satius.io

A CISO's Guide to Reporting Cyber Risk to the Board

This ebook delves into the challenges of communication and offers strategies to report to the Board with confidence and precision

The cybersecurity stakes have dramatically increased for modern organizations

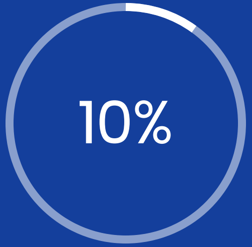
To report cybersecurity risk to the board effectively, it is crucial to present the information in a manner that is easily quantifiable and comprehensible to all stakeholders. Avoid technical jargon and focus on translating the potential impact of vulnerabilities, such as XYZ, into business-centric terms.

Demonstrate how improvements or setbacks over time directly influence the organization's bottom line and key performance indicators. By correlating cybersecurity posture with tangible business drivers, you can bridge the communication gap between your role as the CISO and the board's need for actionable, risk-based insights. This approach ensures that the board understands the cybersecurity landscape, enabling them to make informed decisions that optimize outcomes and mitigate unnecessary risk.

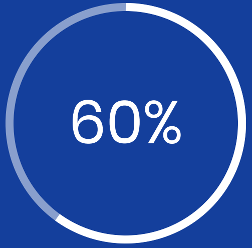
Cyber Risk Reporting: Often Incomplete, Seldom Executed Properly

Despite your clear understanding of the organization's cybersecurity risks, structural obstacles often impede the delivery of your invaluable insights to the critical decision-makers who require them.

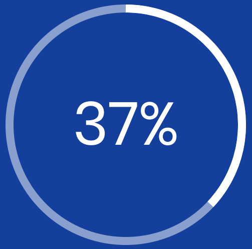
According to Heidrick and Struggles, leading executive consulting services, only 5% of CISOs report directly to the CEO, indicating a potential lack of high-level influence, and 2 ⁄3‘s of CISOs are two levels down from the CEO in the reporting structure.



According to Gartner, ONLY 10% of boards have a dedicated cybersecurity committee overseen by a board member, though that number is expected to quadruple in just 5 years.



Among that 60% of CISOs reporting to CEOs, nearly half report such briefings occur exclusively in the wake of a newly discovered security problem.

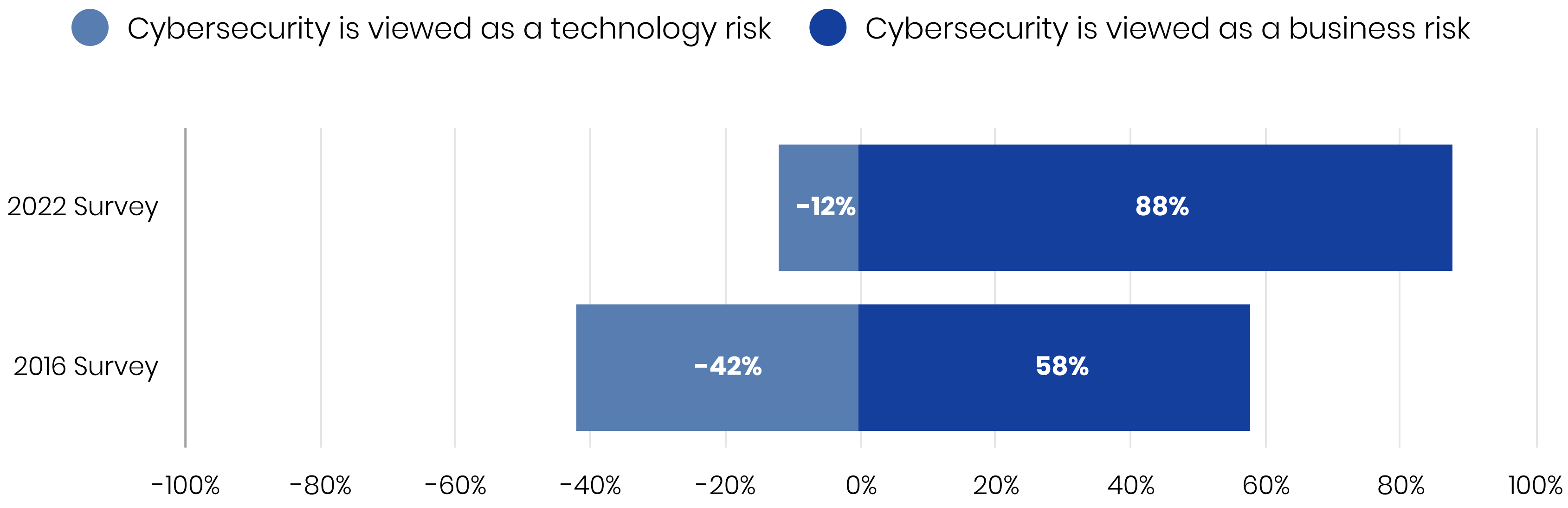


The majority of cybersecurity leaders report being at least three steps away from the CEO in the reporting structure, while only 37% report that their organization effectively leverages their expertise.

The proportion of board-level executives perceiving cybersecurity as a direct business concern has increased substantially

Climbing from 58% to 88% over the span of six years.

Corporate reporting structures and boardroom procedures harbor grave deficiencies. Despite the CISO's growing involvement, effectively conveying business risks remains a persistent challenge.



Gartner View from the Board of Directors' Survey

Transforming cybersecurity's image from a cost burden to a business-driving asset is vital for CISOs. Yet, this challenge demands a clear, intuitive presentation of security investments' returns.

Quantifying risks must accurately reflect the true stakes involved.

The Challenges of Reporting

4 Key Challenges Organizations Face When Reporting Risk to the Board

As a CISO, effectively communicating technical risks to a non-technical leadership demands clear, measurable metrics. These data points directly influence critical decisions on budget, resources, and the organization's overall security stance.

The ability to quantify the risk of breach to businesscritical assets across on-premises and cloud environments through a single pane of glass.

1

Identifying the risk of potential M&As and the steps necessary to mitigate them.

2

The path of least cost for maximum impact on the organization’s security posture and where to focus remediation efforts to get there.

3

The impact of security investments to security posture over time.

4

The Metrics That Matter

Current CISO reporting falls short in addressing these challenges

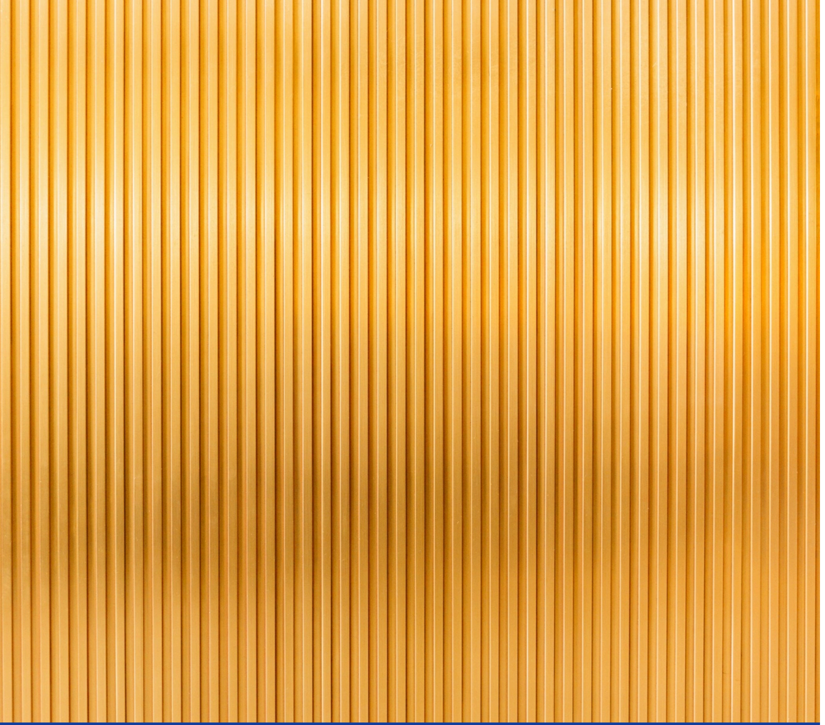
$$RISK = LIKELIHOOD \times IMPACT$$

THE RISK EQUATION

The potential for a successful cyberattack and its financial consequences to the organization represent the critical factors that define and quantify organizational risk

Threat Likelihood: A Tangled Web of Ambiguity and Uncertainty

Quantifying likelihood can be achieved through various means. Analyzing historical statistical data offers insights, yet it overlooks the unique context of an organization, including its specific threat landscape, evolving environmental factors, and critical business assets. As a CISO, conveying a comprehensive, context-driven assessment of risk is essential. Without a nuanced understanding of these elements, answering crucial questions like "Are we secure?" or "Are we improving?" becomes a challenge.



Rethinking Risk Reporting: Exploring Alternative Approaches

Understanding the risks to critical business assets and contextualizing them across the organization is crucial for boards. Visibility into the ramifications and the efficacy of risk reduction efforts is essential. Stakeholders' willingness to defend cybersecurity investments during incidents demonstrates the importance boards place on this domain.

As a CISO, it is crucial to present the business value of any security investment and establish metrics that define specific, mutually agreed-upon protection levels. When reporting on risk, the focus should be on the actual metrics driving business decisions, not just security tools. Importantly, a CISO must be able to defend the security program with key stakeholders. By delivering outcome-oriented reporting, organizations can achieve their goals.

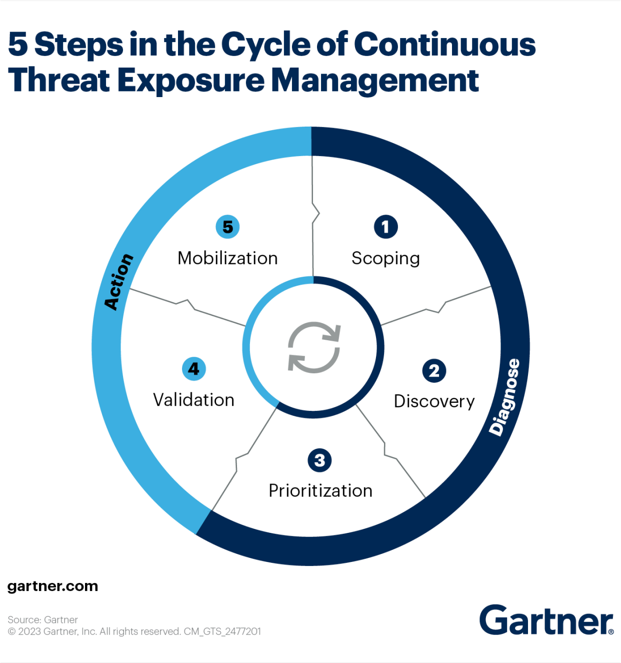
Most importantly, they need answers to the key questions:

- ***What can be compromised today?***
- ***What is the likelihood of that happening?***
- ***What is the aggregate impact?***
- ***What is the level of operational risk?***

The Optimal Way to Report Risk to the Board

For reporting to achieve the desired effect, a new approach is needed. This approach should leverage the ongoing and holistic methodology of the Continuous Threat Exposure Management (CTEM) framework by Gartner®. CTEM continually assesses the entire ecosystem, including networks, systems, assets, and more, to identify exposures and weaknesses to reduce likelihood of impact.

SATIUS SECURITY's Threat Exposure Management as a Service enables organizations to leverage a CTEM-based approach, reducing risk and enhancing their security posture. The platform offers valuable prioritization, guided remediation, executive-level reporting, and posture trending, allowing CISOs and their teams to demonstrate how attackers can compromise critical assets across hybrid environments. It provides clear, context-based insights into all exposures, utilizing sophisticated attack modeling to map potential attack paths arising from misconfigurations, vulnerabilities, and overly permissive identities. Additionally, the service quantifies risk to critical assets and identifies techniques attackers can use, empowering organizations to focus their remediation efforts effectively.


5 Steps in the Cycle of Continuous Threat Exposure Management

gartner.com

Source: Gartner
© 2023 Gartner, Inc. All rights reserved. CM_GTS_2477201

Gartner.

CTEM as a Service

Why Satius Security's CTEM as a Service?

Operationalizing The Framework requires:

Comprehensive

- holistic
- Structured
- clear

Technology & Tools

- Breach & Attack Simulation
- Attack Surface Monitoring
- Vulnerability Scanning
- Phishing Attack Simulation
- App Security, 3rd party risk, Cloud Sec, Detection Validation, etc.

Experience

- certified engineers in all tools used
- Experienced project managers

Unified Threat Exposure Insight

The Optimal Way to Report Risk to the Board

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%

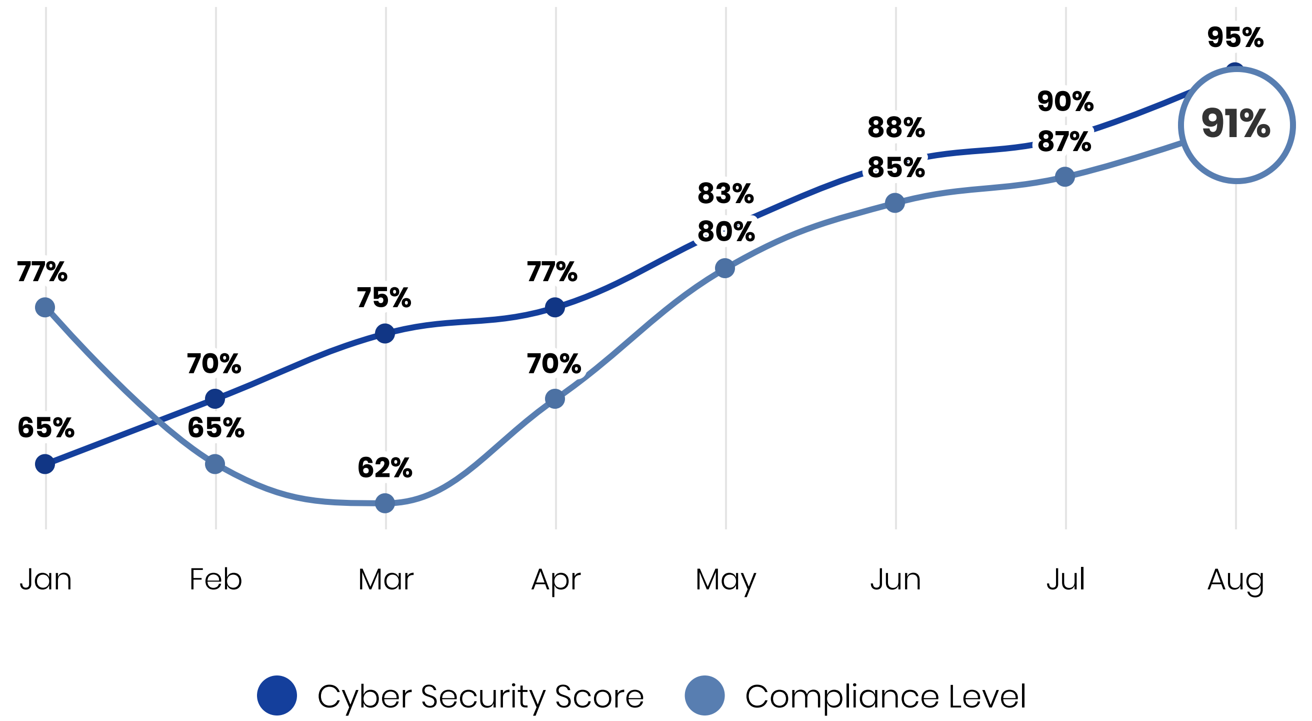
Active critial findings

34

Unified Threat Exposure Insight

Comprehensive Cyber Security Posture Score

Threat Exposure Management Quantified



+5%

August over June

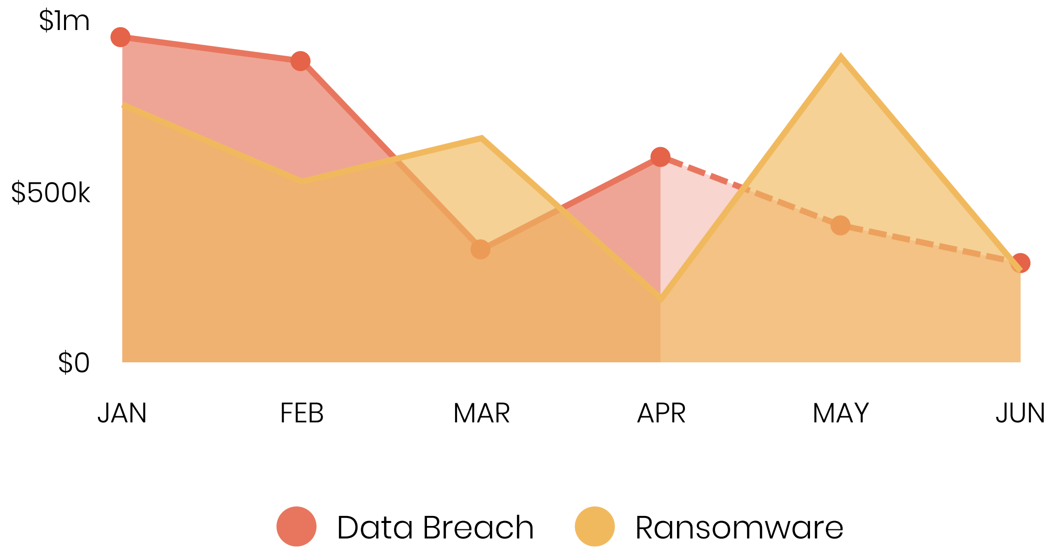
The Unified Threat Exposure Insight consolidates the organization's security posture into a single, comprehensive view. We utilize powerful visualizations, such as risk heat maps, scorecards, and trend analysis graphs, to provide stakeholders with a clear and actionable understanding of the overall cybersecurity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

Unified Threat Exposure Insight

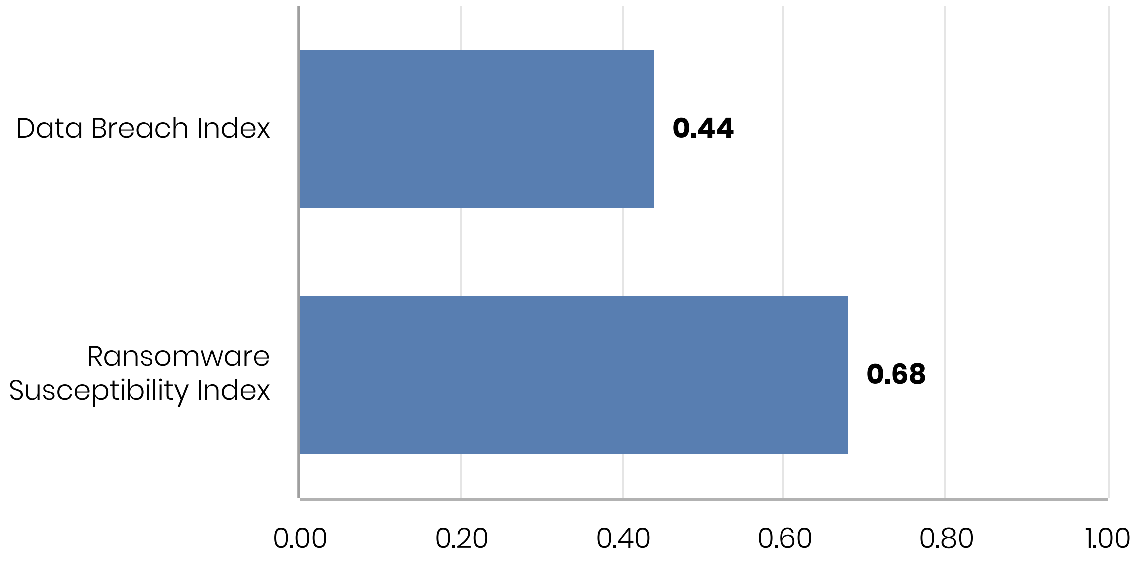
Annualized Breach, Ransomware, and Reputation Loss Risk

Threat Exposure Quantified

Annualized Financial Loss Risk



ACME company



Attack Surface Monitoring with 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

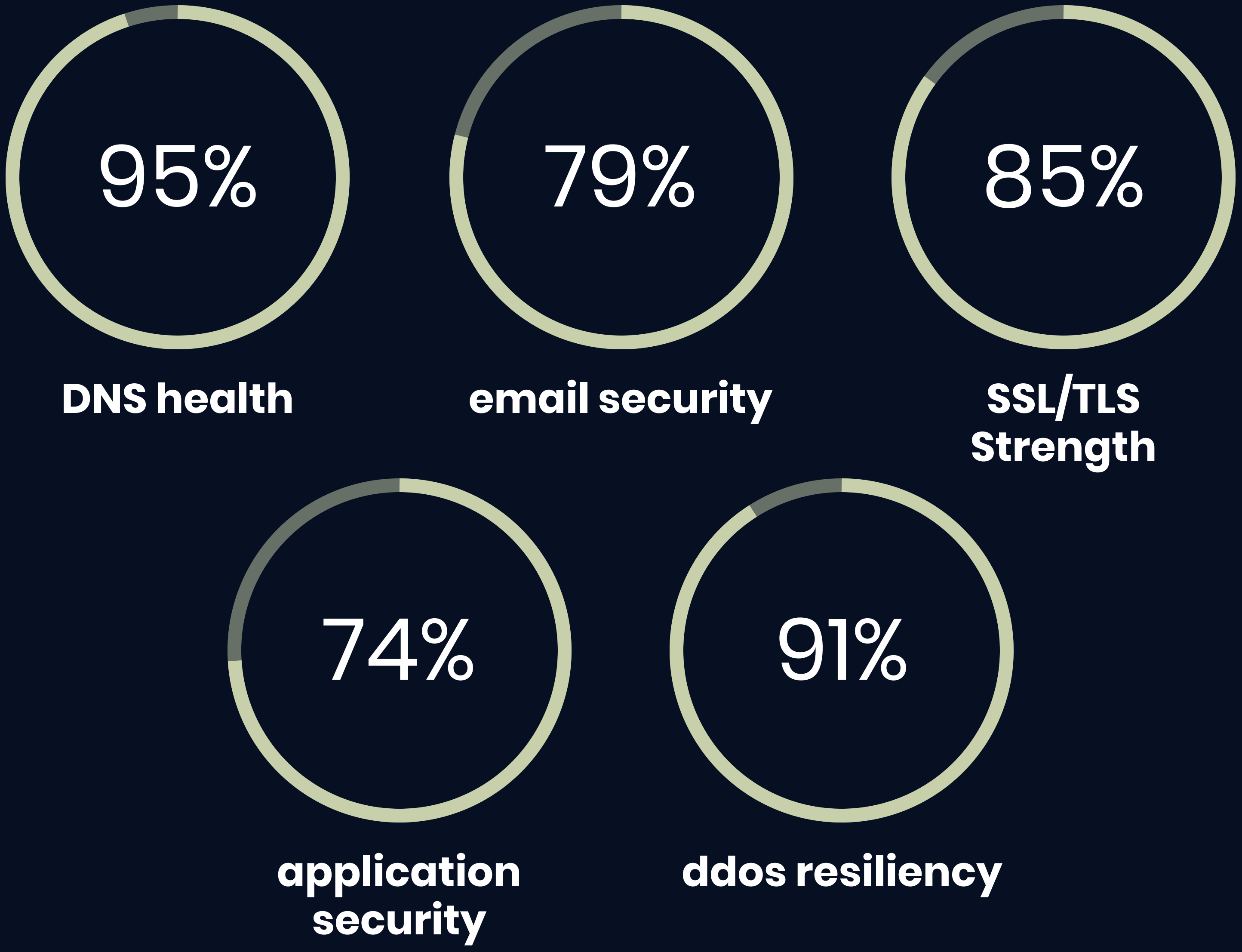
PATCH MANAGEMENT

WEB RANKING

INFORMAITON DISCLOSURE

CDN SECURITY

WEBSITE SECURITY



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

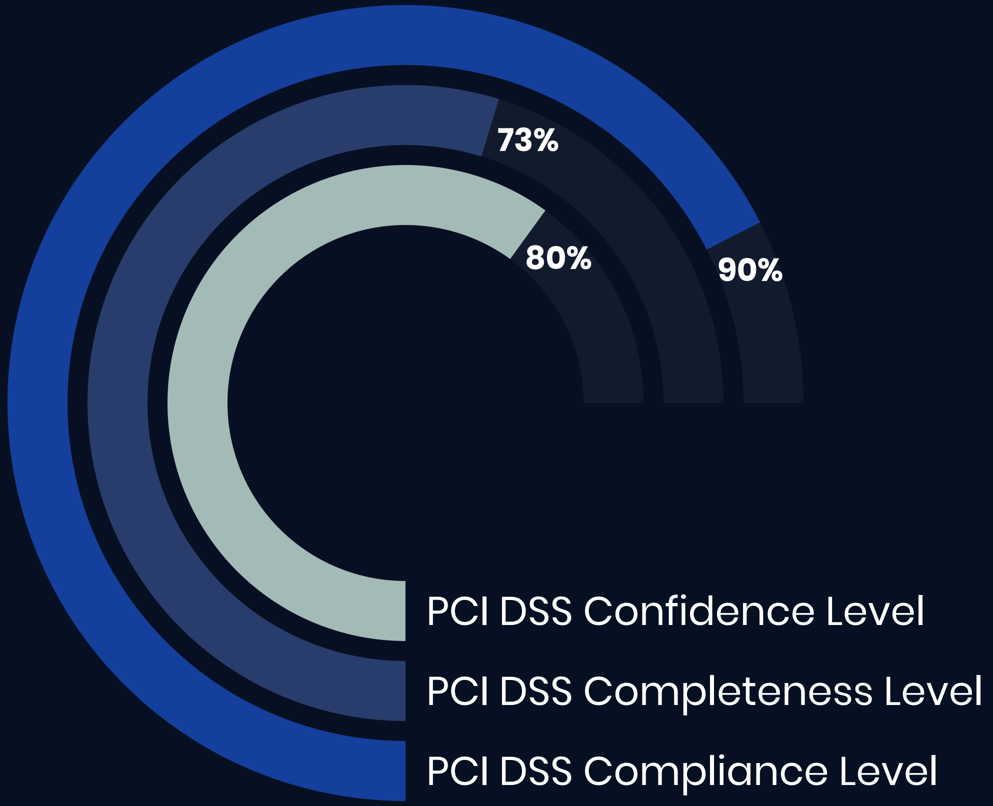
NIST 800-53

Custom Standard

CTEM Risk Categories

Attack Surface Monitoring

Over 15 Regulatory Standards



Risks Based Campaigns

Users' roles

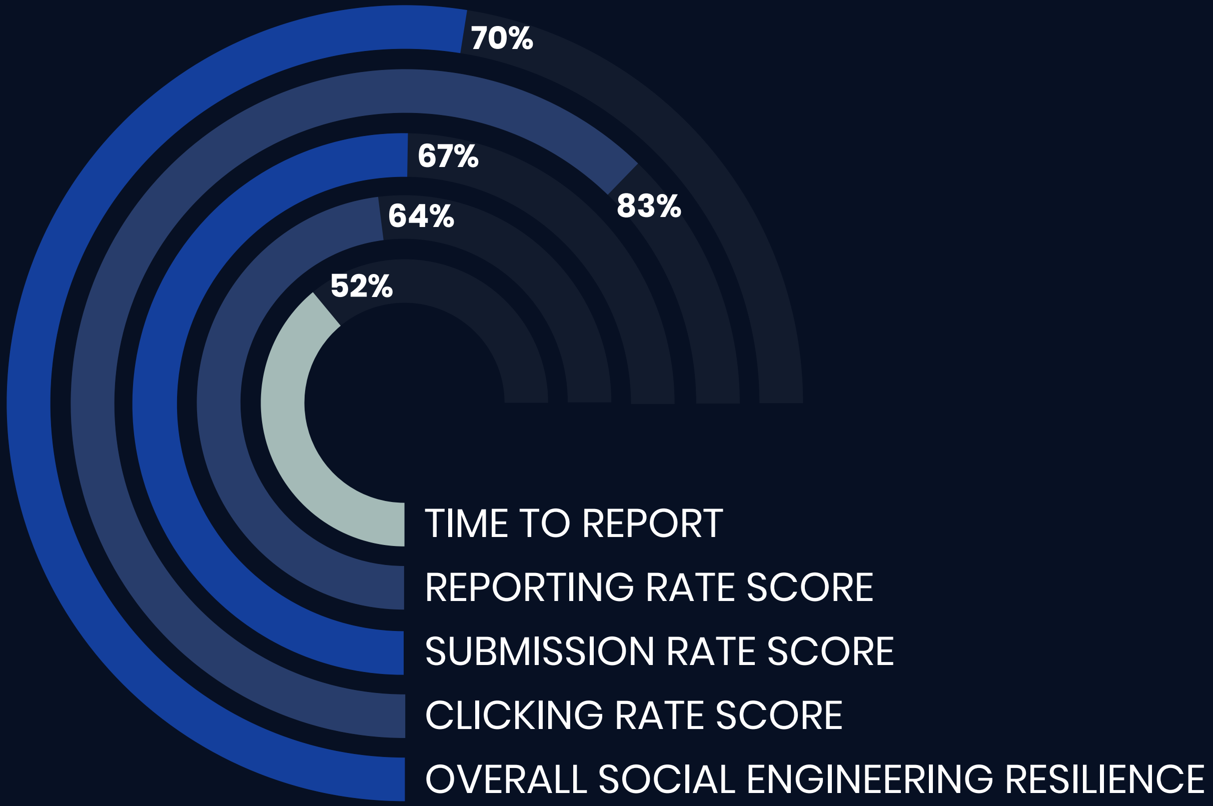
Leaked Credentials

Leaked Emails from social media

CTEM Risk Categories

Social Engineering

Fully understand employees' performance after each campaign



CTEM 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.

CTEM Risk Categories

Add-On Categories/Modules

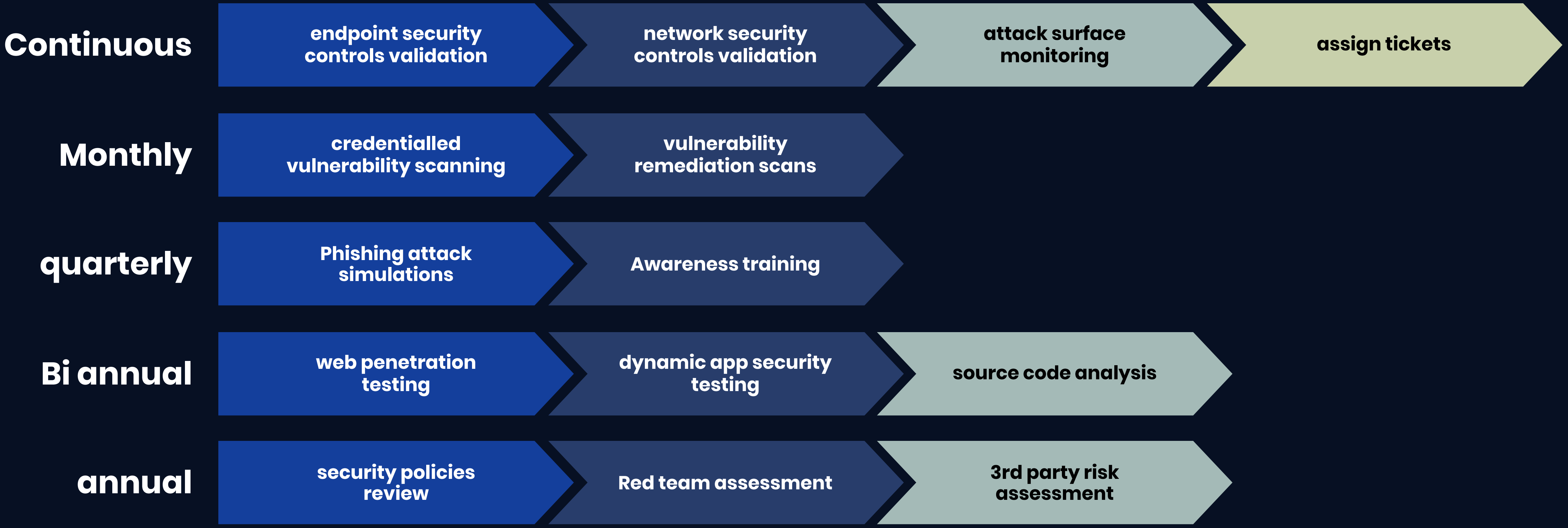
Adaptive solution to fit your environment and budget

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 as a Service

Build Your Service Profile

Customize the Risk Categories, Assessment Modules included and frequency of assessments



Continuous	endpoint security controls validation	network security controls validation	attack surface monitoring	assign tickets
Monthly	credentialled vulnerability scanning	vulnerability remediation scans		
quarterly	Phishing attack simulations	Awareness training		
Bi annual	web penetration testing	dynamic app security testing	source code analysis	
annual	security policies review	Red team assessment	3rd party risk assessment	

Unified Threat Exposure Insight

Your Roadmap to improvement

Aggregated, Validated, and Prioritized findings

Critical

Endpoint Security Module
Create a scheduled task "GameOver" using schtasks command Variant-1

Network Security Module
Order Cake

Vulnerability Scanning Module
Schedule Band

DAST Module
Decorate

High

SAST Module
Source code vulnerability

Web Pentest
App logic

CDN Security
Approve Menu

Medium

Web Pentest
Guest List

Vulnerability Scanning
Send Invitations

Leaked Credentials
Hire Caterer

Credentials Mgmnt.
Get Budget Approval

LOW

Website security

Vulnerability scanning

endpoint security

HQ

5112 Preston Pkwy, Perrysburg, OH

☎ 419-601-8694

@ gus@satius.io