satius.io

Satius Security Continuous Threat Exposure Management as a Service

Enhancing your organization's cybersecurity posture through a comprehensive, adaptable, and validated security program.

NOVEMBER 19TH, 2024

SMBs

Why CTEM Matters

The Value Proposition

REGULATORY ALIGNMENT

Maintaining a proactive and continuous compliance approach alleviates operational burdens by adhering to strict data protection and security mandates year-round, as ensured by out CTEM as a Service.

REPUTATION PROTECTION

A data breach or cyberattack can severely damage trust and credibility, impacting customer loyalty and market perception.

DATA PROTECTION

Secure critical information through a comprehensive program that swiftly identifies and addresses potential threats, minimizing vulnerability windows.

PROACTIVE DEFENSE

Proactive cyber resilience reduces vulnerabilities, lowers insurance premiums, and supports long-term strategic planning against emerging threats.

SMBs

Why CTEM Matters

Bridge The Gap between IT and Executive Management

TRANSLATE TECHNICAL RISKS INTO BUSINESS IMPACT

- ✔ Executive-Friendly Reporting.
- ✔ Prioritization of Risks

ALIGN IT ACTIVITIES WITH BUSINESS GOALS

- ✔ Compliance Readiness.
- ✔ Strategic Investment.

FOSTER COLLABORATION AND COMMUNICATION

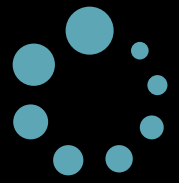
- ✔ Unified Language.
- ✔ Cross-Functional Insights.

DEMONSTRATE ROI AND BUILD TRUST

- ✔ Prove Value of Security Initiatives.
- ✔ Focus on Outcomes

Challenges In Maintaining Compliance

Adopt a Proactive, Continuous Approach to Strengthen Security and Simplify the Compliance Lifecycle



EVOLUTION OF THREATS AND COMPLIANCE

This makes it challenging for organizations to keep up with both. Constantly changing technology environments and the complexity of managing multiple security controls further complicate efforts to maintain compliance.

RESOURCES CONSTRAINTS

SMBs, in particular, may face resource constraints that make it difficult to perform regular assessments, update policies, or address new vulnerabilities as they emerge.

NO ORGANIZATION CAN PROTECT AGAINST EVERY CYBERSECURITY EVENT. INSTEAD, COMMIT TO TACKLING EXPOSURES THAT MOST THREATEN YOUR BUSINESS.

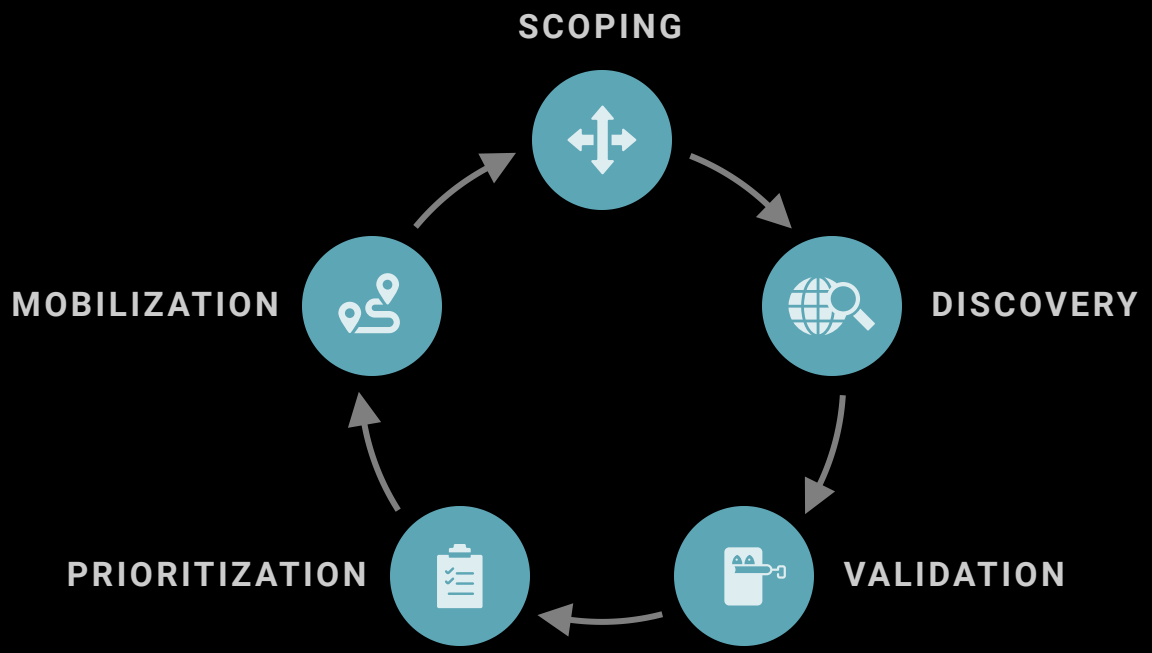
How to Manage Cybersecurity Threats, Not Episodes

By 2026, organizations that prioritize their security investments based on a continuous exposure management program will be 3x less likely to suffer a breach.

GARTNER, 2023

What is Continuous Threat Exposure Management (CTEM)?

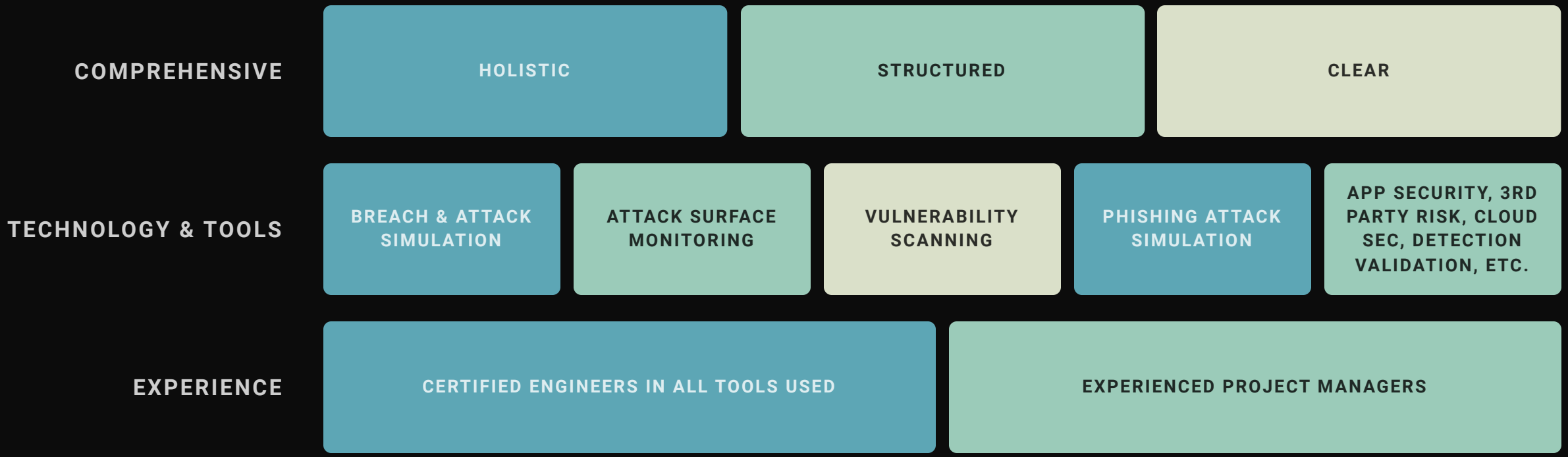
The Framework



- **SCOPING**
  Identifying an initial scope of the attack surface with a plan to extend it as the program advances.
- **DISCOVERY**
  Discover assets and their risk profile, identifying security gaps including misconfiguration of security controls and vulnerabilities.
- **VALIDATION**
  Assessing the likelihood of attack success, analyzing all potential attack paths, and verifying the effectiveness of the detection, response, and remediation processes.
- **PRIORITIZATION**
  Prioritizing identified gaps and remediation efforts covering the asset's business criticality, likelihood of the asset's being exploited, and availability of compensating security controls.
- **MOBILIZATION**
  Ensuring the teams almost frictionlessly operationalize the CTEM findings.

Why Satius Security's CTEM as a Service?

Operationalizing The Framework requires:



CTEM as a Service

How Satius Operationalizes CTEM?

Satius's CTEM Functions

UNIFIED THREAT EXPOSURE INSIGHT

Provides a consolidated view of the organization's security posture with visualizations like risk heat maps, scorecards, and trend analysis graphs. Aggregates data across risk categories to give stakeholders a high-level, actionable perspective on security gaps and improvements.

RISK CATEGORIES

Scores are based on specific categories, such as Security Controls Validation and Attack Surface Monitoring. Each category has its own assessment modules, which provide granular insights into areas like endpoint security, network defenses, and third-party risk.

DRIVING IMPROVEMENT

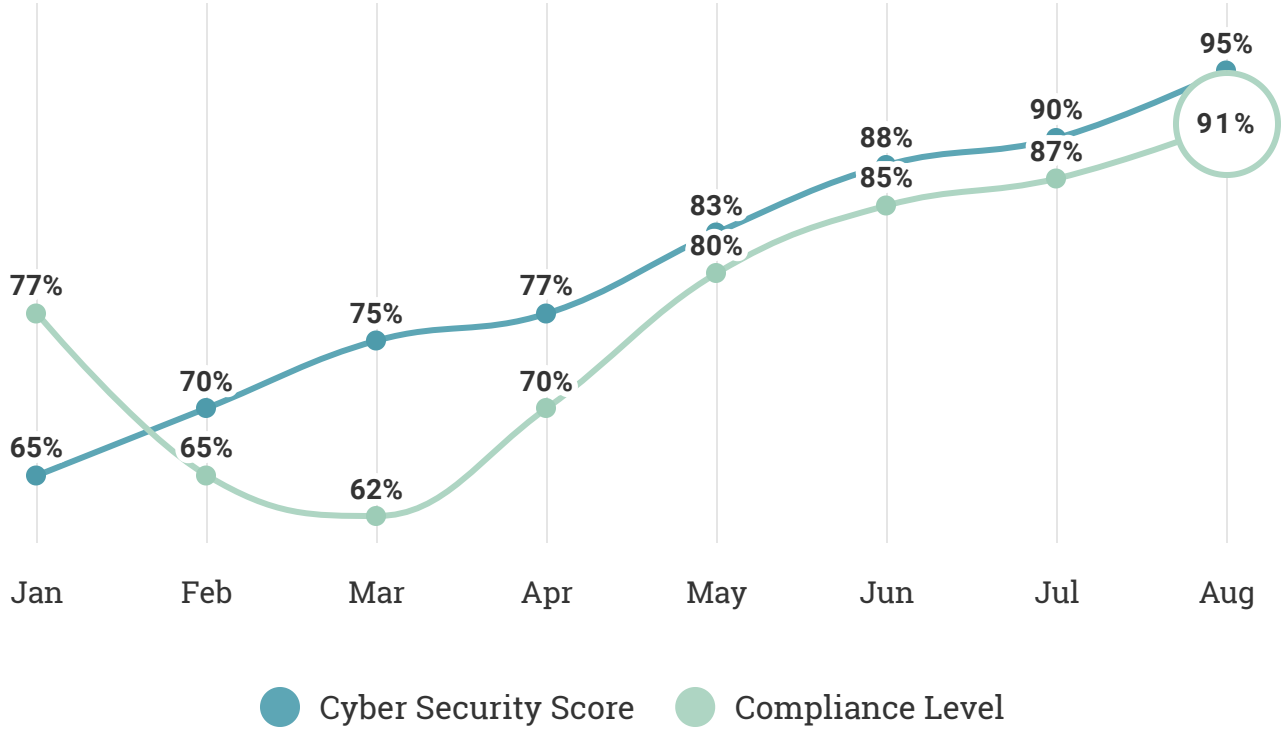
We follow Gartner's CTEM phases from the initial discovery to the mobilization of efforts to close gaps and enhance security posture. even though the phases are clear in order, they are not sequential in the sense of the overall program. We continuously perform each phases

CTEM OPERATIONALIZED

Unified Threat Exposure Insight

Comprehensive Cyber Security Posture Score

Threat Exposure Management Quantified



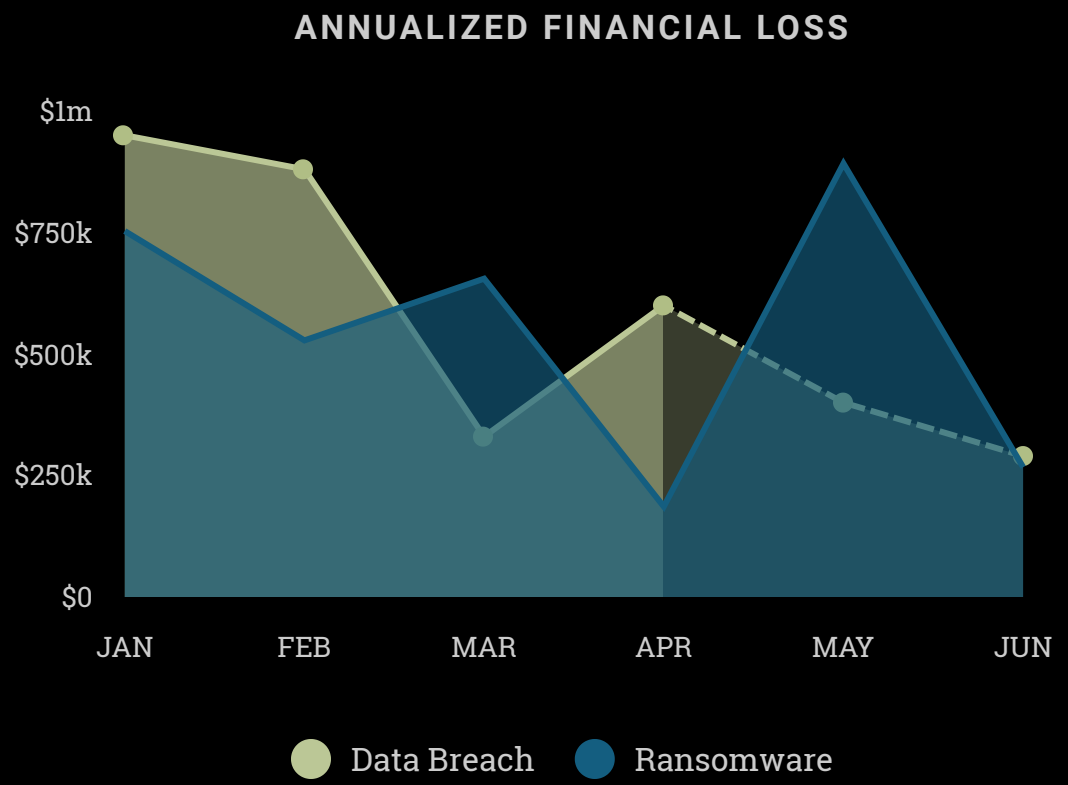
+5%

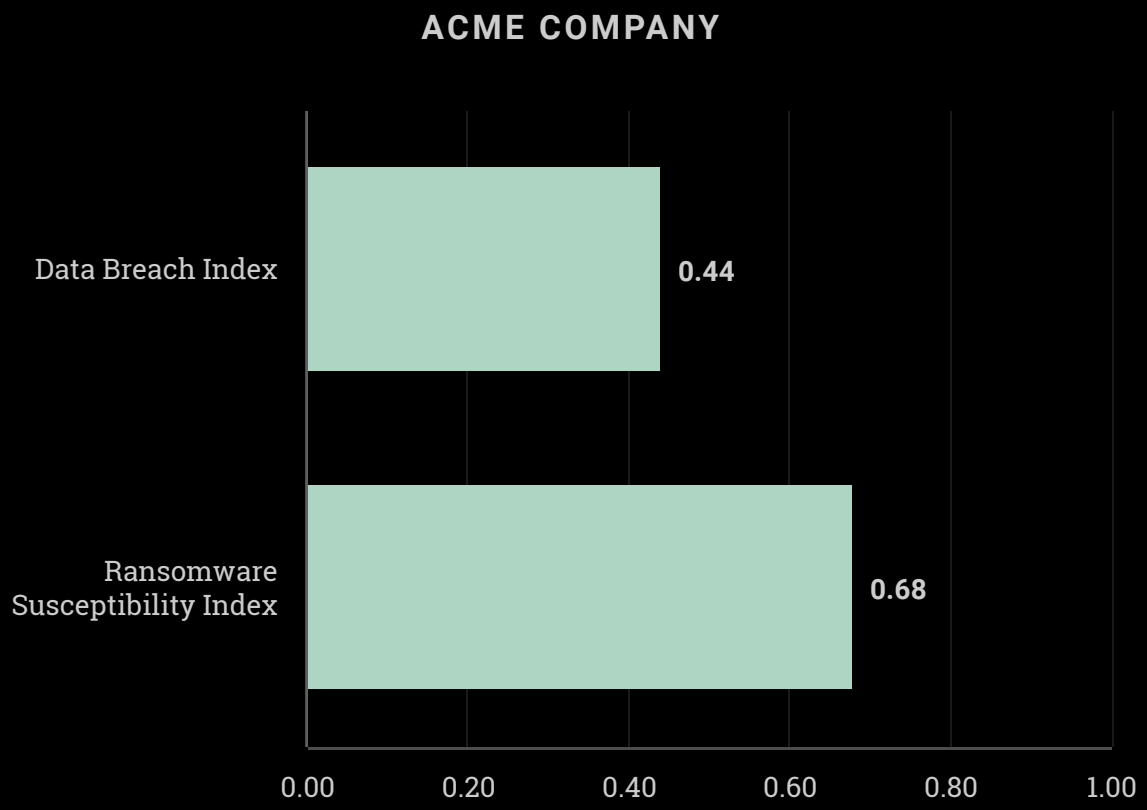
AUGUST OVER JUNE

The Unified Threat Exposure Insight consolidates the organization's security posture into a single, comprehensive view. We utilize powerful visualizations, such as risk heat maps, scorecards, and trend analysis graphs, to provide stakeholders with a clear and actionable understanding of the overall cybersecurity risk landscape.

Annualized Breach, Ransomware, and Reputation Loss

Threat Exposure Management Quantified





Unified Threat Exposure Insight

Understand your Security Posture

The road to cyber resilience begins with a quantifiable and clear measure of your security posture.

Finally executive management can get the answers they've been looking for. With a clear actionable insight, they can be a positive force behind implementing and aligning strategy with business.

OVERALL CYBER SECURITY SCORE

85% ▲ 10%

PCI COMPLIANCE

79% ▼ 8%

ANNUALIZED RANSOMWARE LOSSES

250k

SOCIAL ENGINEERING SCORE

90%

THREAT PREVENTION SCORE

76% ▼ 15%

ACTIVE CRITIAL FINDINGS

34

CTEM OPERATIONALIZED

Security Risk Categories

Risk Categories

Categorized Modules to assess threat exposure

SECURITY CONTROLS	ENDPOINT CONTROLS VALIDATION	NETWORK CONTROLS VALIDATION	WEB APPLICATION CONTROLS VALIDATION	
ATTACK SURFACE	REPUTATION	RESILIANCE	PRIVACY	SECURITY
SOCIAL ENGINEERING	PHISHING ATTACK SIMULATION	RISK BASED CAMPAIGNS		
SYSTEMS VULNERABILITIES	PUBLIC IPS SCANNING	NETWORK SCANNING	INFRASTRUCTURE SCANNING	
COMPLIANCE	PCI DSS	HIPPA	NIST	CMMC	ISO 27001	ETC.

RISK CATEGORIES | STANDARD MODULES

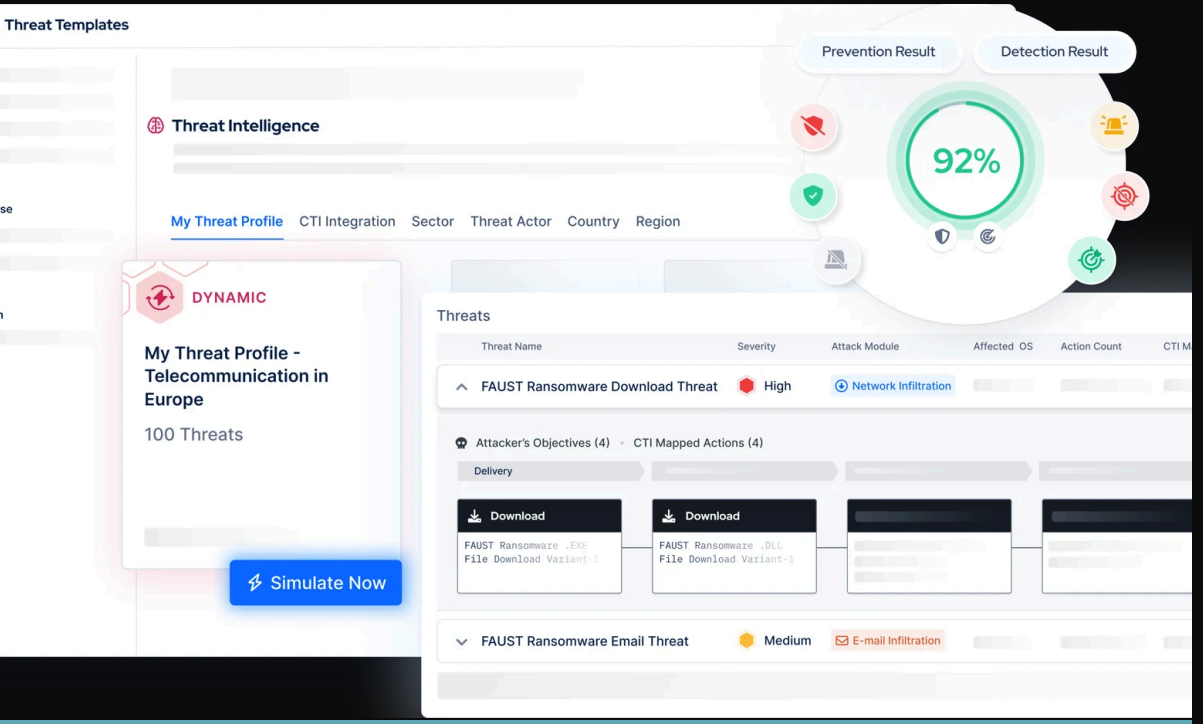
Security Controls

Gain Confidence in Your Security Controls

Only 22% of organizations are highly confident that their security controls work as they are supposed to.

PONEMON INSTITUTE

The dynamic nature of cyber threats and constant changes within IT landscapes necessitate regular review and refinement of security control configurations. Out-of-the-box deployments of firewalls, SIEM, and EDR tools require ongoing tuning to maintain effectiveness. Security control validation enables the identification of policy gaps impacting control efficiency and provides actionable mitigations to optimize these controls swiftly and effortlessly.



- ENDPOINT ATTACK SIMULATION
- NETWORK INFILTRATION ATTACK SIMULATION
- EMAIL INFILTRATION SIMULATION
- WEB APPLICATION ATTACK SIMULATION

CTEM as a Service

Security Controls Validation

How Satius Helps

Prove controls are working up to expectations

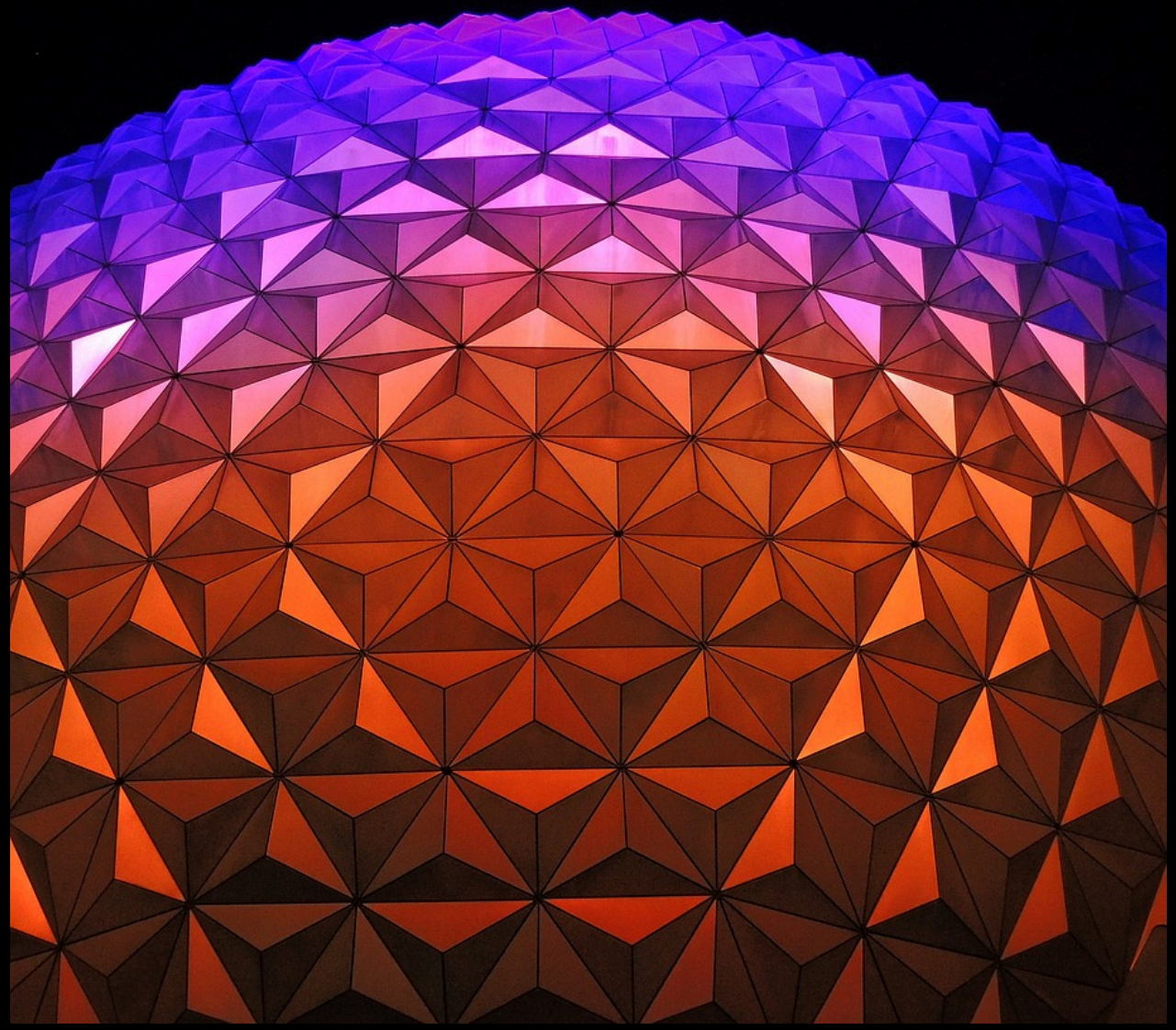
Measure readiness to prevent and detect threats.

Quickly respond to changes in the threat landscape.

Get the best ROI from your investments.

RISK CATEGORIES | STANDARD MODULES

Attack Surface



CTEM as a Service

Attack Surface Management

Continuously monitors your ever-changing cyber-ecosystem so you can

- IMPROVE BUSINESS RESILIENCE
- QUANTIFY AND COMMUNICATE CYBER RISK TO YOUR EXECUTIVE STAKEHOLDERS
- SHORTEN PROCUREMENT TIMES
- UNDERSTAND A THIRD-PARTY'S REGULATION COMPLIANCE*
- RESPOND TO HIGH-PROFILE CYBER EVENTS
- CHANCES OF RANSOMWARE ATTACK ON AN ORGANIZATION

Risk Categories

Attack Surface Monitoring

Over 20 Technical Modules

Digital Footprint

DNS Health

Email Security

SSL/TLS STRENGTH

DDOS RESILIENCY

NETWORK SECURITY

FRAUDULENT DOMAIN

FRAUDULENT APPS

CREDENTIAL MGMNT.

IP REPUTAITON

HACKTIVIST SHARES

SOCIAL NETWORK

ATTACK SURFACE

BRAND MONITORING

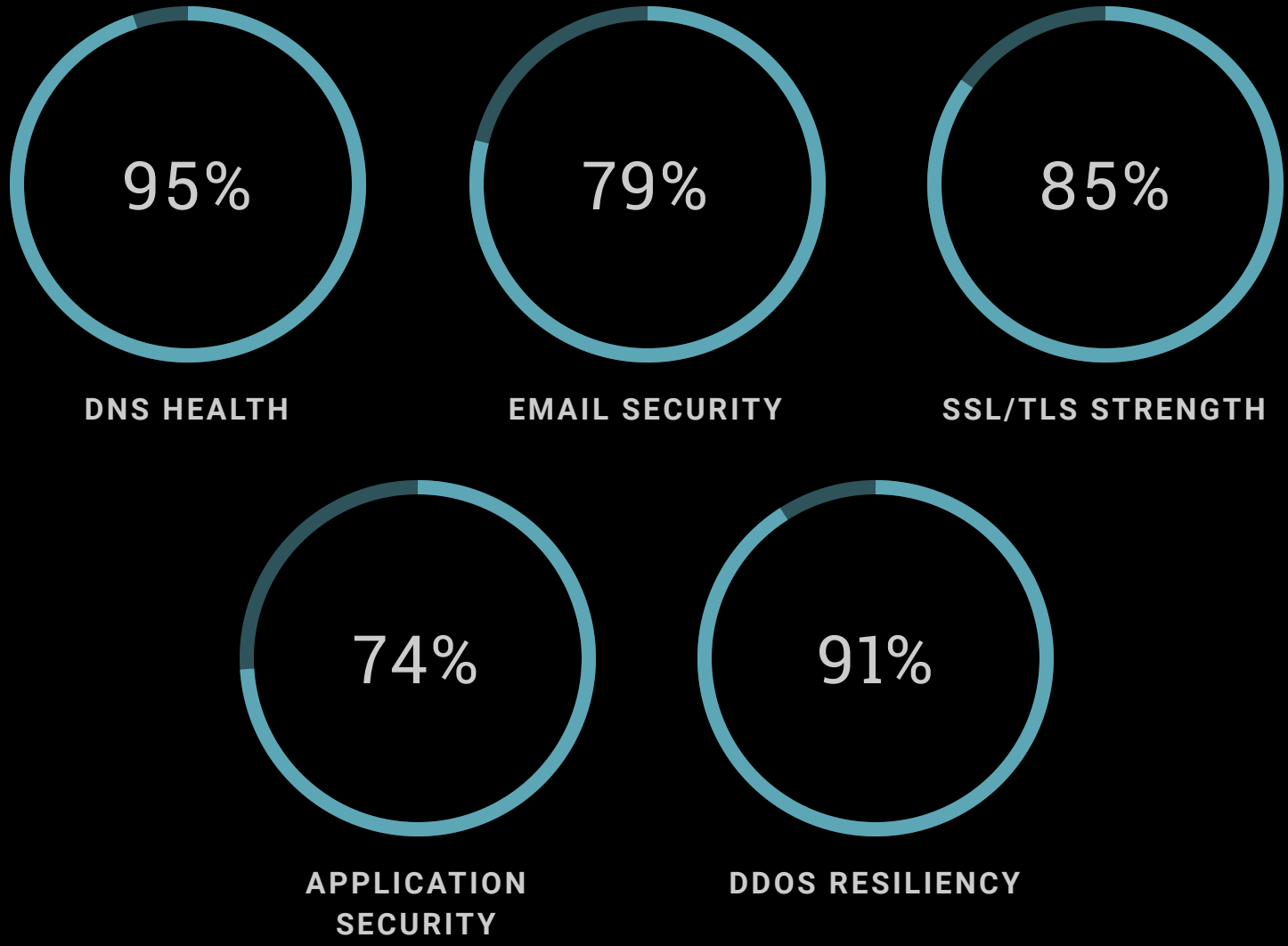
PATCH MANAGEMENT

WEB RANKING

INFORMAITON DISCLOSURE

CDN SECURITY

WEBSITE SECURITY



CTEM Risk Categories

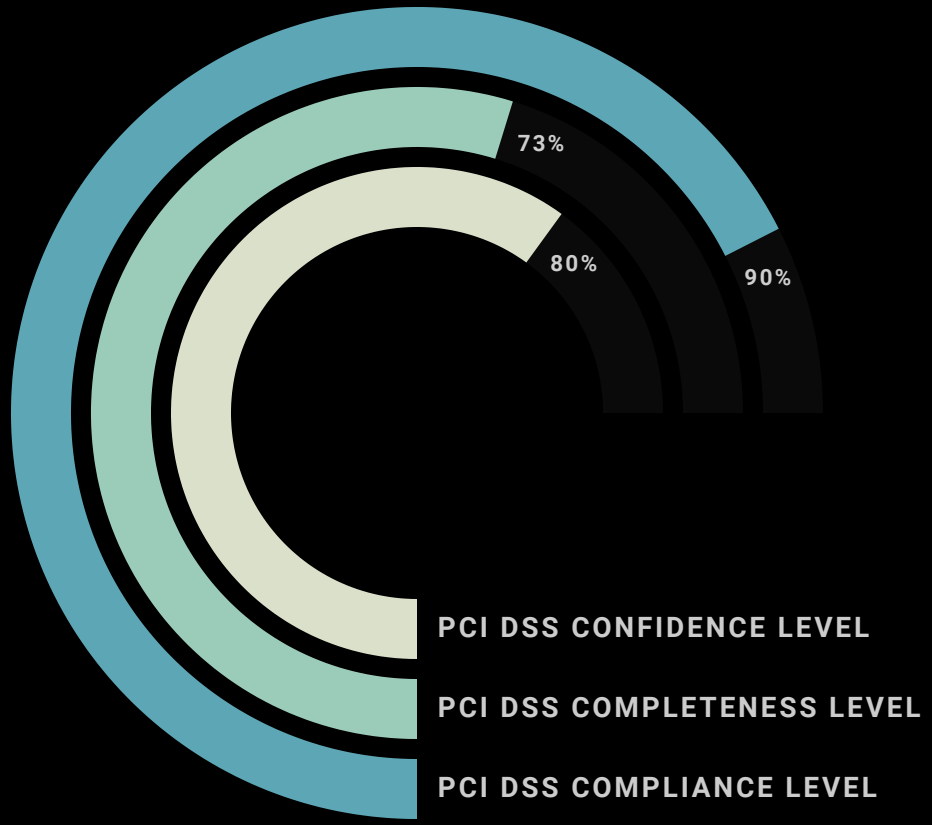
Attack Surface Monitoring

Over 15 Regulatory Standards

MAP COMPLIANCE WITH EXTERNALLY EXPOSED CONTROLS.

Parse Policies and assessments to improve "Confidence and Completeness" levels

Manually update Compliance Domains/Items to enhance score



Supported Standards

PCI DSS

HIPPA

GDPR

ISO 27001

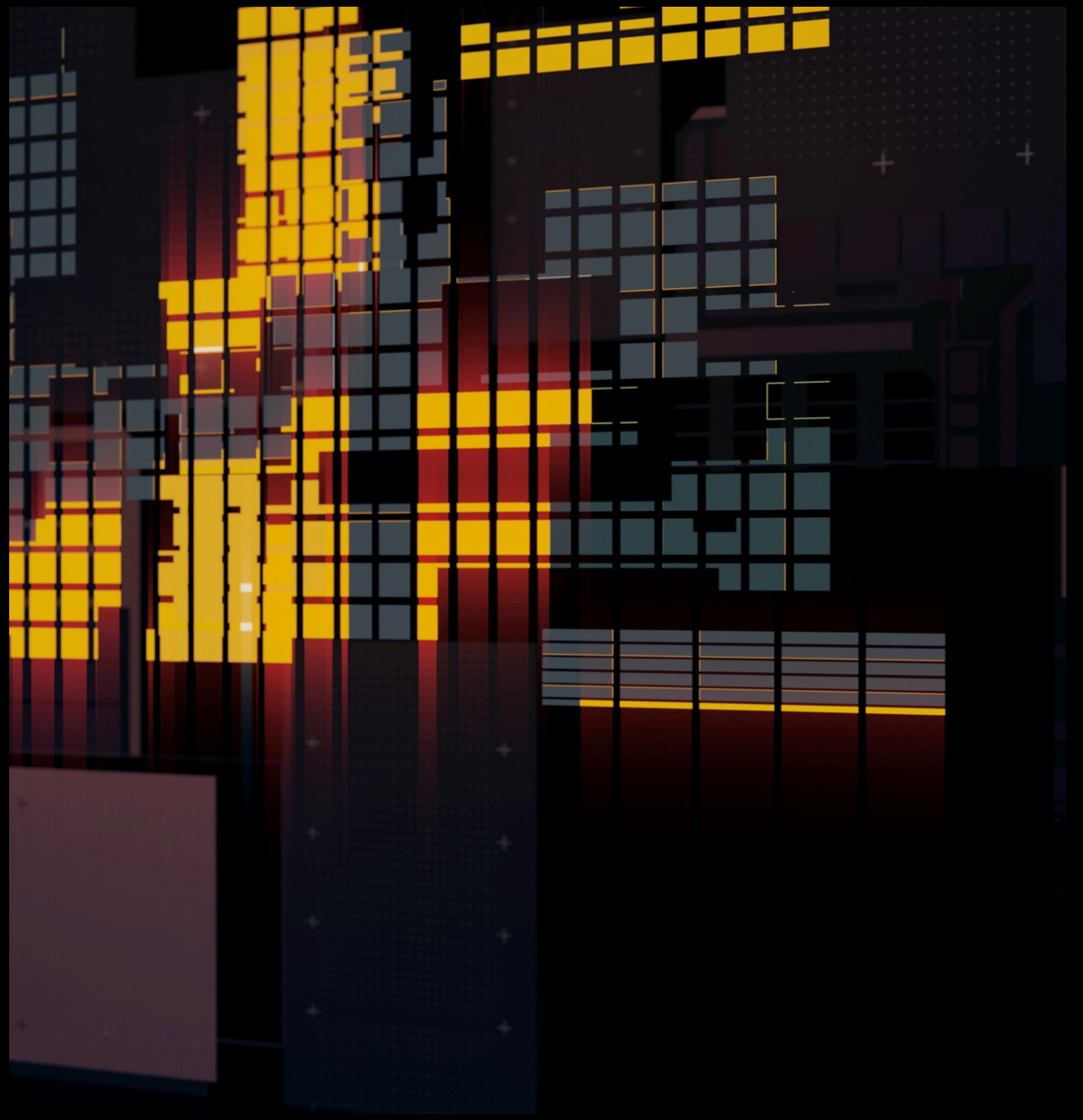
CMMC

NIST 800-53

Custom Standard

RISK CATEGORIES | STANDARD MODULES

Vulnerability Management



CTEM as a Service

Strengthening Security Posture Through Proactive Vulnerability Scanning

The Critical Role of Network and Infrastructure Scanning in Reducing Risks and Enhancing Defenses

SUPPORT FOR CONTINUOUS THREAT EXPOSURE MANAGEMENT

Aligns with CTEM strategies by ensuring that security controls are validated and up-to-date.

PROACTIVE RISK IDENTIFICATION

Detects weaknesses in network devices, servers, and infrastructure before attackers can exploit them.

REGULATORY COMPLIANCE

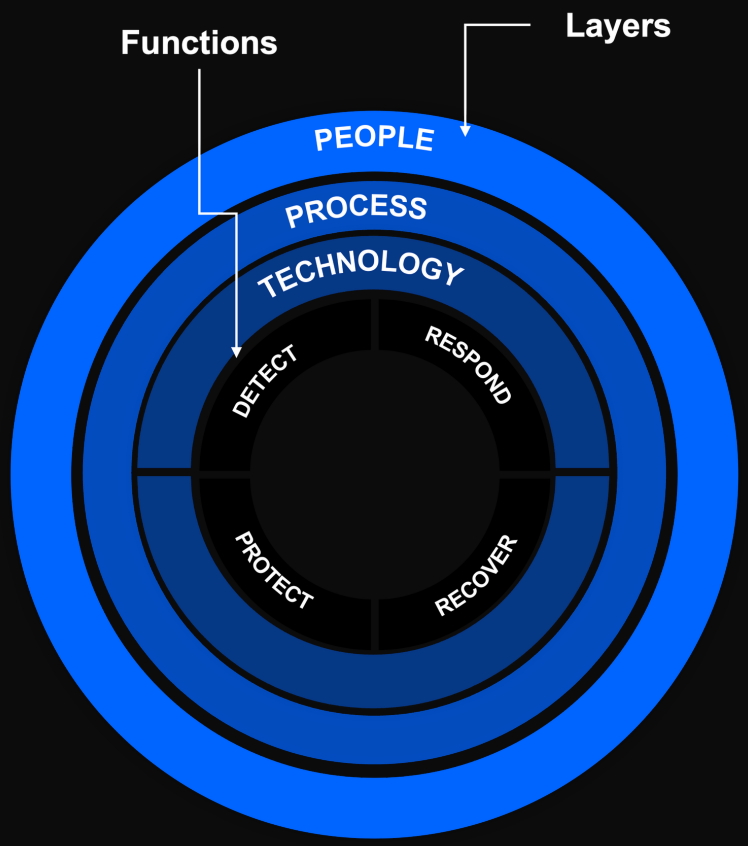
Ensures adherence to industry standards and regulations by identifying non-compliant components in the IT environment.

MINIMIZED ATTACK SURFACE

Reduces potential entry points for attackers by addressing exposed and misconfigured systems.

RISK CATEGORIES | STANDARD MODULES

Social Engineering



CTEM as a Service

Strengthening Security Posture Through Phishing Attack Simulations

Building Awareness, Resilience, and Proactive Defense Against Social Engineering Threats

RISK REDUCTION

Reduces the likelihood of successful phishing attacks by training employees to respond appropriately to suspicious emails.

SUPPORT FOR CONTINUOUS THREAT EXPOSURE MANAGEMENT

Ensures phishing-specific risks are addressed as part of a broader security strategy.

COMPLIANCE AND REPORTING

Demonstrates proactive measures to meet regulatory and industry standards requiring cybersecurity awareness training.

REALISTIC THREAT ASSESSMENT

Provides insights into how employees might react during actual phishing attacks, helping to fine-tune incident response plans.

Risks Based Campaigns

Users' roles

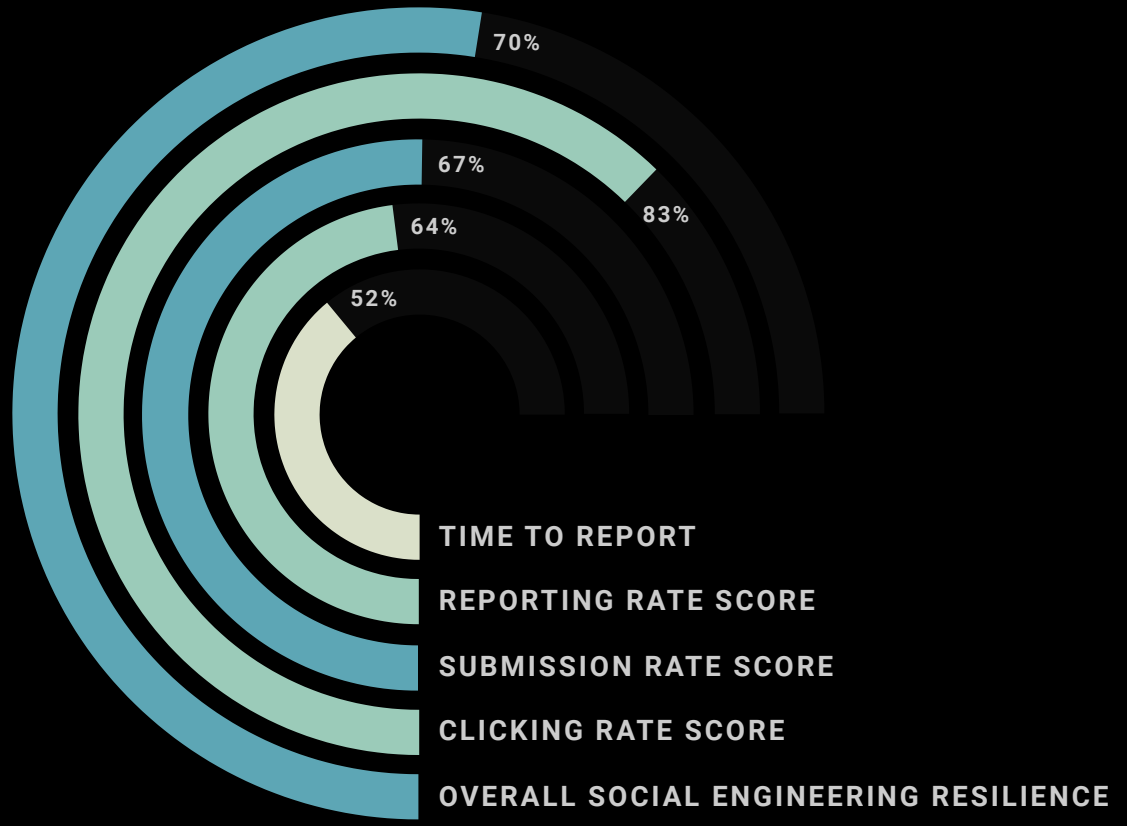
Leaked Credentials

Leaked Emails from social media

CTEM Risk Categories

Social Engineering

Fully understand employees' performance after each campaign



RISK CATEGORIES | ADD-ONS

Close The Gaps

CTEM Risk Categories

Add-On Categories/Modules

Adaptive solution to fit your environment and budget

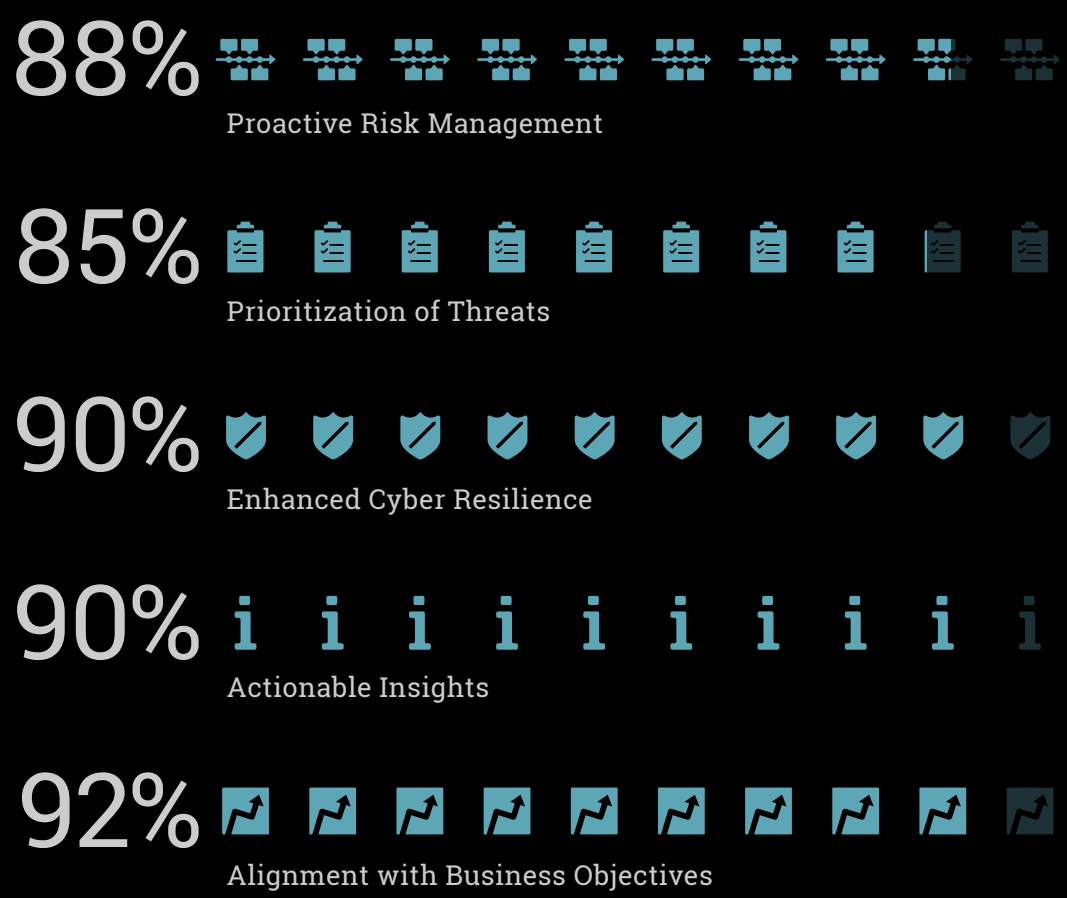
SECURITY CONTROLS	ENDPOINT DETECTION VALIDATION	NETWORK DETECTION VALIDATION	CLOUD ATTACK SIMULATION	CLOUD SEC AUDIT	SIEM RULES VALIDATION
APPLICATION SECURITY	SOURCE CODE	API	RUNTIME VULNERABILITIES		
3RD PARTY RISK	COMPLIANCE LEVEL	CYBER RATING	COMPLIANCE CORRELATION	FINANCIAL RISK	
RISK ASSESSMENT	WEB APP PEN TESTING	MOBILE APP PEN TESTING	NETWORK PEN TESTING	RED TEAMING	

CTEM OPERATIONALIZED

Driving Improvement

Continuous Threat Exposure Management (CTEM) Benefits

Comparison of Security Posture Metrics Before and After CTEM Implementation (0-100% Scale)



CTEM AS A SERVICE

Next Step

Contact Us for a Presentation

5112 Preston Pkwy, Perrysburg, OH

419-601-8694

info@satius.io