ThreatConnect™

RISK | THREAT | RESPONSE

The Strategic Advantages of Shifting to a Risk-Led Security Program

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: +1.703.229.4489
www.ThreatConnect.com

TABLE OF CONTENTS

CEO PERSPECTIVES

An Open Letter to CISOs, CROs, and SOC Directors

Welcome and thank you for downloading ThreatConnect's new white paper Risk | Threat | Response: The Strategic Advantages of Shifting to a Risk-Led Security Program.

At ThreatConnect we recently celebrated our 10-year anniversary. And while a lot has changed since then, our mission remains the same: Fundamentally improve the way security works by developing software for security leaders and analysts alike that improve cybersecurity outcomes.

ThreatConnect has long been known as a leader in the Threat Intelligence Platform (TIP) market. We understood the need to enable large enterprises to aggregate all available threat data – both internal and external, structured and unstructured – analyze it rapidly, distill it down to understand the most critical threats, automate actions, and then produce tactical, operational, and strategic threat intelligence all in one place. But our TIP Platform is now one component of a much more powerful brain trust.

We were the first in the market to introduce intelligence-driven security orchestration, automation, and response (SOAR) capabilities. This provided security leaders with critical capabilities to break down silos and helped unify the actions of the entire security team with a true threat-oriented view — a major leap forward for security at the time.

Our September 2020 release of ThreatConnect Risk Quantifier™ (RQ) – formerly Nehemiah Risk Quantifier – created the market's only portfolio of products that unifies the actions of the security team around the most critical risks, supports their response with streamlined and automated workflows, and strengthens the entire security ecosystem through powerful technology integrations.

This is the missing link in the ability of CISOs to communicate the risks facing their companies.

The combination of RQ, TIP and SOAR is what we refer to as the **Risk, Threat, Response** paradigm. It is how organizations can move their cybersecurity programs from good to great. While each capability is a necessity for any modern cybersecurity program, their combination reduces complexity to help make decision-making easy, unites processes and technology, and continually drives down risk to help you strengthen your defenses.

I welcome you to engage us in more discussion around risk, threat, and response. You can reach out to me directly or request a demo through our website, or follow us on social media. I look forward to hearing from you.

Sincerely,

Adam Vincent

EXECUTIVE SUMMARY

Chief Information Security Officers (CISOs) operate in a world full of systemic risk, fueled by forces beyond their individual control.

Unfortunately, despite a myriad of technological advances and the adoption of seemingly countless security products — **CISOs have gained little in terms of a competitive advantage over their adversaries.**

According to a recent World Economic Forum (WEF) future series report, *Cybersecurity, emerging technology, and systemic risk*, *"the approach to cybersecurity needs to be overhauled before the industry finds itself in any fit state to tackle the threat."*

Overhauling and future-proofing cybersecurity will require a new strategic technological approach to addressing five global cybersecurity challenges:

1. The inability to assess, communicate and manage the financial impact of cyber events — and thus the business risk to the organization
2. The increasing sophistication of cyberattacks and cyber adversaries
3. Widening cybersecurity skills gap
4. Lack of intelligence and operational information sharing
5. Underinvestment and lack of business buy-in

There is a tendency in the cybersecurity industry to conflate tactical changes in the threat landscape with structural and strategic imperatives that are fundamentally altering the role and responsibilities of CISOs. Today's CISOs must do more than protect systems and data from the latest threats; they must become business enablers and champions of risk-based security programs.

That's where our risk, threat, response paradigm comes into play. It is a truly revolutionary risk-led approach that is improving security outcomes by marrying cyber risk quantification (CRQ), threat intelligence platform (TIP) capabilities, and security orchestration, automation, and response (SOAR).

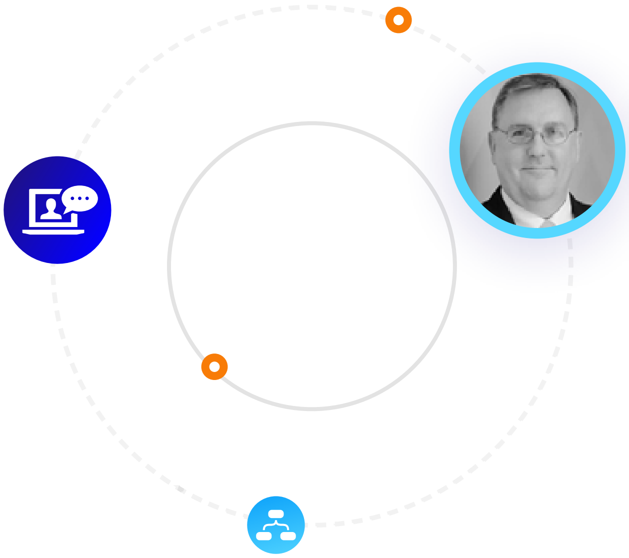
At ThreatConnect, we believe the first step in tackling each of the strategic business challenges facing CISOs starts with understanding the strategic advantages of shifting to a risk-led security program. Without understanding that risk is a business issue, not a technical issue, CISOs will likely not focus their resources on the right things.

This inability to understand the core mission of cybersecurity at a business level is one of the most critical challenges facing CISOs today. Our role as cybersecurity professionals is not solely about defending IT systems, it's about risk mitigation and protecting the business from harm. But to do this effectively requires security professionals to come to grips with how to quantify risk and communicate risk in both cyber and financial terms. Once translated into this view, security and business are on the same page. Risk mitigation then becomes the north star focus, and the struggle of resource prioritization finally dissipates as it becomes crystal clear what scenarios matter most.

With the integration of cyber risk quantification (CRQ), threat intelligence platform (TIP), and security orchestration, automation, and response (SOAR) capabilities, CISOs and other security leaders will also know exactly what scenarios to protect against, where to focus threat teams, and how to prioritize SOC team responses.

After you've had a chance to read through this white paper, I encourage you to follow us on social media (Twitter or LinkedIn), read our thought leadership blogs, listen to our podcast interviews with other CISOs and cybersecurity experts, and engage in our LinkedIn Risk-Threat-Response Forum.

**We want to hear from you and
we want to include your voice in our conversations.**



Dan Verton

ThreatConnect
Director of Content Marketing

INTRODUCTION

The global coronavirus pandemic may have dominated headlines over the past year, but business leaders are still losing sleep over cybersecurity risks.

Their worries today are at least as pressing as they were before the outbreak of the pandemic, if not more so.

The threats are still relentless. Attackers continue to build increasingly sophisticated capabilities, deploying them in a precisely targeted and persistent manner and aiming for enterprises' most valuable and sensitive data. Defenders still struggle with widening skills gaps, long-term underinvestment in cybersecurity, and the growing realization that traditional technologies and methodologies are no longer sufficient for the present-day threat landscape.

In both 2019 and 2020, executives from the U.S. and Canada listed cyberattacks as the global risk of greatest concern to their businesses.

World Economic Forum Regional Risks for Doing Business Survey[1]

The total number of cybercriminal incidents reported to the F.B.I. reached an all-time high in 2020, representing an increase of over the previous year's numbers.

FBI Internet Crime Complaint Center, Internet Crime Report 2020[2]

On average, it takes attackers 7 days to develop a fully functioning exploit for a newly discovered vulnerability. That exploit will likely remain useful for nearly 7 years.

RAND Corporation[3]

In many cases, these anxieties are underpinned by a climate of general uncertainty. As digital transformation efforts grow in scope and accelerate in speed, it's becoming more and more difficult for security organizations to keep up with an ever-expanding attack surface. The concerns have been compounded by the pressures that 2020's events placed upon defenders, of course, but they are also the natural result of longstanding trends.

In particular, business and security leaders alike are challenged by:

1. The increasing sophistication of cyberattacks and cyber adversaries
2. A critical shortage of skilled cybersecurity professionals
3. A lack of threat intelligence and operational information-sharing
4. The inability to assess, communicate and manage the financial impact of cyber events – and thus the business risk to the organization
5. Underinvestment and a lack of buy-in from the business as a whole

[1] https://widgets.weforum.org/regionalrisks2020/index.html
[2] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[3] https://www.rand.org/pubs/research_reports/RR1751.html

The natural antidote to uncertainty-based fear is clear communication, but historically it has been difficult for CISOs to translate cybersecurity threats – which are often described in technical terms – into business risk – which is best communicated quantitatively and expressed in financial terms. **As Jack Freund, Head of Cyber Risk Methodology at VisibleRisk explains,** "*Successfully presenting cybersecurity concerns to the board requires the ability to weave a narrative around what is occurring in the broader cybersecurity industry, how attackers are affecting industry peers, and using metrics, financial impact and enterprise maturity to show how cybersecurity events will affect the enterprise.*"[4]

To date, however, it's been difficult for CISOs to have these conversations with board members and other business leaders, in large part because something akin to a language barrier exists between the two groups. According to a recent CEB Research/Gartner survey, 66% of board members struggle to understand the information on cyber risk that's presented to them. And only 40% of business leaders believe such information to be actionable.[5]

What's needed is not more data. In fact, CISOs have more data on emerging cyber threats and vulnerabilities than ever before. Many have growing volumes of log and telemetry data from a continuously expanding ecosystem of cybersecurity tools and solutions. Nearly all security operations teams face far more alerts than they can feasibly investigate within the limits of human attention and the time constraints of the workday.

Instead, security leaders must cultivate the ability to prioritize, so that they're able to concentrate their efforts in the areas where they'll have the biggest impact. It's particularly important to evaluate this impact in terms of mitigating risks to the business as a whole. And they must become capable of translating cyber threats into intelligently-calculated real-world probabilities, so that the business can make reasonable investments and buy down its risks.

At ThreatConnect, we call this approach the **"risk, threat, response" paradigm**. It's a comprehensive and integrated approach that improves security outcomes by marrying cyber risk quantification (CRQ), threat intelligence platform (TIP) and security orchestration automation and response (SOAR) capabilities. In the sections that follow, we'll explain why this revolutionary approach is necessary if security organizations are to achieve their core mission of protecting the business from harm.

We'll also explore how adopting this approach can help Chief Information Security Officers (CISOs) overcome their main business challenges, as well as improve decision-making and manage resources more efficiently. And we'll consider how the paradigm can enhance defenders' effectiveness and ability to truly secure the business.

66%

of board members struggle to understand the information on cyber risk that's presented to them.

[4] https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whprcr?cid=pr_2005997&Appeal=pr&ga=2.139331507.1062586775.1614623649-1964958240.1614373589
[5] https://www.gartner.com/doc/3880379

RISK
QUANTIFICATION

What It Is, and Why It’s Needed

To date, businesses have relied on qualitative assessments of cyber risk which are imprecise and inadequate for exposing the potential harm from cyber events. With this heavily subjective approach — often reliant on the ‘gut feelings’ of experts inside the organization — we’ve tricked ourselves into believing that we understand the risks we face and that we are actually performing risk management in cybersecurity. In reality, we’re focused only on one element of the broader risk equation, and we’re missing the bigger picture and need to assess the potential financial impact of cyber events, inform the business as to that impact and manage cybersecurity with the goal of mitigating potential harm to the business.

Heat maps that seek to translate technical issues into 'red - yellow - green' or 'high - medium - low' understandings of risk provide little in the way of decision support and frankly, mean little to the business. When faced with 1,000 red, 200 yellow, and 40 green indicators, cybersecurity leaders are left with little or no context on what the impact of a red indicator might be.

And there are many other questions that are left unanswered:

1. How much more severe is one red from another?
2. What happens if we focus only on the reds and leave the yellows alone?
3. How much should we invest in addressing these problems? What kind of return do we get in terms of risk reduction?

To fulfill our mission of protecting the organization from harm, we have to actually understand what that potential harm might be. But we cannot reach that level of understanding without a quantitative view of cyber risk. Cybersecurity needs a business-based decision support system that operates in real-time. It needs automated cyber risk quantification.

Automated cyber risk quantification is now a reality, and businesses should move quickly to gain a better understanding of their actual business risks and prioritize mitigation efforts so that critical business processes, applications, and data are protected.

Cybersecurity needs a business-based decision support system that operates in real-time.

It needs automated cyber risk quantification.

What is cyber risk quantification?

Cyber risk quantification involves using scientific evidence and methods – primarily mathematical modeling – to empower business and cybersecurity leaders to make better decisions. Enterprises can achieve and maintain the level of risk exposure that they believe to be acceptable on the basis of objective data, quantitative analytic techniques, and real-world probabilities.

Quantitative modeling of potential financial losses from adverse events has long been standard practice in the insurance industry, banking, and the financial sector as well as in other enterprises across diverse verticals that face an assortment of operational risks. As an approach, it's only recently been applied in cybersecurity, in part because the risks involved have been perceived as too difficult to model.

Real Math

While the vast majority of approaches to CRQ rely on inputs akin to guesswork, ThreatConnect RQ is transparent and computes risk based on real data.

RQ leverages the industry-standard formula for computing risk:

ALE = SLE * ARO

- Annualized Loss Expectancy (ALE)
- Single Loss Expectancy (SLE)
- Annual Rate of Occurrence (ARO) = Likelihood * Probability

Data is automatically entered into the RQ Risk Model and Automation Engine. Those inputs include those from your organization's technical environment as well as industry, attack, and vulnerability data aggregated by ThreatConnect from various sources.

That information is then applied to the risk model and automation engine to determine the financial impact of cyber risks and the probability of success of specific attacks. These calculations drive a variety of other activities within RQ that lead to the operationalization of that information across the rest of your organization, including:

- Prioritization of vulnerabilities not only by CVSS score but by relevance in terms of financial impact to your business
- 'What-if' analysis to help you understand what specific effects certain changes may have on your cyber risk before actually making those changes
- Producing short and long-term recommendations on how specific changes may affect ALE and provide guidance into any 'low hanging fruit' that may exist

The capabilities of RQ give you a clear picture of inherent and residual risk in a dynamic fashion. Not only is the threat landscape and the parts of it that are relevant to your business changing, but the controls, applications, endpoints, and type of data present in your environment are changing as well. RQ enables you to apply these changes instantaneously to your models, allowing the measurement of cyber risk to move beyond point-in-time assessments and become programmatic in nature.

The coming revolution in cyber risk management

With the recognition that cyber events can have an immediate and material impact on the bottom line, business leaders' interest in cyber risk quantification has greatly increased. Across the world and across industries, Boards of Directors, CEOs, CFOs, and Chief Risk Officers are demanding a financial view into cyber risk. As a result, CISOs are responding. In PwC's Global Digital Trust Insights 2021 survey, 77% of cybersecurity leaders reported that they had already begun a cyber risk quantification initiative, or were planning to implement one in the coming months.[6]

Such initiatives promise to greatly improve security leaders' ability to communicate with business stakeholders, providing them with a common language in which to convey potential impacts from cyber events in precise and actionable terms. Leaders can now translate the likelihood of missed revenue, tarnished brand reputation, or direct financial losses resulting from a cyberattack into a clear picture of organizational exposure.

Risk quantification also promises:

- ✓ Improvements in operational decision-making
- ✓ Shortened time-to-value (TTV) for investments in cybersecurity technologies and/or services
- ✓ Reductions in unnecessary costs

This is a brave new world and as such, the majority of organizations (particularly those with fewer than 10,000 employees) lack maturity in terms of how they approach cyber risk quantification. Fewer than half use a formal risk matrix that includes quantitatively defined frequency and impact scales with scores assigned to each category. And companies with less than 10,000 employees are four times more likely not to apply any sort of quantitative assessment whatsoever.[7]

This remains true despite the fact that formal risk management frameworks such as the Factor Analysis of Information Risk (FAIR) model are now publicly available, providing businesses with the ability to understand, in a nuanced fashion, how investments of time and money will affect their security risk profiles. Formal frameworks also allow businesses to integrate cybersecurity risks into their cross-organizational risk portfolios and make standardized comparisons and evidence-based decisions.

[6] https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/pwc-covid-19-ciso-pulse-survey.html

[7] Harvard Business Review Analytics. The Necessity of Cyber Risk Quantification. Retrieved 16 March 2021, from Harvard Business Review: https://hbr.org/resources/pdfs/comm/pwc/TheNecessityofCyberRiskQuantification.pdf

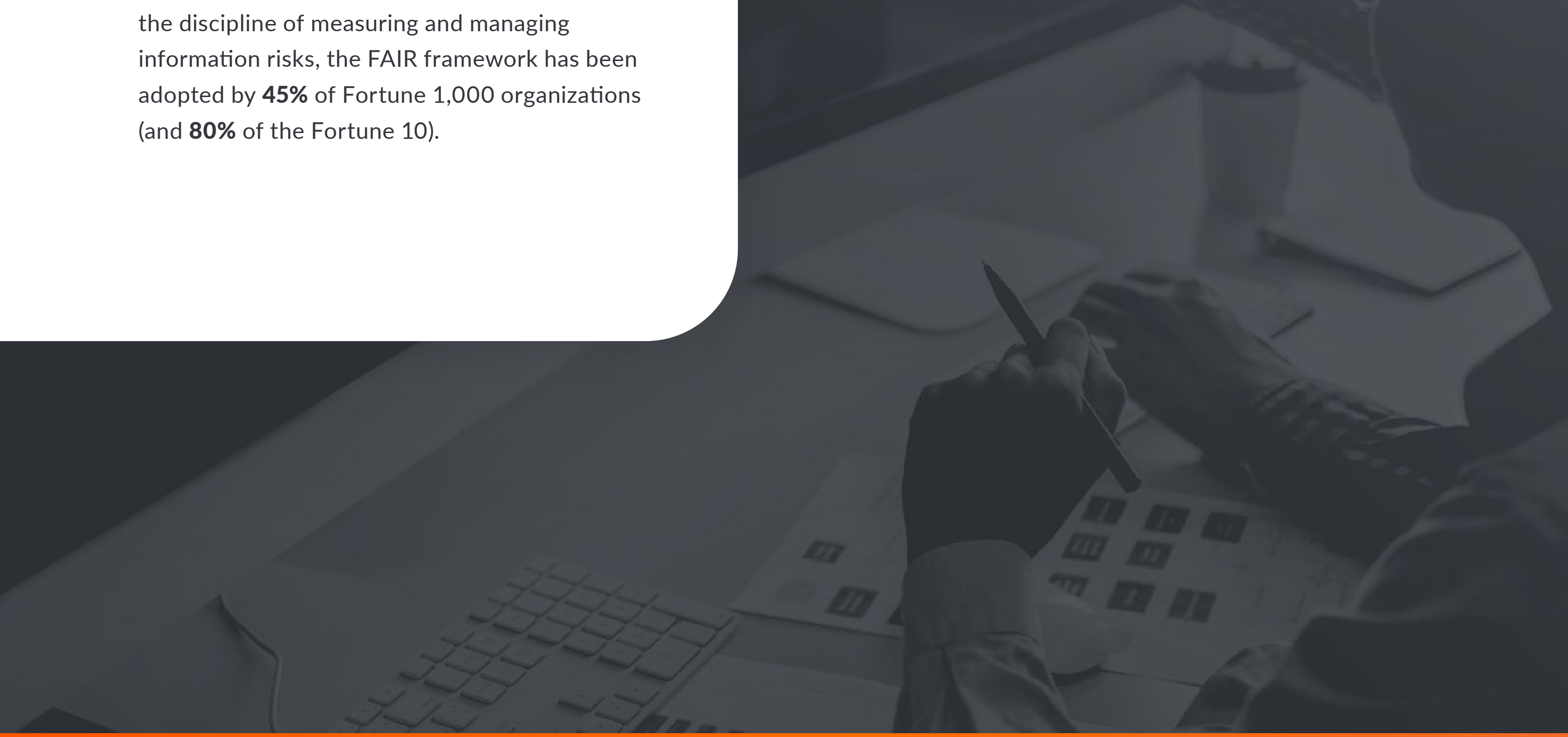
The Fair Standard

The Factor Analysis of Information Risk (FAIR) cyber risk framework is a practical methodology for understanding, measuring, analyzing, and reporting on information security risks.

Its authors contributed the FAIR risk analysis taxonomy and methods to The Open Group in 2007, making the FAIR framework the world's first open-source cyber risk quantification standard. Managed by the FAIR Institute, a nonprofit organization dedicated to advancing the discipline of measuring and managing information risks, the FAIR framework has been adopted by **45%** of Fortune 1,000 organizations (and **80%** of the Fortune 10).

The FAIR frameworks has been adopted by

45% of Fortune 1,000 organizations



While FAIR continues to have a positive impact on how security professionals think about and communicate risk, the upfront costs associated with starting a FAIR program and the time it takes to realize actual value from those investments has made FAIR inaccessible to many enterprises. Even the largest of enterprises have struggled to implement quantitative risk modeling comprehensively, due to a widespread lack of expertise in applying frameworks like the FAIR standard and the difficulty of ensuring consistency across operational processes and business units.

Ultimately, cyber risk management frameworks need to be employed because they're the only way of forging a strong link between probability-weighted cybersecurity risk scenarios and business outcomes. Access to these insights will enable business and cybersecurity leaders alike to make strategic and tactical decisions that are evidence-based and data-driven.

But the benefits promised from cyber risk quantification cannot be accompanied by complexity, major organizational cultural changes, and massive costs. Even Jack Freund, the Head of Cyber Risk Methodology at VisibleRisk and the co-author of *"Measuring and Managing Information Risk: A FAIR Approach,"* the book that laid the foundation for the FAIR standard, calls the manual nature of FAIR adoption a legitimate criticism.

"I think there's some truth to that. I've struggled myself with this because it's difficult to pay enough people to click and type your way to getting all the different types of a FAIR analysis you might need," Freund said, during a recent interview with the ThreatConnect Podcast.[8]

"I think there's definitely space for people to say, 'Okay, I like FAIR. I think it makes sense, but let's go ahead and find a way to automate this and to sort of pull in a bunch of data crunched up together and then spit it out the other side in seconds.' I think there's definitely a need for that," said Freund.

[8] Dan Verton, Improving Upon The FAIR Standard's Time-to-Value, ThreatConnect, Feb. 11, 2021. https://threatconnect.com/blog/improving-the-factor-analysis-of-information-risk-standard-time-to-value/

The Business Benefits

Most businesses don't know what their exposure is to any given cyber event, including what the impact is in terms of response costs, lost revenue, and other secondary forms of loss such as fines and judgments. Until now, the result has been a lack of focus on the risks that matter most to the business and an inability to communicate an accurate risk posture to the C-Suite and board of directors.

The Rosetta Stone that translates the technical nature of security into the language of the business is here – cyber risk quantification. By quantifying cyber risk, Chief Information Security Officers have the ability to speak the language of business.

"I think it's incredibly important to evolve the way that we talk about cybersecurity," **said Michael Daniel, a former White House cybersecurity policy advisor and the CEO of the Cyber Threat Alliance**, in a recent interview with the ThreatConnect Podcast.[9] *"Cybersecurity is now a critical enabler for most businesses to continue operating. And it needs to be framed in that way. And I think that's very much the place that we need to move is putting it in those business terms, framing it in those risk terms."*

Risk scenarios should be and can be quantified in a way that the board can understand. A board that understands the risk, threat, response paradigm is better equipped to understand prioritization and resource allocation – and the need for right-sizing of security investments.

By leveraging CRQ, a threat intelligence platform (TIP), and intelligence-driven security orchestration, automation, and response (SOAR), CISOs can more easily demonstrate what risks they are prioritizing, the actions they are taking to mitigate those risks, and the outcomes associated with those actions.

[9] Dan Verton, Improving Upon The FAIR Standard's Time-to-Value, ThreatConnect, Feb. 11, 2021. https://threatconnect.com/blog/improving-the-factor-analysis-of-information-risk-standard-time-to-value/

Make Quantification Simpler, Make It Faster, Make It More Reliable And Based On Real-World Threats

Proactive Risk Modeling and Prediction

Leverage existing data to map a forensic view of the unified risk environment. You can use that data to model probable attack vectors against the entire security lifecycle in key areas of your business to predict loss exposure and business impact, so you stay ahead of unacceptable losses.

✓ **Business Benefit?** C-Suite leaders and board members can clearly see potential hazards, narrow the focus to the risks that matter most, and better understand the need to fund and support specific mitigation measures.

Establish a Baseline, Mitigate and Monitor for Changes

Monitor changes to the threat landscape built into your modeling and then assess the potential of those changes to cause your business harm.

✓ **Business Benefit?** Armed with metrics like business interruption, reputational damage, and legal fines, leaders can proactively escalate security initiatives.

Recommend and Drive Smart Action

Activate risk mitigation plans with recommended security controls to reduce loss exposure. Engage the entire security team in response to the risks that matter most, automate workflows to increase efficiency, and use orchestration to integrate your technology stack.

✓ **Business Benefit?** Calculate the return-on-investment of your security tools and technologies by demonstrating risk reduction to underpin budget proposals and defend security decisions.

PUTTING RISK QUANTIFICATION INTO PRACTICE:

CVEs and Patch Management

In theory, applying software patches as soon as they're released seems like a low-cost and highly effective means of reducing any business's information security risks. In practice, however, security and IT organizations struggle to patch vulnerabilities in their environment in a timely manner. Security researchers estimate that it takes an average of 151 days for organizations to patch a low to medium priority vulnerability and 16 days to address a critical one. [10]

[10] https://vzmediaplatform.medium.com/how-fast-can-you-patch-how-to-buy-time-during-the-next-zero-day-vulnerability-6c5772ee3ba8

Only 44% of security professionals believe their organization is able to patch vulnerabilities at an adequate speed. Seventy-seven percent (77%) say they lack the resources necessary to keep up with the volume and pace at which patches are being released by vendors.[11]

Simply put, the number of vulnerabilities that IT and security operations teams are expected to patch in today's world far exceeds their capabilities. Given this reality, it's imperative that teams prioritize their efforts so that they're addressing the vulnerabilities that matter most.

Using a tool like the Common Vulnerability Scoring System (CVSS), an open industry standard for assessing the severity of software or information system vulnerabilities, seems like it would solve the problem. And, in fact, CVSS scoring is the most commonly-used metric for patch prioritization, employed in nearly a third of organizations.[12] However, one problem with CVSS scores is that they lack business context. Vulnerabilities are scored on the basis of how easily each could be exploited, and how much impact exploitation could have. And because CVSS scoring was explicitly designed for ease of use and repeatability across many different audiences and verticals, it's not tailored to incorporate individual industry risk profiles, though an updated extension to the framework does include a limited number of vertical-specific scoring factors.[13] Nor does it consider business context, or attempt to translate the probability of any particular vulnerability's exploitation into the financial risks that an organization that had failed to patch it might incur.

Another issue with CVSS scoring is that a very large number of vulnerabilities are classified as "critical" (i.e., scored a 9 or 10). More than 13% of currently-identified CVEs fall into this category, for a total of 16,185 vulnerabilities.

The question then becomes: how can resource-constrained security and IT operations teams decide which of these 16,185 vulnerabilities to address first?[14] In reality, once the percentage of total vulnerabilities that are deemed critical passes a certain point, the designation becomes largely meaningless, since the flood of critical vulnerabilities is simply too much for resource-constrained teams to manage.

Challenging resource allocation issues like this one can be resolved with Cyber Risk Quantification. Since it's informed by multiple data sources and leverages risk and financial models, RQ is able to accurately calculate the real-world ROI for operational decisions like which critical vulnerabilities to patch first.

Cyber Risk Quantification delivers value by:

- ✓ Solving issues of prioritization
- ✓ Determining how much financial risk any particular CVE contributes to the organization
- ✓ Providing recommendations that users can act on within a short time frame

Furthermore, Cyber Risk Quantification is not a static measure. As attackers' capabilities change over time, or your business model or IT ecosystem evolves, assessments should continuously be adapted.

[11] https://vzmediaplatform.medium.com/how-fast-can-you-patch-how-to-buy-time-during-the-next-zero-day-vulnerability-6c5772ee3ba8
[12] https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf
[13] https://www.first.org/cvss/specification-document
[14] https://www.cvedetails.com/

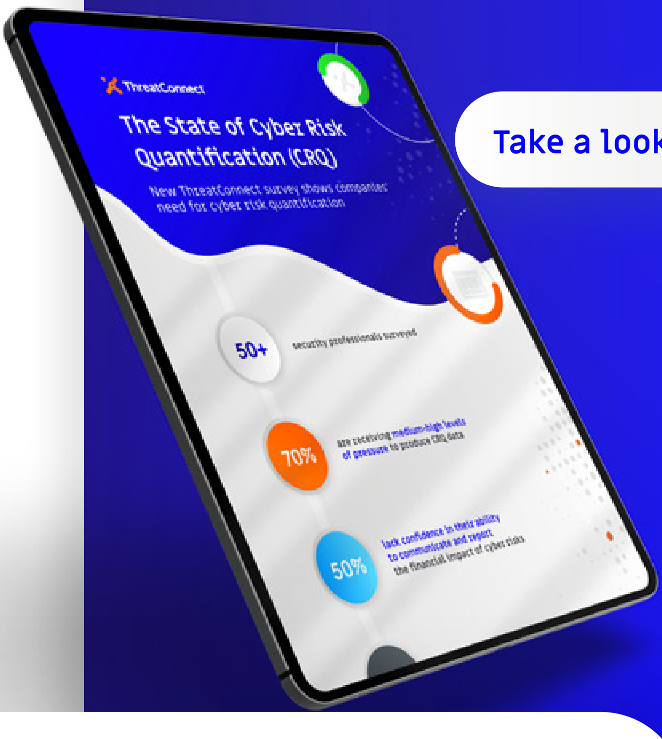
ThreatConnect Risk Quantifier (RQ)

ThreatConnect RQ is the only cyber risk quantification product on the market today that's able to fully automate the financial computation of an organization's cyber risk.

The FAIR proposition to CISOs can't be to hire more experts, add more complexity, spend hundreds of thousands of dollars on professional services, and spend a year or more building a system. That's just an untenable position for most CISOs.

ThreatConnect RQ is designed to drive complexity, time and cost out of the CRQ process. We deliver a decision support system that operates in real time rather than waiting for lengthy interviews, training and manual reviews. It is also supported by a threat intelligence platform (TIP) that injects real-world threat actor analysis into your risk models, and security orchestration, automation and response (SOAR) to turn that intelligence into action throughout your existing security infrastructure.

7 Reasons Not to Build Your Own CRQ System



ThreatConnect

The State of Cyber Risk Quantification (CRQ)

New ThreatConnect survey shows companies need for cyber risk quantification

50+ security professionals surveyed

70% are receiving medium-high levels of pressure to produce CRQ data

50% lack confidence in their ability to communicate and report the financial impact of cyber risks

Take a look →

The requirement to automate the quantitative process, to map to FAIR but make it better, could not be more urgent. ThreatConnect RQ automates the process, where others don't.

Automation boosts three specific areas for your cyber team:

- ✓ Proactively Model and Predict Risk
- ✓ Establish a Baseline, Mitigate and Monitor for Changes
- ✓ Recommend and Drive Smart Action

THREAT INTELLIGENCE

Informing Your Understanding of Risk by Providing Real-World Context

Because the threat landscape is ever-changing, calculations of risk are most meaningful when they take into account specific information about the capabilities, intentions, and most frequently employed techniques and tactics of present-day adversaries.

In order for quantitative risk calculations to be both accurate and actionable, they must incorporate contextual knowledge into their determinations of probability. An enterprise's cyber risks are not merely vertical-specific or size-specific.

They also vary according to a myriad of other factors ranging from the organization's overarching IT and computing strategies to its presence in the media. And attackers are diverse – possessing a broad array of motivations, tools, skills, and strategies.

Bringing current threat intelligence into your risk assessment and decision support procedures enables you to discern which adversaries are most likely to target your organization, based on what's been observed in the real world. Without this perspective, your analysis will remain incomplete and retain blind spots.

What is threat intelligence?

Threat intelligence is current and accurate information about threat actors' capabilities, infrastructure, motives, goals and resources. This information is gathered in order to assist in the operational and strategic defense of your computing environment.

The data can come from two general types of sources:

Internal sources

Information collected within your own computing environment will reveal which threats are truly the most relevant to you. Many security teams leverage a System Information and Event Management (SIEM) solution as their primary repository of internal threat intelligence; they may also consider log files and alerts as well as historical knowledge of what has occurred during incident response engagements in the past.

External sources

These can include open source threat intelligence feeds such as security researchers' and vendors' blogs, and publicly available site reputation and blocklists. Security organizations may also subscribe to private or commercial threat intelligence sources, some of which may be refined for a particular audience or other purposes.

> Cyber Threat Intelligence involves analyzing information about threats and producing guidance to determine what steps must be taken in response to those threats. This process... is incredibly complex and relies on a combination of people, processes and tools to generate, consume and act on the intelligence."
>
> SANS Institute, 2020 SANS Cyber Threat Intelligence (CTI) Survey.[15]

[15] https://vzmediaplatform.medium.com/how-fast-can-you-patch-how-to-buy-time-during-the-next-zero-day-vulnerability-6c5772ee3ba8

The value of threat intelligence

Knowledge without action is futile. This old saying is particularly relevant for security organizations. The key determinant of a cyber threat intelligence program's success is its ability to generate actionable insights. Threat intelligence enables teams to focus their attention on how the threat landscape is evolving, and thus to understand how the risk scenarios that the business faces are also changing. The information can be used to inform alerting systems, to generate domain or file signature blocklists, to guide incident response procedures or to aid in strategic planning.

Threat intelligence is of particularly high value when applied dynamically in a risk quantification program. It serves as the primary technical information source that feeds the risk quantification algorithm, where it is translated into business intelligence. Without this knowledge, risk calculations cannot account realistically for adversarial capabilities.

Operationally, the process of gathering and applying threat intelligence should take place within and support a set of feedback loops that are both internal and external. When leveraged internally, threat intelligence can enable continuous improvement in an alert investigation, incident response, vulnerability prioritization, and risk quantification. When published externally, threat intelligence that mature security teams have collected in their organization's environment can enrich open-source threat intelligence feeds and boost the capabilities of defenders everywhere — from those in governments and NGOs to those operating on behalf of commercial entities.

Why the Threat Intelligence Platform (TIP) is now essential enterprise software

A TIP centrally aggregates threat data from a comprehensive array of feeds, both internal and external. Integrated with SIEM solutions and other security tools, an organization's TIP serves as a place where security information can be organized and prioritized so that it's useful for driving action.

Aggregate

The TIP facilitates the collection and processing of data from internal sources as well as external feeds, normalizing and parsing this data in order to prepare it for use.

Analyze

The aggregated data can be analyzed manually or automatically, though automated methods are faster and more scalable. Analysis should validate that indicators remain valid, and should highlight associations within the data. Indicator enrichment and ranking are also important TIP functions.

Enable Action

A TIP should make threat intelligence available for use in network defenses and other integrated security products within the environment. It can also feed external threat intelligence sources, enabling the organization to contribute to the greater good of the security community.

In particular, a TIP should integrate with your security orchestration, automation and response (SOAR) platform – so that you can readily and automatically translate threat intelligence into efficient and streamlined responses.

4

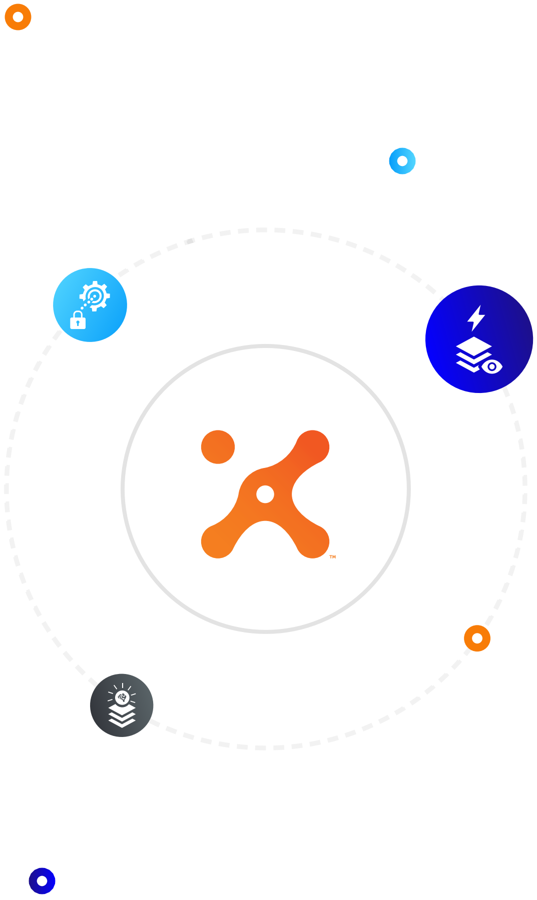
Closing the Gap Between Risk and Response with SOAR

It's an old saying, but one that still rings true. When it comes to containing attackers and limiting their ability to cause harm within your environment, time is money. On average, a company able to detect and contain a breach in less than 200 days will spend $1.1 million less than one that needs more time.[16] Yet organizations still struggle to respond to security events in a timely and effective manner. Though these metrics vary enormously depending upon the maturity of an individual security operations center (SOC), mean-time-to-detection (MTTD) and mean-time-to-response (MTTR) still averages between 100 and 150 days in most industries.

Security Orchestration, Automation and Response (SOAR) platforms were developed to speed up these response times and accelerate defense.

[16] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

What is SOAR?



First described by analyst firm Gartner in 2015, SOAR platforms incorporate automated security operations, analytics, and response capabilities. By integrating with a variety of tools and solutions across the enterprise security stack, SOAR provides for the centralization and normalization of logs and data from other sources and enables security teams to create and run automated incident response workflows.

SOAR provides the analytic engine capable of transforming raw data into the intelligence that can guide decision-making in security operations. It can also run playbooks that automatically take action, facilitating rapid, intelligence-driven response.

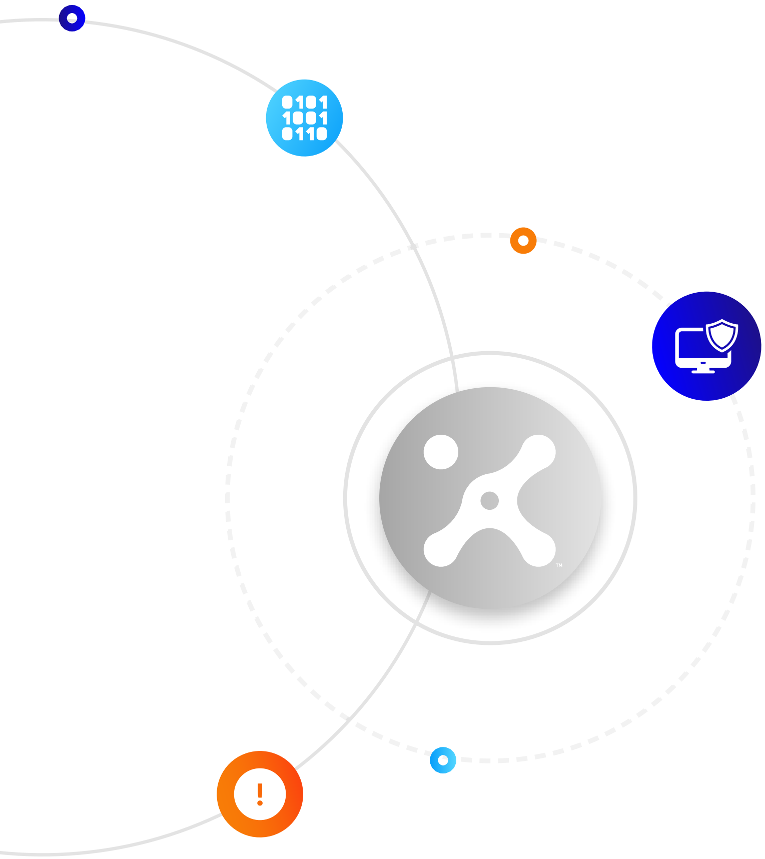
This technology brings together data from a variety of security-specific and non-security-specific log sources and enriches it with context. Analysis reveals patterns within the data, rendering it meaningful. This intelligence then drives incident response sequences, performing repetitive, task-oriented work to save human security analysts time and increase operational efficiency.

Benefits of SOAR Platforms

By coordinating multiple tasks within the security operations workflow, SOAR eases many of the burdens faced by today's security teams.

In particular, SOAR:

- **Saves security analysts' time,** enabling them to accomplish more with fewer resources. This makes it possible for resource-constrained teams to have a greater impact, even in the face of the increasing sophistication of contemporary cyberattacks and adversaries.
- **Serves as a central information repository** that not only facilitates knowledge sharing but also operationalizes this information.
- **Supports regulatory compliance** by capturing knowledge to expedite and simplify reporting.



As a technology category, SOAR was borne from the convergence of several formerly distinct products or platforms. And as a converged solution, it's most effective when used in concert with other tools and threat intelligence. This way, threat intelligence, and orchestration can feed and enable one another in an ongoing feedback loop. This makes it possible for security teams to build playbooks that orchestrate responses to newly-discovered threats across the entirety of the security technology stack.

In particular, this sort of unified and integrated platform approach enables:

- Automation of simple preventative tasks like alerting and blocking, based on relevant threat intelligence.
- Understanding of context in order to continuously improve processes.
- The capture of insights and artifacts from your own operations and IR processes to create your own organic threat intelligence.
- Automatic adjustment of processes as the threat landscape changes.

5

BETTER
TOGETHER

The Risk, Threat, Response Paradigm

Bringing these three capabilities — cyber risk quantification, threat intelligence, and security orchestration, automation, and response — together achieves a result that's already proving essential to the future of security: It enables organizations to understand what financial risks current real-world cyber threats pose for the business, and provides them with a unified, efficient and streamlined means of responding to the threats that are most pressing.

This is a truly revolutionary approach that gives cybersecurity professionals the opportunity to realign with their true mission – mitigating risks and protecting the business from harm. To achieve this aim, however, requires CISOs and other senior security leaders to view cyber risk as a business issue, not solely a technical issue. This puts security and the business on the same page – at long last – and gives both a true north focus on the shared objective of risk mitigation.

The Four Core Tenets of the Risk-Threat-Response Paradigm:

1. Reduce complexity for business leaders and security operations teams alike.
2. Make decision-making easy by turning intelligence into action.
3. Continually reduce risk and strengthen defenses – within a set of internal feedback loops that work towards continuous improvement.
4. Unify processes and technologies.

Risk-Threat-Response is based on breaking down silos and removing barriers between traditionally distinct disciplines within the business and security operations, between threat and response, and between real-world risks and operational action.

ThreatConnect and Risk-Threat-Response

ThreatConnect's solution is unique in the marketplace today in that it provides complete operational and decision support for cybersecurity as well as the business. It's capable of serving as a single source of truth for all stakeholders from the SOC to the C-suite.

ThreatConnect has long been known as a leader in the TIP market. This expertise has taught us the value of aggregating all available data. In essence, we build upon this ability to bring information together with the Risk-Threat-Response approach. That's why our SOAR solution includes hundreds of integrations. We use them to connect the dots – between threat intelligence, internal security tools, security analysts and IT operations professionals, and business decision-makers. Our platforms bring together all the strategic, analytical, and operations capabilities that security teams – and the business – need to achieve meaningful results.

Setting the Foundation for the Next Generation of Security

Risk-Threat-Response promises to change the game for business and security leaders alike. It offers to replace anxieties about cyber risk that are founded upon uncertainty with confidence based on fact.

For far too long, defenders have struggled to quantify risks – and communicate those risks to the business.

The Risk-Threat-Response paradigm instead enables an informed understanding of risk that can seamlessly be translated into action. It helps security teams manage the threat landscape by giving them a prioritized view of the risks that are most pressing. And it enables teams to orchestrate efficient, streamlined responses across the entire tech stack for faster mitigation. Finally, and most importantly, it resolves once-competing priorities into a clear view of where the business should head next.

1 Risk

- Scope the risk scenarios that matter most – in financial terms
- Align businesses and security to a north star focus
- Solve the issue of prioritization and demonstrate security ROI

2 Threat

- Support the quanitification process with real world understanding of threat
- Manage the threat landscape with a priority view into the risk scenarios that matter most
- Continually improve security with feedback loops to both risk and operations

3 Response

- Focus response on the risks that matter most to the organization
- Unify and streamline processes
- Utilize streamlined and automated playbooks to enable smarter, faster SOC mitigations and IR
- Orchestrate response across the entire technology stack

ThreatConnect™

ThreatConnect, Inc. provides cybersecurity software that reduces complexity for everyone, makes decision-making easy by turning intelligence into action, and integrates processes and technologies to continually strengthen defenses and drive down risk. Designed by analysts but built for the entire team (security leadership, risk, security operations, threat intelligence, and incident response), ThreatConnect's decision and operational support platform is the only solution available today with cyber risk quantification, intelligence, automation, analytics, and workflows in one. To learn more about our Cyber Risk Quantification, Threat Intelligence Platform (TIP) or Security Orchestration, Automation, and Response (SOAR) solutions, visit www.ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708

Copyright © 2021 ThreatConnect, Inc.