Continuous Cyber Risk

RIZQ

Continuously adaptive cyber risk assessment, vulnerability remediation, and industry cyber standards compliance.

Included in RIZQ Continuous Cyber Risk

RIZQ Continuous VM
Discover and remediate vulnerabilities every day

vCISO
Align business risk with IT & cyber deployments

RIZQ Cyber Risk & Compliance
Gain regulatory certainty with industry cyber standards compliance

Enables compliance with the cybersecurity requirements of cyberinsurance and government regulations.

SERVICE BRIEFING

RIZQ Continuous VM

Endpoint protection products detect attacks after they reach your systems.

The only way to prevent an attack is to eliminate cyber vulnerabilities.

RIZQ Continuous VM scans all your systems every day using the world's largest built-in database of over 160,000 security vulnerabilities.

Vulnerability Management



Scan Windows, Mac & Linux every day



Remediate vulnerabilities according to business risk acceptance

Did you know?

Security researchers discovered and published 50 new ways to attack systems every day in 2021.

RIZQ

SERVICE BRIEFING

RIZQ vCISO

INDUSTRY LEADING CYBER EXPERTISE RETAINED.

Your RIZQ vCISO is your high level point of contact with the MIS CCR service.



Your vCISO will:

- Help you establish the right cybersecurity targets for your business
- Orchestrate strategic hardening of your cyber infrastructure through the RIZQ services delivery team
- Enable compliance with government regulations like the Bank Secrecy Act (BSA) by participating in your organization's Incident Response Plan.

National/International cyber regulations from the FDA, FTC, Sarbanes-Oxley (SOX), HIPAA, GLBA and PCI may apply to you.

What about PR (PUERTO RICO)? About the Citizen Information on Data Banks Security Act, Act No. 111-2005

Any entity that as part of their operations resells or provides access to digital databases that at the same time contain personal information files of citizens must notify the proprietor, custodian, or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons within 10 days after violation of the system's security.

RIZQ

SERVICE BRIEFING

RIZQ Cyber Risk & Compliance

GAIN REGULATORY CERTAINTY AND KNOW YOUR LEVEL OF CYBER COMPLIANCE EVERY DAY

Face every cyber due diligence challange with assurance visibility and up-to-date transparency into your compliance posturing.

Know exactly what security you have now, where you want to be in the future, and the roadmap you will take to get there over time.

Essential for organizations in healthcare, financial services & technology.

Gain visibility into current compliance and set goals for improvement against industry standard security frameworks like:

- CIS
- CMMC
- FedRAMP
- HIPAA
- NIST
- DFARS
- SOC 2



Realtime dashboard and instant attestation documentation included.

RIZQ

RIZQ CONTINUOUS CYBER RISK

Onboarding Timeline

WEEK 1

01 CCR uplift service order

02 Deploy vulnerability scanners

03 Establish level of customer cyber risk appetite

04 Align to industry cyber standards

05 Deliver compliance documentation to customer

On day one of your service uplift RIZQ deploys nonintrusive cyber vulnerability scanners across all your desktop devices.

A single client interview allows us to establish risk and compliance targets and we are able to deliver early security attestations as soon as your first week.

Then we continue to harden your systems from attack over time while we respond to new vulnerabilities discovered every day.

RIZQ

Ready for industry leading cyber compliance? Contact us.

www.rizq-consulting.com
844-440-7640

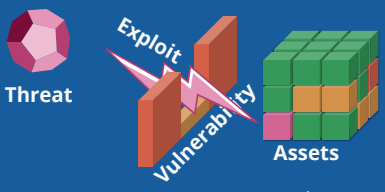


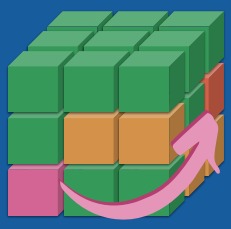
RIZQ

What is Vulnerability Management?

The Attack Chain

A threat actor exploits a vulnerability to attack an asset.





Attackers chain multiple vulnerabilities and exploits to reach a target.

After gaining a foothold, an attacker can move across systems.

Your security surface has vulnerabilities



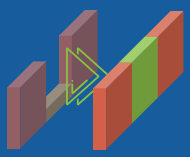
Vulnerabilities exist in:

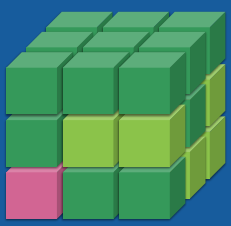
- Perimeter systems
- Anything that reads email
- Any device used to browse the web
- Any system that downloads software
- Any company you exchange data with

Breaking The Attack Chain

When you fix a vulnerability, it can no longer be exploited.

Effective vulnerability management stops attacks by breaking the attack chain.







FortMesa

Simple cyber for businesses and service providers.

... and vulnerability management too.

fortmesa.com

Find them
Scan systems and networks



Don't stop at the surface
It's critical to scan inside systems with authenticated agents



Make a list
Inventory and triage





Low risk vulns can often be accepted, others are remediated with a fix or compensating control.



Set the stage
Informed business leaders unwilling to accept risk will advocate for security investment





Fix It

A technical custodian can remediate the vulnerability with a patch or config change.



Accept The Risk

If nothing is done, this is the default.

A functional business leader accepts responsibility for risk.

A smart business leader should make informed decisions.

Deploy A Control



With engineering time or security product spend, compensating controls can harden systems to eliminate risk.

Glossary



Vulnerability
A weakness in an asset or protection



Threat
A threat is any actor that can cause losses



Exploit
Action or code used by a threat to create loss



Asset
This is the thing with value you're trying to protect



Loss
Negative impacts that damage asset value

RIZQ