



Cyber Risk Monitoring and Management

Protect your organization's good name in the face of cyber threats.

From top-level executives to IT leaders, the concern for maintaining the company's good standing is universal. It's not just about protecting against cyber incidents; it's about preserving your brand's credibility in the digital age. Our experts will ensure that your organization is well-equipped to preemptively address any cyber threat that could lead to lasting reputational harm.

What is Cyber Risk Monitoring and Management?

Cyber risk monitoring and management is a strategic, ongoing approach that involves keeping a close eye on a company's public perception while taking steps to minimize potential threats that could negatively impact its reputation. It combines visibility with action, empowering an organization to pinpoint their risks and actively implement solutions.

In the realm of cybersecurity, these processes play pivotal roles in safeguarding an organization's integrity and trustworthiness, involving constant and targeted measures to prevent and mediate security incidents that could compromise a company's reputation, such as data breaches.

With Quest's Cyber Risk Monitoring and Management services, you can focus on proactively identifying and mitigating potential threats that could tarnish your organization's hard-earned reputation. Trust us to provide the shield that guards your reputation, reinforcing the confidence your stakeholders place in your organization.

Cyber Risk Monitoring and Management Is Now a Complex Process

Cyber risk monitoring and management has evolved into a comprehensive, in-depth process that encompasses several components, including:

Third Party Risk Management (TPRM)

With an interconnected web of partners, consultants, vendors, and customers, your organization needs to identify all potential groups where a security incident could occur.

Security Rating Services (SRS)

Gain perspective on where your organization stands when it comes to cybersecurity, specifically compared to your competitors — because you don't want to be the weak link.

Risk Management

Decrease your risk and strengthen your position with new and current clients alike by maintaining a good rating and taking a proactive approach.



Reputation Monitoring

Learn how the world (insurance companies, competitors, partners, customers, and threat actors alike) see your organization, so you can be prepared for anything.

As the reach of reputation monitoring continues to expand, it's time to look toward a comprehensive program that incorporates all relevant elements:

- Monitoring
- Reporting
- Risk Management
- Vulnerability Management
- Threat Response
- Mapping to YOUR exact partners
- Managing risk with all internal/external partners

Otherwise, you run the risk of making your organization vulnerable—especially as others ramp up their security efforts.

Do You Know Your Risks?

Understanding the nature and extent of your cybersecurity risks is a crucial first step for proactive risk management. Our expert team performs an in-depth risk assessment to identify potential vulnerabilities in your cybersecurity systems and processes.

From analyzing your susceptibility to common threats like ransomware, phishing, and insider threats, to examining more complex, targeted cyber threats specific to your industry or business, we provide a clear, detailed picture of your risk landscape. As a result, your organization can make informed decisions about where to focus your risk mitigation efforts.

Are There Undetected Threats?

As cyber threats become increasingly complex and prevalent, having clear visibility into your overall cybersecurity risks is paramount. Our Cyber Risk Monitoring and Management services provide a comprehensive overview of your cybersecurity posture, so you're equipped to stay one step ahead.

We evaluate potential cyber threats and assess your readiness to respond to such threats effectively. Our team of professionals also take a deep dive into your existing cyber-insurance coverage, ensuring that you understand its scope and are adequately protected against the financial impact of potential cyber incidents.

Will Your Cyber Insurance Protect You?

Compliance with your cyber insurance policy and ensuring you are adequately covered in the event of a cyberattack are critical aspects of cybersecurity risk management.

Our services include a thorough review of your existing cyber insurance policy to ascertain your level of coverage and whether it aligns with your current risk profile. We also guide you on steps to maintain compliance with policy conditions, which can include regular cybersecurity assessments, implementation of recommended security measures, and prompt reporting of cyber incidents.

Ultimately, Quest's goal is to confirm that you are not only compliant, but also that your insurance coverage is robust enough to protect your organization should a cyberattack occur.





Why Your Organization Needs Cyber Risk Monitoring Now

A ransomware attack costs an average of \$4-5M: A single incident can quickly become a financial disaster — why not do everything possible to protect yourself now?

Cybersecurity insurance costs have gone up 50-100%: As you invest even more in your insurance, make sure you're adequately protected.

Insurance companies want to have more information: Insurance providers are expecting organizations to come prepared with key details proving due diligence.

Data is everywhere, increasing threats dramatically: The expansion of both direct and third-party relationships opens new vulnerabilities.

Full visibility is a must: Without a clear view of your organization's risks, how will you know if something important shifts?

The Unseen Threats of Ransomware as a Service: What Most Organizations Overlook

Ransomware as a service (RaaS) is a malicious cybercrime model that has become increasingly popular, raising the stakes and putting more organizations than ever at risk. And unfortunately, most organization leaders are not aware of the unique challenges posed by this rapidly developing threat.

Intricate Business Structures

RaaS exists within a complex network of ever-changing business and partner models. With cybercriminals innovating new threats daily and relentlessly seeking vulnerabilities, your cybersecurity strategy must be adaptive and vigilant to keep pace.

Universal Access Point

In the realm of RaaS, threats can emerge from any connection to your business. This wide potential for breach points underscores the need for comprehensive security measures and education across your entire organization.

Multi-Faceted Extortion Techniques

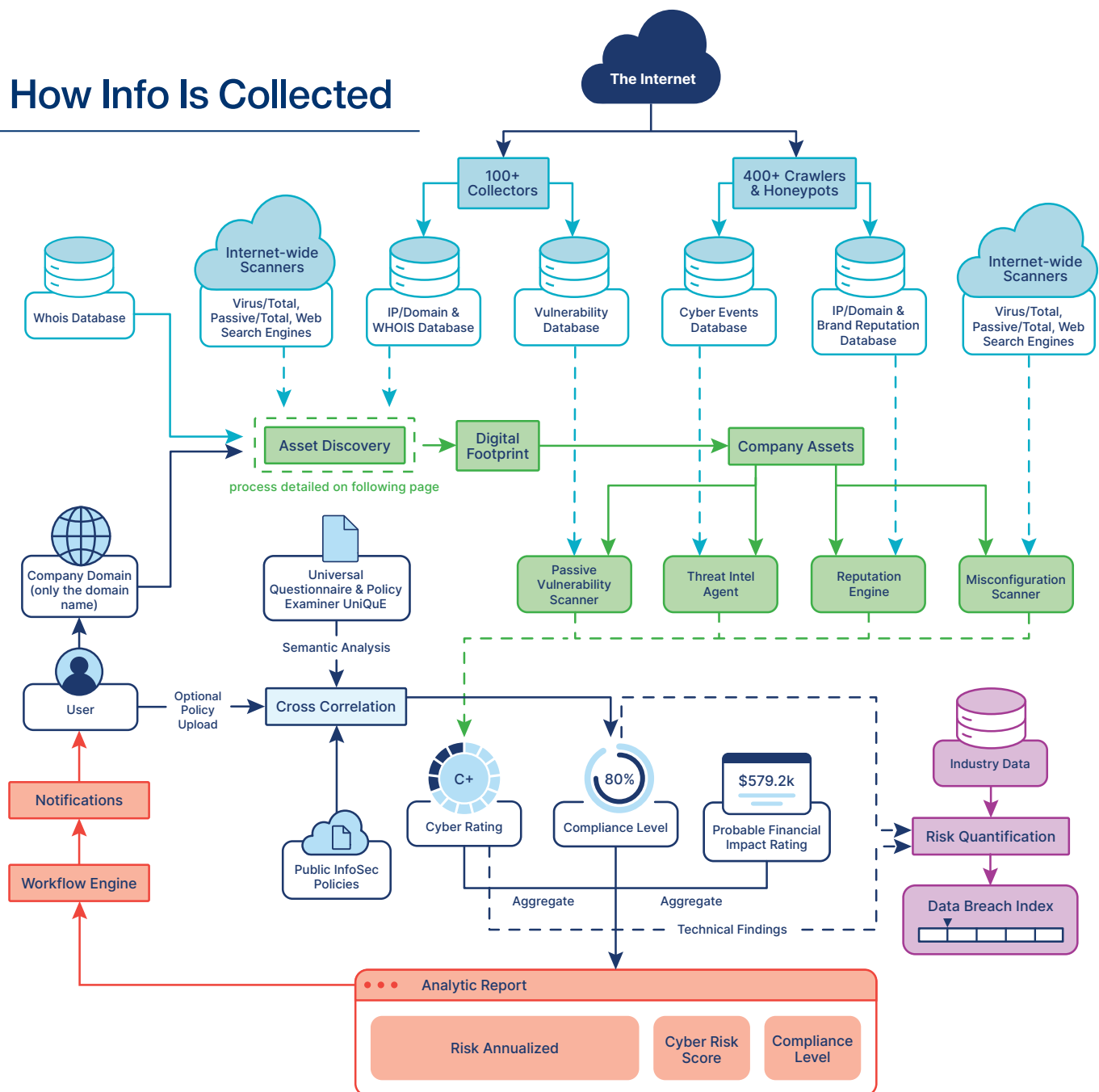
RaaS operators are experts at extortion, leveraging business interruption, data exfiltration, and encryption to coerce ransoms from their victims. Proactive measures to ensure data integrity and business continuity are vital to withstand such attacks.

Unpredictable Attack Timelines

Ransomware attacks can happen within minutes or slowly progress over months, making the need for constant vigilance and real-time threat monitoring non-negotiable. Preparedness for prompt incident response at the first sign of intrusion is crucial.



How Info Is Collected



Using open-source intelligence (OSINT) techniques, non-intrusive scans amass highly accurate data from hundreds of sources, with no interaction with the target.

False positives are no longer a problem, thanks to standard scoring models such as the MITRE Cyber Threat Susceptibility Assessment (CTSA), Common Weakness Risk Analysis Framework (CWRAF), and Common Vulnerability Scoring Systems (CVSS).

With access to massive IP & Domain Whois databases, as well as an authorized IP zone transferer, our system can utilize over a billion historical items, as well as every company-related domain name and IP address.

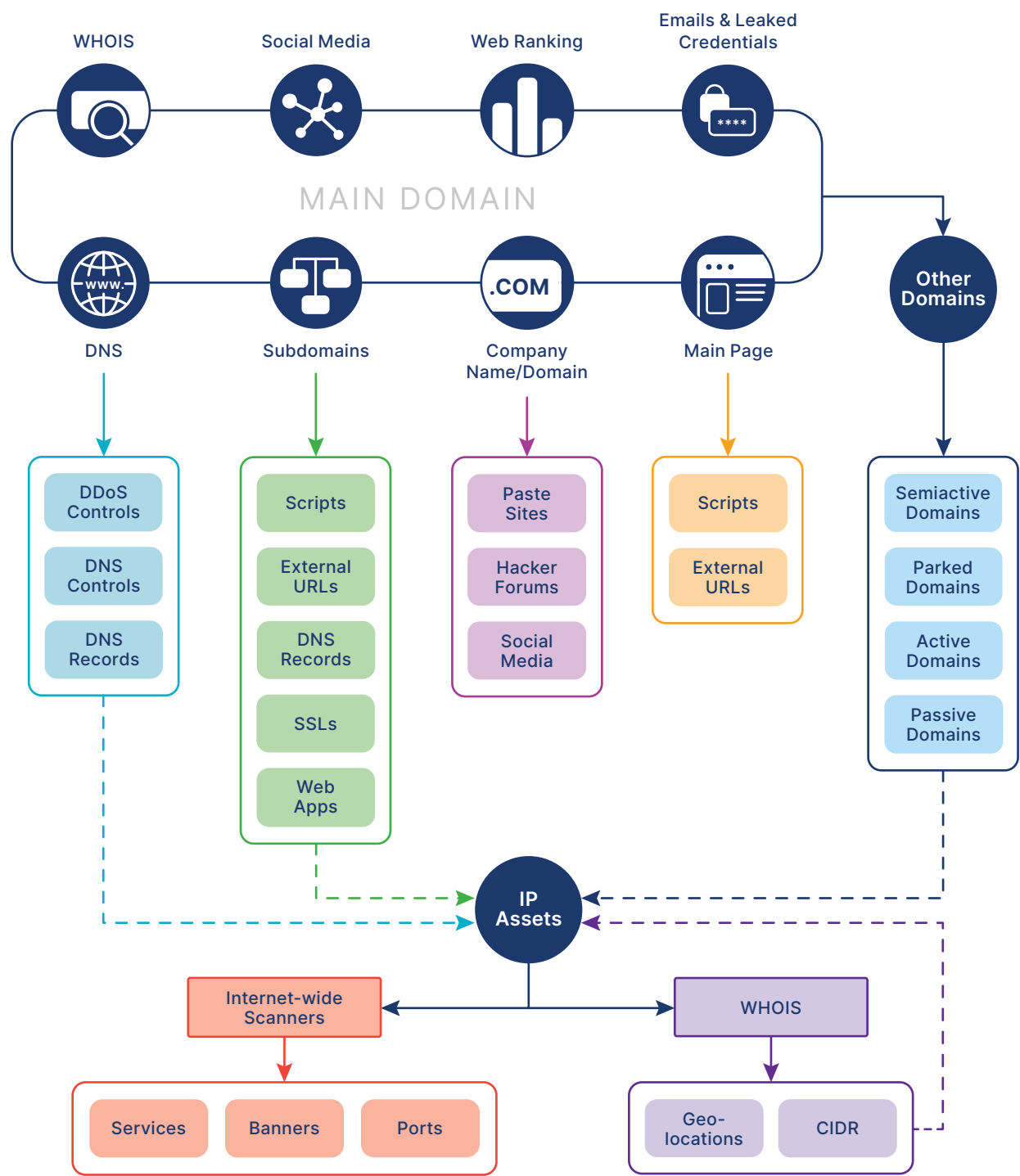
All data is assessed and compiled into an easy-to-read report, using a letter-grade approach to determine potential risks and translate technical information into relevant business concepts.



Asset Discovery

This flowchart features the process in which a network scanning tool is used to identify hardware and software, and gather precise information from each asset.

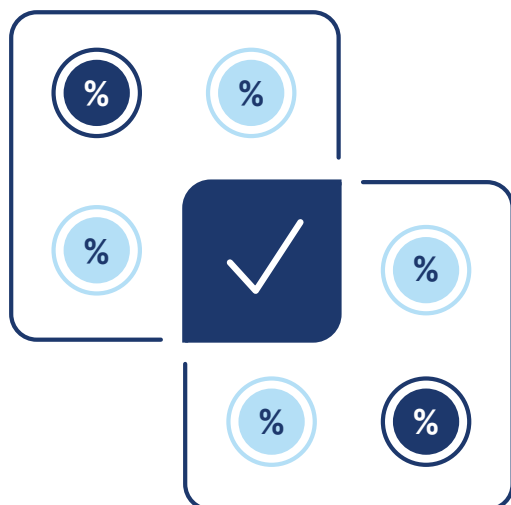
The process starts from a main domain and works through each subsequent element, leading into the IP assets branch of the systematic procedure.



Regulation Discovery

Based on Industry Standards

Strict adherence to cybersecurity compliance requirements reduces the risk of a data breach and the associated response and recovery costs, as well as the less-quantifiable costs of a breach such as reputation damage, business interruption, and loss of business.



Cross-Correlated

The cross-correlation capability measures the compliance level of a target company based on the standard input, saving time and effort for both you and your vendors.

PCI-DSS



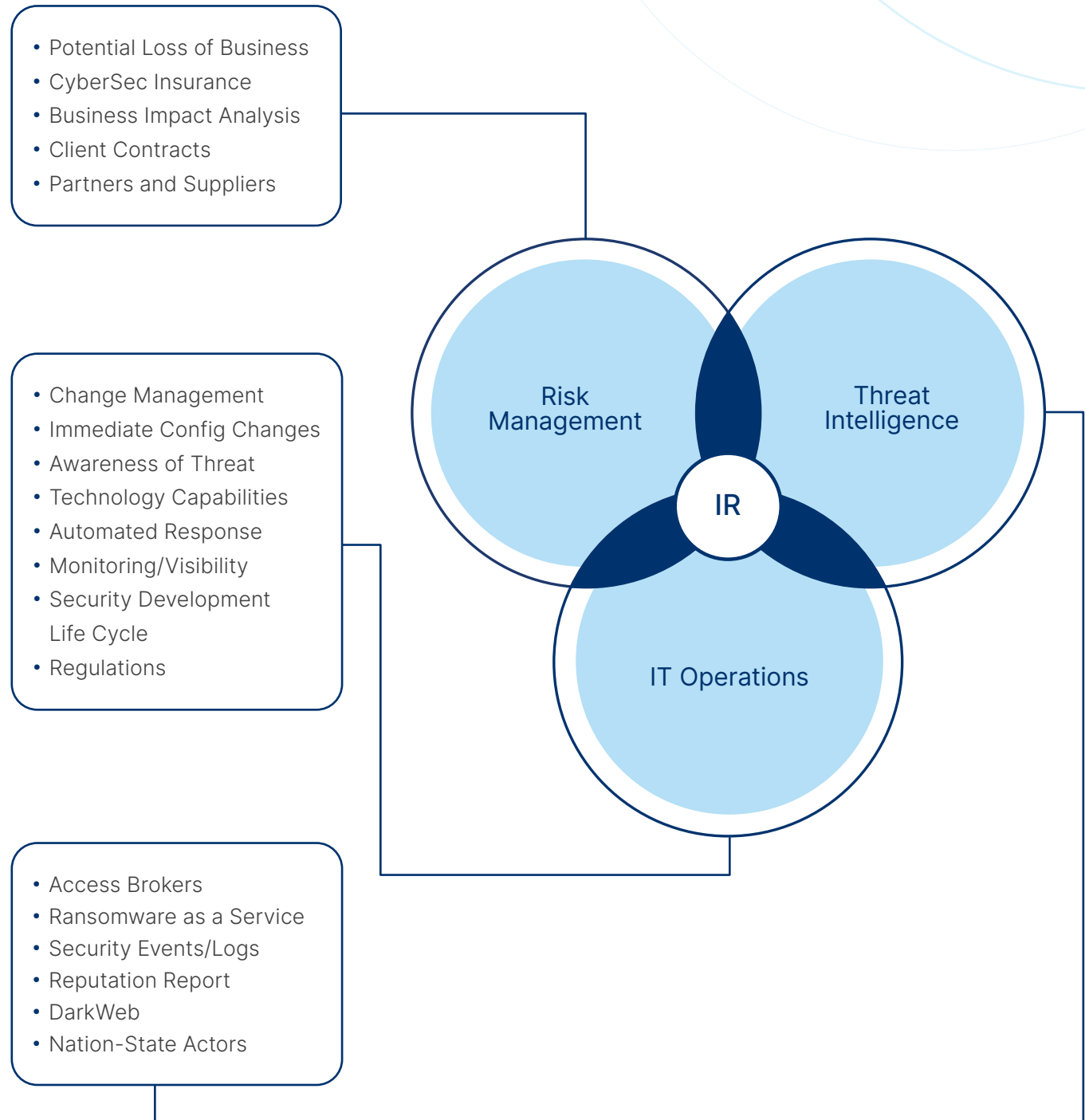
NIST 800-53



GDPR



Incident Response: Taking Action



Cyber Risk Monitoring and Management Services from Quest

Quest's team of experts have devised a comprehensive approach to cyber risk monitoring and management, so you can be confident that all your bases are covered.

Flexible Options for a Solution That Suits Your Needs

Security is never one-size-fits-all, which is why we make it simple to customize services based on your key objectives. Options include:

- 24/7 Monitoring, monthly reports, or one-time assessments
- Optional tracking for competitors, suppliers, partners, and/or potential acquisitions
- Personalized technical resources
- Industry-based comparisons
- Tailored security recommendations, including specific action steps for remediation

Detailed Reporting to Keep You Informed

Our Cyber Risk Monitoring and Management services include in-depth reporting, providing your organization with a clear understanding of the elements being monitored and the actions taken to respond to and mitigate risk.

Quest uses an innovative assessment system to provide a snapshot of your organization's security status, framing complex details in easy-to-understand letter ratings and numeric scores. For our clients, it has been proven to be a game-changing solution.

"Thanks to Quest, understanding security has never been simpler. Being able to see industry-based comparison models alongside our monthly security rating report keeps everyone on the same page – not just our IT team."

Safeguard Your Reputation Today and Tomorrow

Navigating the ever-evolving complexities of cybersecurity can be challenging, but with our Cyber Risk Monitoring and Management services, you don't have to face them alone. We provide the expertise and tools necessary to identify, assess, and mitigate your cybersecurity risks.

Don't leave your organization's reputation and financial stability to chance — be proactive, understand your risk landscape, and secure your peace of mind with our help.

Let's have a conversation.

How can we help?



www.questsys.com
1.800.326.4220

Quest[®]
TECHNOLOGY MANAGEMENT