareness training, human error continues to dominate as a root cause of security breaches.

The 2024 Verizon DBIR reports that **68% of breaches** involve human mistakes. Meanwhile, Crowdstrike's 2025 Global Threat Report reveals that **79% of attacks in 2024 were malware-free**, relying instead on credential theft, social engineering, and direct system manipulation.

As attackers evolve faster than users can adapt, the next phase in cyber defence must centre around understanding and managing human risk, not just teaching employees to spot threats. Particularly as emerging threats are almost always impossible for humans alone to spot.

This is where the Human Threat Map comes in.

The Evolution of Security Strategy

Era	Focus	Why it failed
1990s	Network Perimeter	Attackers shifted to user-focused entry points
2000s	Endpoints	Endpoint protection couldn't keep up with phishing
2010s	Identity	Credential theft outpaced awareness training
2020s	Users	AI-fuelled deception exceeds human capacity to detect

What is the Human Threat Map (HTM)?

The Human Threat Map, developed by CultureAI, is a comprehensive framework that allows security teams to:

Identify human-centric cyber threats

Understand the user behaviours that enable them

Proactively close security gaps with targeted human risk management strategies

Learn more about the HTM

The only constant? Humans.

Attackers will increasingly attempt to bypass network defences, endpoint protections, and even identity safeguards by going directly after the human element at the forefront of it all.

Understanding the Human Perimeter

As traditional perimeters crumble, people have become the new perimeter. Threat actors bypass firewalls and malware scanners by directly manipulating users.

These modern threats include:

- AI-powered phishing
- Deepfake voice/video scams
- SaaS tenant poisoning
- MFA fatigue (MFA bombing)

Security awareness alone isn't enough.

To truly defend the human perimeter, organisations must adopt **Human Risk Management (HRM)** — proactive, real-time strategy centred on behavioural data and context, not just awareness.

Threats can also be explored by domain (Phishing, SaaS, AI, Identity, etc.) to zero in on your specific environment or team.

Each threat tile expands to show:

- Threat overview and real-world examples
- Linked user behaviours and risk signals
- Research references and intervention ideas

How the HTM Works

The HTM is inspired by frameworks like MITRE ATT&CK and is structured around familiar threat lifecycle stages:

1. **Reconnaissance**
   Techniques used for gathering information about potential targets.
2. **Initial Access**
   Techniques used for gaining initial entry into target systems.
3. **Persistence**
   Techniques used for maintaining a foothold within compromised systems.
4. **Defence Evasion**
   Techniques used for avoiding or undermining detection by security systems.
5. **Credential Access**
   Techniques used for stealing or capturing user or system credentials.
6. **Discovery**
   Techniques used for gathering information about additional systems and environments.
7. **Lateral Movement**
   Techniques used for moving between systems and networks.
8. **Collection**
   Techniques used for gathering and exfiltrating data from compromised systems and accounts.
9. **Impact**
   Techniques used to cause damage or disruption to compromised systems, users, and data.

A Practical Example – From Breach to Defence

Let's walk through a realistic breach scenario to demonstrate how HTM works in practice.

The Attack:

1. **OSINT** on employees via social media.
2. **SaaS Tenant Poisoning** – sending legitimate invites via fake SaaS tenant.
3. **SAMLJacking** used to harvest credentials.
4. **MFA** Fatigue tricked the user into granting access.
5. **Data exfiltration** from Slack and email.

Step-by-Step HTM Application:

Step 1: Identify Threats

Map each attack stage to HTM categories:

- SaaS Poisoning → Initial Access
- MFA Bombing → Defence Evasion
- Slack Scraping → Collection

Step 2: Understand Behavioural Risks

HTM reveals that the poisoned tenant attack is enabled by:

- Users joining unverified SaaS tenants
- Low scrutiny during onboarding

Step 3: Determine Security Gaps

The HTM allows you to view threats across categories and domains such as identity, phishing, AI, SaaS platforms, and endpoint usage.

For each category, consider:

- Where do we already have strong controls in place?
- Where are controls outdated, reactive, or overly reliant on user action?
- Which threats are increasing in frequency but not yet being addressed?

Step 4: Deploy Interventions

Use HRM tools like CultureAI to build automated interventions that fix, nudge, adapt, coach and block human cyber risks.

Implementing HTM in Your Organisation

The HTM is a powerful tool to help organisations identify, understand, and mitigate human-centric cyber threats. But to be effective, it must be embedded into your daily operations, linked to real behavioural data, and used to guide ongoing human risk strategies.

Here's how to operationalise HTM in a way that benefits your long term security strategy:

Step 1: Audit and Assess Your Human Risk Landscape

Before deploying the HTM, start with a clear picture of where your organisation stands today. This initial audit is the foundation for effective use of the framework.

- **Conduct a human risk assessment:**
  Review previous security incidents, near-misses, and common user behaviours that may contribute to risk.
- **Map existing controls to HTM categories:**
  Use the HTM to compare your current controls against known threat behaviours.

Step 2: Identify and Classify Threats Using HTM

Now that you've assessed your environment, begin using the HTM to categorise potential threats by mapping attacker actions to specific stages and behaviours.

- **Map incidents to the HTM attack lifecycle:**
  Align observed threats to HTM categories. For example:
  - **SaaS Poisoning →** Initial Access
  - **MFA Bombing →** Defence Evasiono
  - **Slack Scraping →** Collection

This exercise will help you visualise where human behaviours intersect with known attack tactics, and where defences need to be strengthened.

Step 3: Profile Risky Behaviours

With the HTM in hand, start linking specific risks to human actions and behaviours. This is about getting more precise—pinpointing who is at risk and why.

- **Classify the risky behaviours that matter most to your organisation:**
  Use the HTM to identify the behaviours most relevant to your organisation, such as:
  - Ignoring MFA prompts
  - Reusing passwords
  - Sharing data in unauthorised AI tools
  - Downloading unverified attachments
  - Poor onboarding or offboarding processes

This classification allows for a targeted, behaviour-specific risk mitigation approach.

Step 4: Identify Security Gaps and Prioritise Controls

Now that you know which behaviours present risk, assess your controls through the lens of the HTM.

- **Cross-reference behaviours and controls:**
  Are your existing tools and policies sufficient to address the specific behaviours you've identified? Where do controls rely too heavily on user judgment or manual enforcement? Which areas are you currently struggling to surface data on?
- **Focus on specific gaps:**
  HTM spans identity, phishing, AI usage, endpoint hygiene, SaaS, and more. Use it to prioritise controls where risks are most urgent or growing fastest.

Step 5: Introduce Interventions

Here's where the HTM becomes operational. With behaviours and gaps identified, now you can implement dynamic interventions through your chosen HRM platform

- **Build automated intervention playbooks tailored to risk type and user context. Categories might include:**
  - **Fix:** Automatically undo risky actions (e.g. removing sensitive data from public channels)
  - **Nudge:** Real-time prompts that guide better choices (e.g. alerting users before joining unverified SaaS tenants)
  - **Adapt:** Adjust policies dynamically based on user behaviour (e.g. restrict sharing after repeated risky actions)
  - **Coach:** Provide just-in-time education to prevent errors (e.g. password guidance when a weak one is detected)
  - **Block:** Stop high-risk actions outright (e.g. prevent uploads to unauthorised AI platforms)

Interventions make the HTM actionable—transforming insights into direct outcomes.

Step 6: Evolve Continuously

Human risk is dynamic—new threats, behaviours, and vulnerabilities emerge constantly. Your defences must evolve just as quickly.

The HTM is designed to adapt over time, incorporating the latest intelligence on emerging human-centric threats. When paired with a robust HRM platform, it enables your organisation to stay proactive rather than reactive.

By continuously leveraging HTM insights and behavioural data, your organisation can:

- **Surface risks in real-time:** Detect risky actions as they occur—such as unapproved app usage, unusual login patterns, or sensitive data sharing and act immediately.
- **Gain deeper insights into human risk:** Understand where risk is concentrated, which behaviours are most problematic, and which teams or roles require additional risk management.
- **Continuously refine intervention strategies:** Use behavioural data to adjust intervention playbooks. Improve approach and tactics to increase impact and risk reduction rates.
- **Drive measurable risk reduction:** Over time, reduce the frequency and severity of human-driven incidents through targeted interventions, without overwhelming SOC teams.

Conclusion: Securing the Human Perimeter

We cannot train our way out of modern cyber threats.

Awareness training is no longer the frontline —behaviour-driven human risk strategy is.

The Human Threat Map provides a modern, actionable way to:

- Go beyond theory into practical, real-time human risk management
- Understand and mitigate human cyber risk at scale
- Keep ahead with ever-evolving attacker tactics

Security is no longer the employee's responsibility — it's ours.

Learn more about the Human Threat Map and CultureAI today.

See the Human Threat Map

Learn about CultureAI