ARCTIC WOLF

Cyber Resilience Assessment

<ENTER PRESENTER NAME>

The Challenge in the Landscape

Cyber resilience and cyber risk quantification are still just in the early stages of adoption into the broader business risk/resilience initiatives. Organizations need a quick and easy way to get up to speed.

What are Orgs Doing Today?

Excel-Based Mappings

Time consuming internal process to map industry-standard frameworks to an Excel document. Internal stakeholders may not be able to easily track the logic, or more importantly, the importance of the mapping.

Custom Scoring

Each organization using their own scoring system means that there isn't a way to benchmark the posture of an organization relative to industry peers

Costly Outsourcing

Organizations contract with 3rd parties for assessments to map against controls. These efforts are costly, time consuming and difficult to maintain over time.

CISO Storytelling

The weight of the storytelling falls to the CISO to highlight how posture shortfalls and strengths impact cyber resilience (business resilience), which is a burden and inconsistent

Assess cyber risk, Improve cyber resilience.

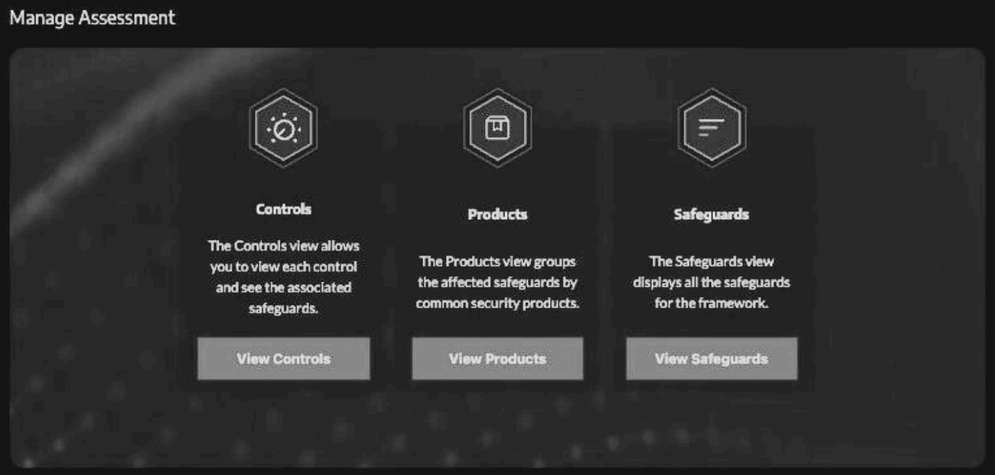
Cyber Resilience Assessment

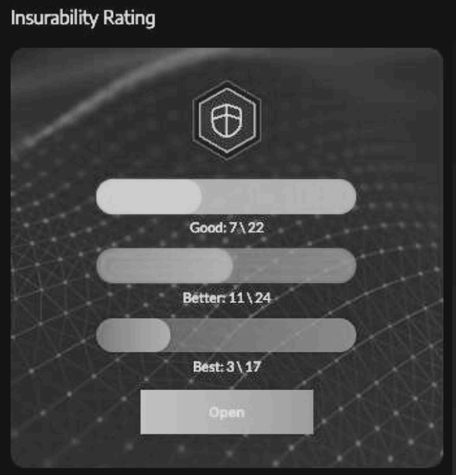
Arctic Wolf Cyber Resilience Assessment enables you to map your security posture against industry standard frameworks, such as NIST CSF and CIS, so you can prioritize risk mitigation initiatives.

Arctic Wolf Cyber Resilience Assessment

Assess your security posture against industry-standard frameworks

- Establish a baseline and track progress
- Leverage insights to prioritize and address gaps
- Quantify how new capabilities and mitigations impact risk



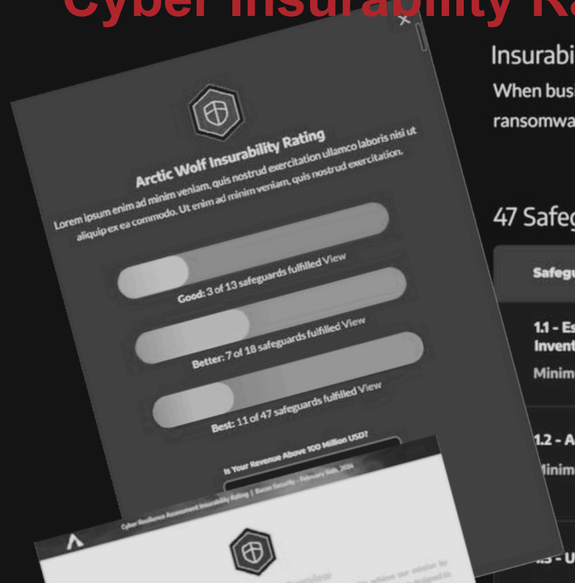


Cyber Insurance Rating

- Identify and address risks to reduce risk profile and improve insurability

Assess your Cyber Risk: Cyber Resilience Assessment

Cyber Insurability Rating



Insurability Rating

When businesses fall victim to a ransomware attack, they can't do business. Tetra Defense is one of the few incident response firms to prioritize restoration from ransomware attacks while simultaneously conducting our investigation, getting you back to business faster.

47 Safeguards | Hide Requirements | Filters: Best | Impact +3.3

Safeguards	Policy Definition	Activation & Enforcement	Consistent Review & Reporting	Impact	Current / Maximum Assessment
1.1 - Establish and Maintain Detailed Enterprise Asset Inventory Minimum Requirements: Not Met	No Policy Approved + Comm	> 60 + Critical > 60 + Critical	None > 20%-60%	+.4	6.2/11
1.2 - Address Unauthorized Assets Minimum Requirements: Not Met	Approved + Comm Approved + Comm	None > 60 + Critical	Infrequent > 20%-60%	0	8.2/16
- Utilize an Active Discovery Tool Minimum Requirements: Not Met	No Policy Approved + Comm	< 20%-60% > 60 + Critical	Needs Review > 20%-60%	0	0/1
1.4 - Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory Minimum Requirements: Not Met	Approved Approved + Comm	< 20% > 60 + Critical	None > 20%-60%	0	2/5
1.5 - Use a Passive Asset Discovery Tool Minimum Requirements: Not Met	Approved Approved + Comm	Needs Review > 60 + Critical	> 20%-60% > 20%-60%	0	0.6/1
- Establish and Maintain Detailed Enterprise Asset ntory um Requirements: Not Met	No Policy Approved + Comm	> 60 + Critical > 60 + Critical	None > 20%-60%	0	6.2/11
Totals					17/34

Safeguard 1.3

Utilize an Active Discovery Tool

Implementation Group: IG2 **Insurance Class:** Good

Description: ipsum enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo...more

Assessment Impact: Safeguard 1.3 can contribute up to 5 points to your overall score. The current score is 2 based on several factors as shown below. A maximum score is achieved when all factors are set to the highest value.

Assessment Breakdown — **Based on Model:** AW-1

Factor		Value
Policy Definition	Approved Policy Communicated & Acknowledged	10%
Activation & Enforcement	Active and Enforcing on 20%-60% of Systems	30%
Consisten Review & Reporting	No Review or Reporting	0%

Total: 40%
*Maximum Possible Score: 5
Current Score: 2

Change History

Date	User	Factor	Updated To
10/10/23	First Last	Consistent Review & Reporting	<20%-60%
10/4/23	Long First Long Last	Policy Definition	Approved + Comm
9/28/23	First Last	Activation & Enforcement	>60 + Critical

View More

Close

Cyber Resilience Assessment Key Benefits

Assess

Industry-Standard Frameworks:

- NIST CSF 1.1, 2.0
- CIS Critical Controls v8

Plan

Stack-rank mitigation activities based on security item scorings

Communicate

Share reports with leaders and 3rd parties:

- Assessment Report
- Insurability Rating Report