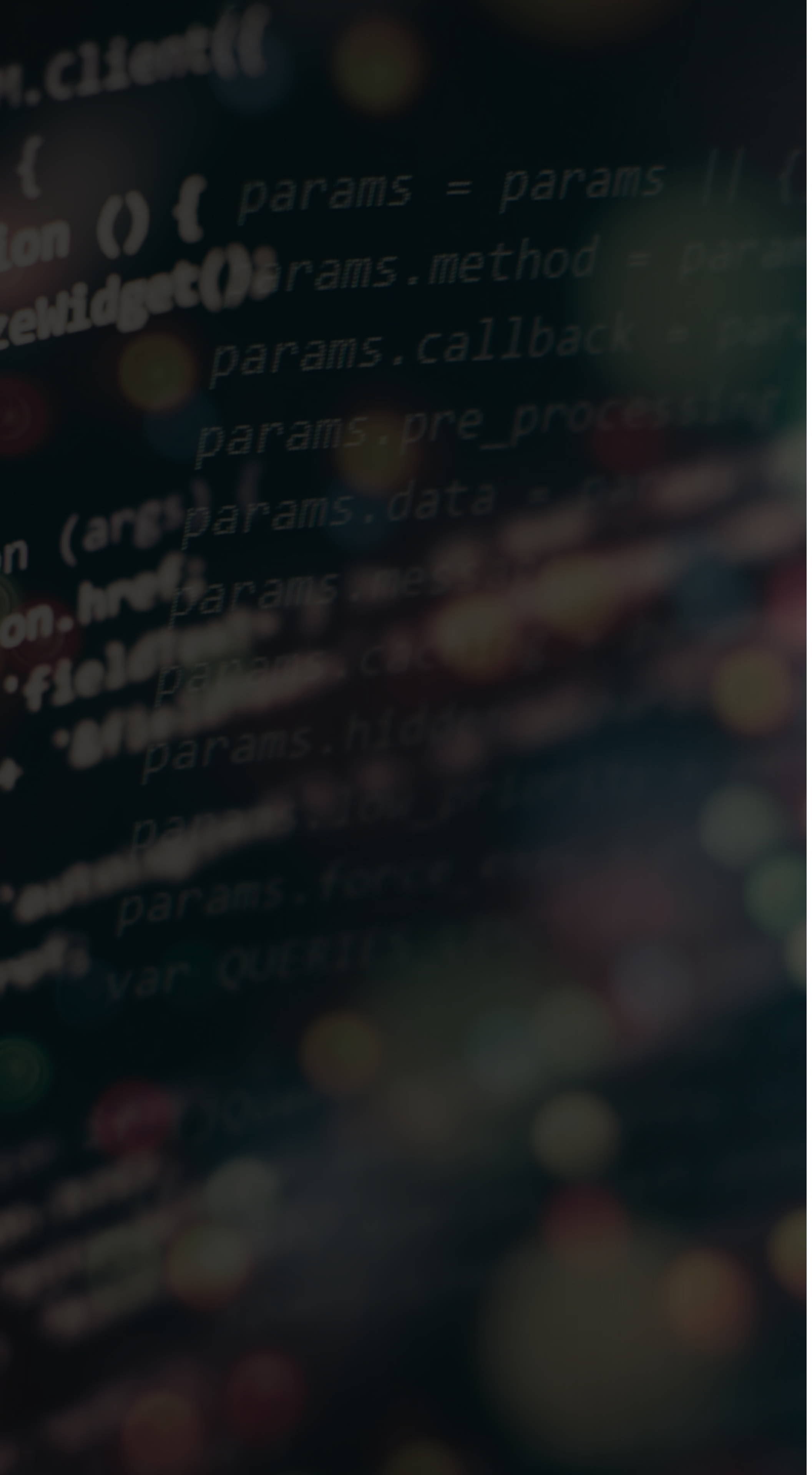
CyberProof®

SKYBOX® SECURITY

A GUIDE TO THREAT-CENTRIC VULNERABILITY MANAGEMENT

FOCUSING TIME, MONEY AND EFFORT
ON WHAT MATTERS MOST

TABLE OF CONTENTS



THE CHALLENGES OF SECURITY FATIGUE

If you talk to any C-level executives about cyber security, they will tell you that their focus needs to be on their core business – and that they need to ensure they can continually operate with confidence. If you probe a little further and ask what they mean by "operate with confidence," they will tell you that it boils down to three things, each of which is equally important:

I NEED TO PROTECT MY CUSTOMERS

I NEED TO PROTECT MY BRAND

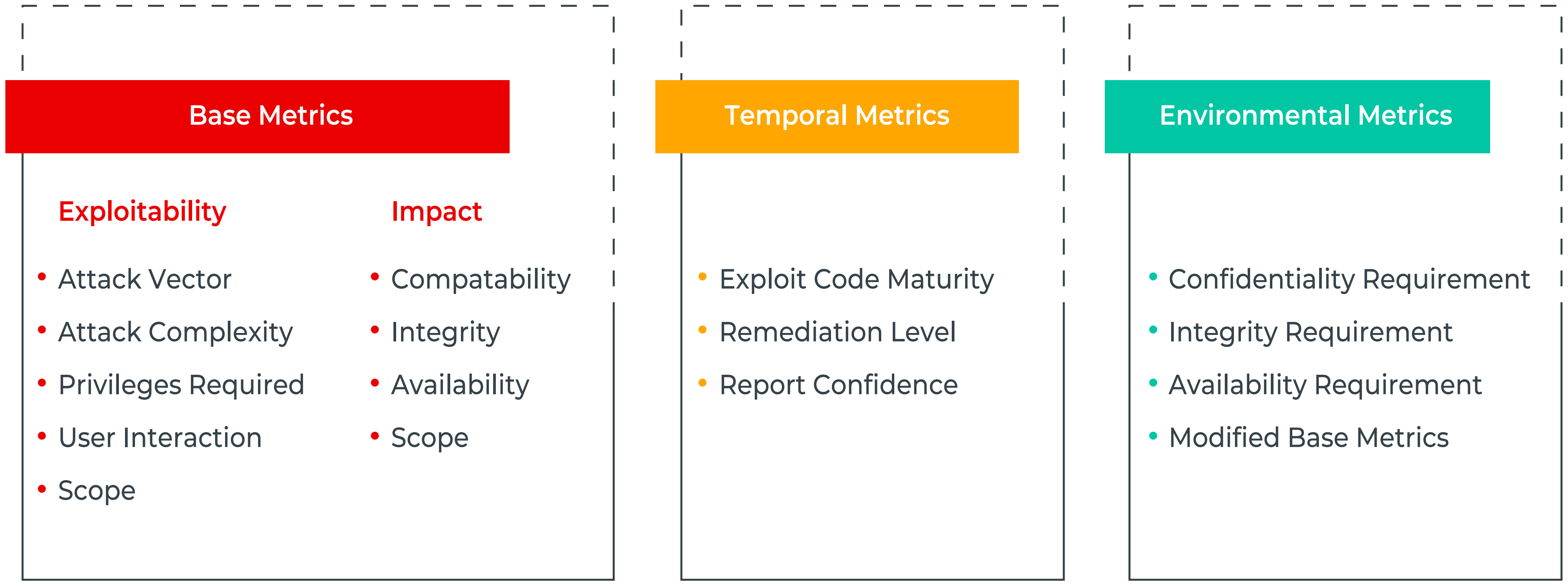
I NEED TO PROTECT MY REPUTATION

If the goal really is that simple, why is achieving it so complex? For a start, there's so much technological and data-driven noise that it can sometimes be hard to see the wood from the trees. Organizations have succumbed to this fact of life by investing heavily in multi-layered security tools – but in doing so struggle to understand if or how these investments have actually helped them manage their vulnerabilities and improve their security posture, or if indeed those three simple requirements are being met.

Most security leaders try to explain their risk exposure but often struggle to do so in a language that the board will understand. There will no doubt be a vulnerability management scanning tool in place which uses the widely known Common Vulnerability Scoring System (CVSS) to provide a scoring mechanism (0-10) that helps rate or measure the severity of vulnerabilities. But is a CVSS score alone enough to tell you where you need to focus time, effort, and money to meet those three requirements? The following illustrates the CVSS scoring in more detail.

CVSS Score Metrics

A CVSS score is composed of three sets of metrics (Base, Temporal, Environmental), each of which have an underlying scoring component:



Base Metrics

Exploitability

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope

Impact

- Compatability
- Integrity
- Availability
- Scope

Temporal Metrics

- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental Metrics

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement
- Modified Base Metrics

- **Base Metrics –** Base metrics are static; they don’t change over time. They are inherent to the vulnerability and are not modified based on characteristics such as real-world exploits or compensating controls.
- **Temporal Metrics –** Temporal metrics change over time. These include characteristics such as the maturity and availability of exploit code, as well as the availability of patches.
- **Environmental Metrics –** Environmental metrics are specific to your organization and are subject to the vulnerabilities you are exposed to. They include characteristics related to the exposed asset(s), how business critical they are, and whether or not you have appropriate mitigations or compensating controls in place.

A few questions now need to be addressed:

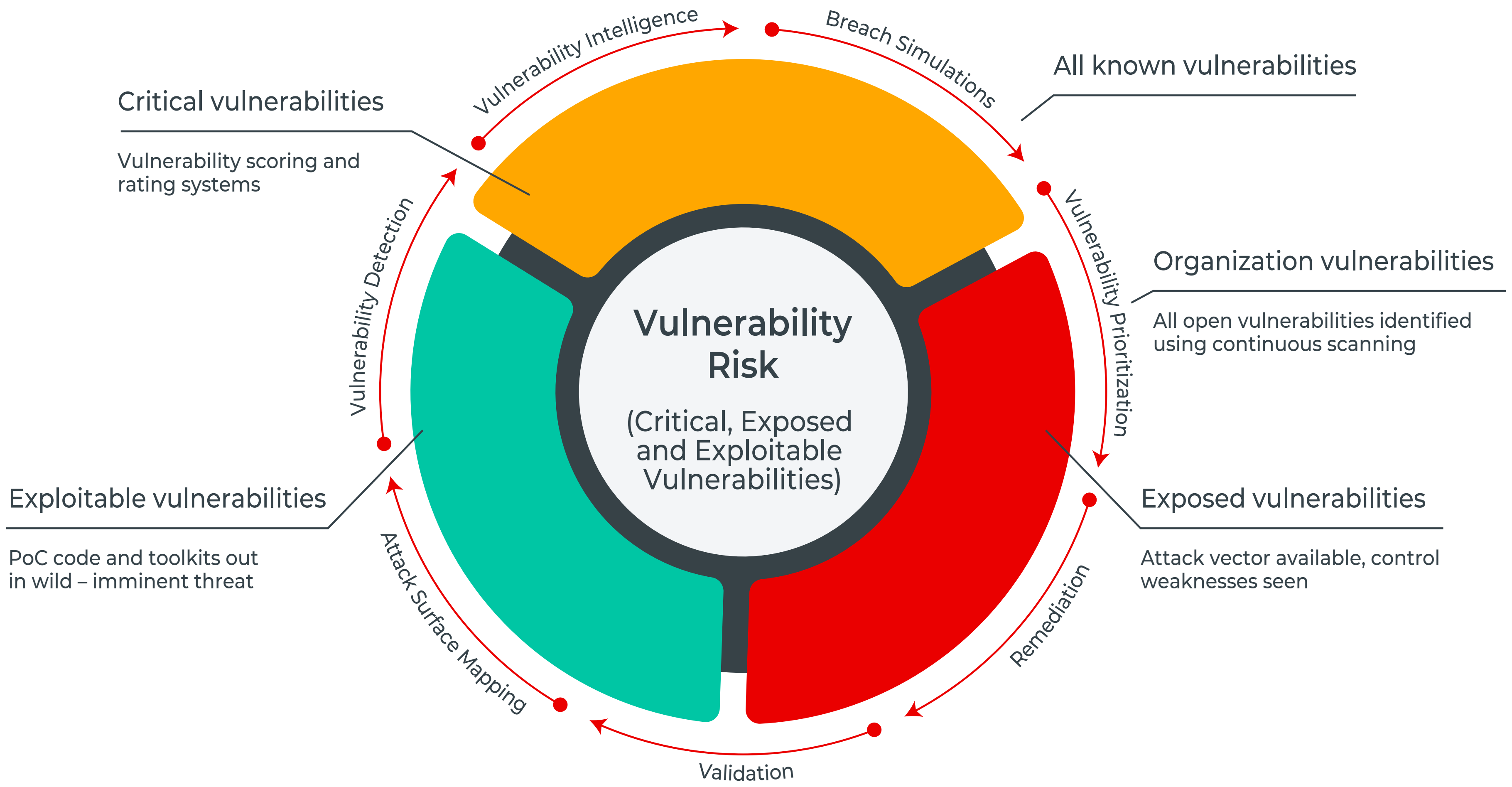
> Is a vulnerability scanning tool intelligent enough to take into account the temporal and environmental aspects that provide context and shine a spotlight on the vulnerabilities that are likely to cause the most harm?

> A scanning tool may highlight a vulnerability as “Critical,” but if it has never been exploited before or you have compensating controls to mitigate it, do you really need your high-value resources to fix it? In this case, would you still prioritize it over another vulnerability?

> Are you using the outputs from your scanning tool to guide where you employ more rigorous testing methods (i.e., ethical hacking) and are you utilizing those more expensive resources, in the right places at the right time?

> **Traditional vulnerability management methods are focused on severity, not risk.**

The following image illustrates how we are able to find the vulnerabilities that are not only exploitable and exposed – but, more importantly, are relevant to your business:


Vulnerability Intelligence
Breach Simulations
Vulnerability Prioritization
Remediation
Validation
Attack Surface Mapping
Vulnerability Detection
Vulnerability Risk
(Critical, Exposed and Exploitable Vulnerabilities)

All known vulnerabilities

Critical vulnerabilities

Vulnerability scoring and rating systems

Organization vulnerabilities

All open vulnerabilities identified using continuous scanning

Exploitable vulnerabilities

PoC code and toolkits out in wild – imminent threat

Exposed vulnerabilities

Attack vector available, control weaknesses seen

The bottom line is this: Traditional vulnerability management methods are focused on severity, not risk. Scanners leave blind spots due to un-scannable networks; scan results don't map with contextual security controls; and network topology and vulnerability prioritization needs to be aligned to threat exposure and risk.

HOW TO IMPROVE RISK POSTURE

If I understand and prioritize my risk and associated vulnerabilities, I improve my security posture, right?

To a large extent, yes. But you first need to understand where your vulnerabilities are, the risk they pose to your organization, and how they're managed today:

Infrastructure: You operate with a growing multi-device, multi-vendor and multi-platform environment – on premise, in the cloud, hybrid, and multi-cloud.

Threat Landscape: Are your internal and external threats understood within the context of your business, i.e., do you really know who's trying to attack you?

Expertise: Do you have enough of the right resources and skills to maintain robust and proactive security operations?

Attackers: Attackers are becoming increasingly sophisticated, but also very patient. They can sit quietly in your network and systems for months before initiating an attack.

Detection & Response: Do you have the ability to quickly detect and respond to those threats that exploit your vulnerabilities?

Laws & Regulations: You need to keep up with and maintain relevant compliance and regulatory requirements to mitigate potential financial penalties.

It's about understanding where your critical data and systems reside, minimizing your 'unknown unknowns,' and then ensuring the right amount of investment is made in those areas first.

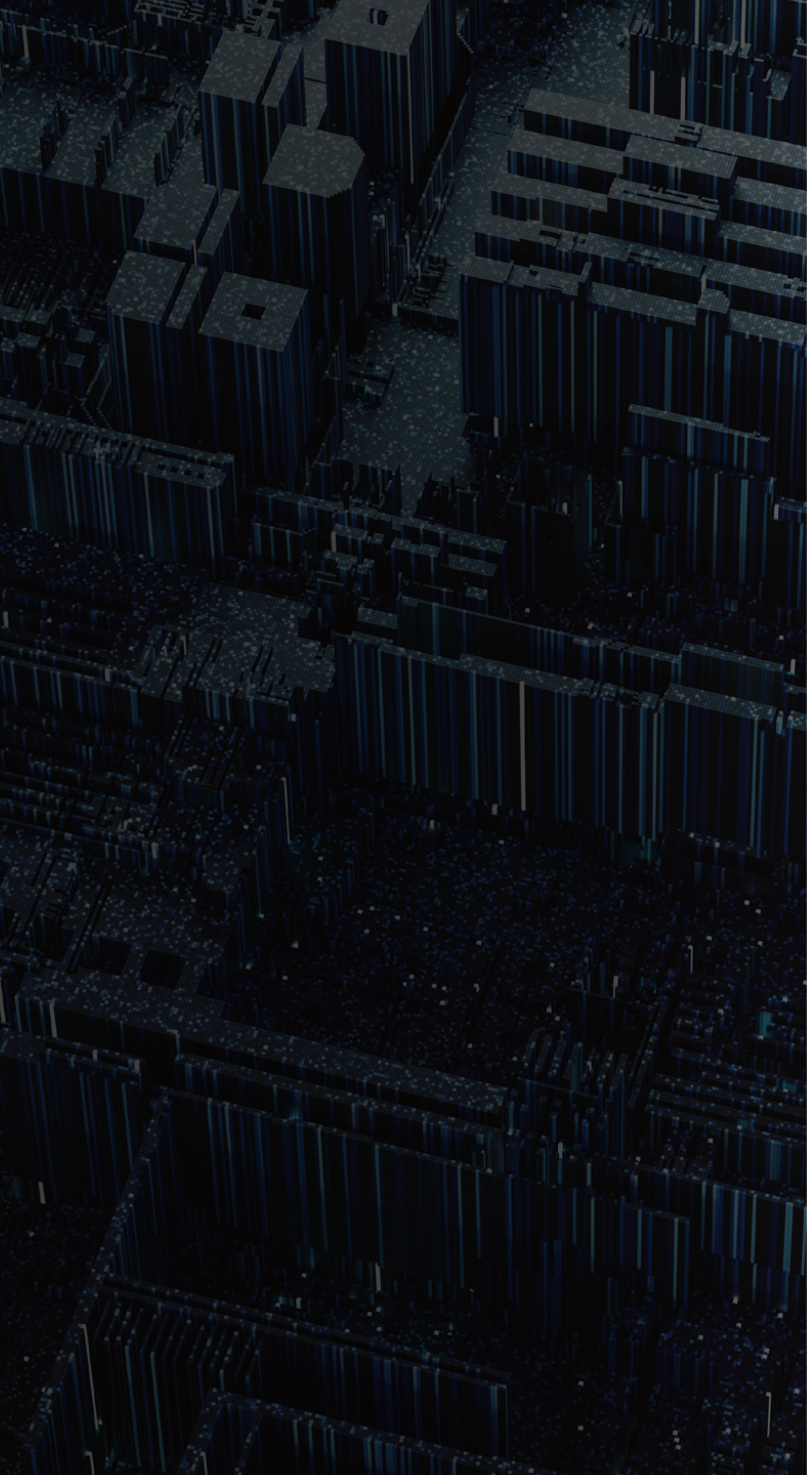
Another thing to consider here is that it isn't about trying to defend everything. It's about understanding where your critical data and systems reside, minimizing your "unknown unknowns," and then ensuring the right amount of investment is made in those areas first.

At CyberProof, we approach risk modeling using a top-down approach where the key question is: What are the primary threats to your business? A top-down approach defining the magnitude of attack and focusing on the top two to three attack scenarios is critical to making it practical.

Based on that information, we facilitate a business-oriented prioritization of your investment in detection and response. To ensure you spend optimally, we break down risk into distinct categories:

Pre-breach – This is what you can do before a breach: Ensure you have the right technologies to protect yourself, manage vulnerabilities, and track a constantly morphing threat environment.

Post-breach – This is what you can do ahead of time to prepare for an attack: Identify how to detect, respond, and recover faster to lessen the impact on your business, operations, and reputation.



HOW TO PRIORITIZE VULNERABILITIES

ATTACK SURFACE MAPPING

Start by creating a comprehensive model of your infrastructure that gives you full context to see and understand your attack surface in a single view.

Using the Skybox platform together with the CyberProof Defense Center gives you the ability to aggregate and normalize data from networking, security and operational technologies, including:

- Hybrid network infrastructure and security controls
- Asset repositories
- Vulnerabilities and security weaknesses
- Threat intelligence feeds
- Security policies

> **Attack simulation shows you how your network and security controls would perform against real-world attack scenarios.**

The platform dynamically analyzes millions of data points from these sources, using multiple perspectives to provide clear and actionable insights for your organization's security.

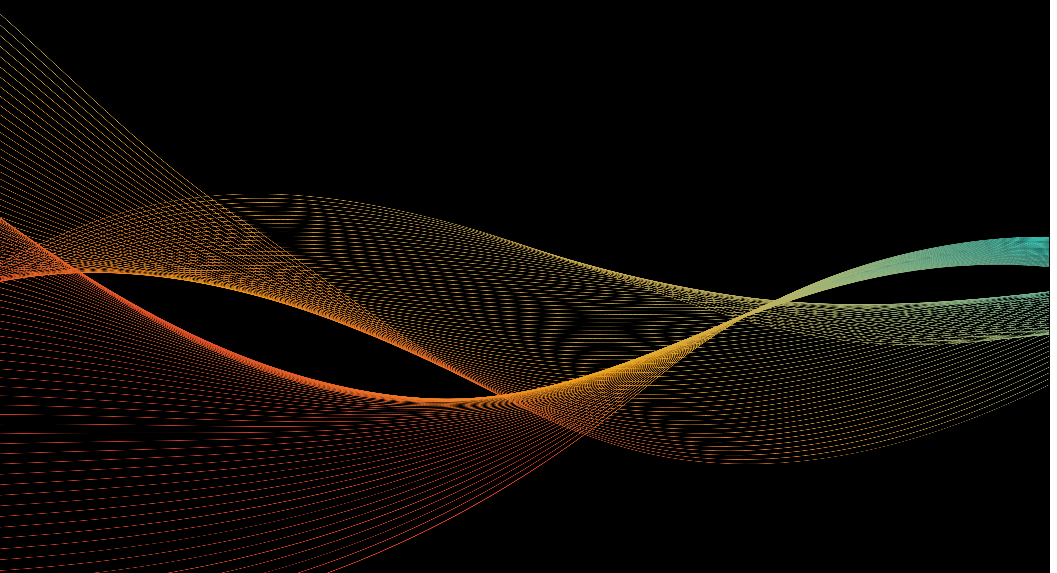
Skybox uses a wide range of sources, including asset and patch management systems and network devices, to assess vulnerabilities without requiring a scan. It can also collect, centralize and merge data from multiple scanners to give you the most accurate vulnerability assessments on demand.

Context is added to vulnerability data via Skybox's threat intelligence feed, which delivers information from the Skybox® Research Lab on vulnerability details, threat intelligence and remediation options. Data is further contextualized by correlating it to a model of your hybrid network topology, security controls and assets.

ATTACK SIMULATION

Attack simulation shows you how your network and security controls would perform against real-world attack scenarios. Finding your weaknesses before the attackers do and learning how to better protect your most critical assets will keep you one step ahead.

Penetration tests, whilst valuable, give you a "point-in-time" view. Skybox gives you the ability to continuously understand how vulnerable you are to attack from a hacker's viewpoint – showing you ways your security controls could be bypassed and vulnerabilities that could be exploited without the disruption or expense of a full penetration test.



PRIORITIZED AND ACTIONABLE GUIDANCE

The reality of vulnerability testing regimes means that very often the outputs result in a long list of remediation activities that take too long to carry out. Quite rightly, the focus is always on critical and high severity issues, with medium and low risk issues largely being consigned to an increasing technical debt. The challenges when it comes to remediation activity are three-fold:

1. Are all the critical and high severity issues going to cause you problems and are you focused on fixing things that, in reality, are unlikely to cause problems in the real world?

2. Do you really have time to manage the technical debt associated with medium and low risk issues to the point where you perhaps miss something that could become critical or high in the future?

3. Do you have a streamlined or automated process in place for communicating those risk issues to the various stakeholders involved in remediation?

> **By understanding your attack surface combined with continuous breach simulation from one platform provides a real-world, consistent and configurable single pane of glass view of your vulnerabilities.**

Wouldn’t it be good if your vulnerability remediation program was an ongoing and iterative process, providing you with the ability to deal with a smaller number of fixes but doing it more often - rather than trying to work through a long cumbersome list?

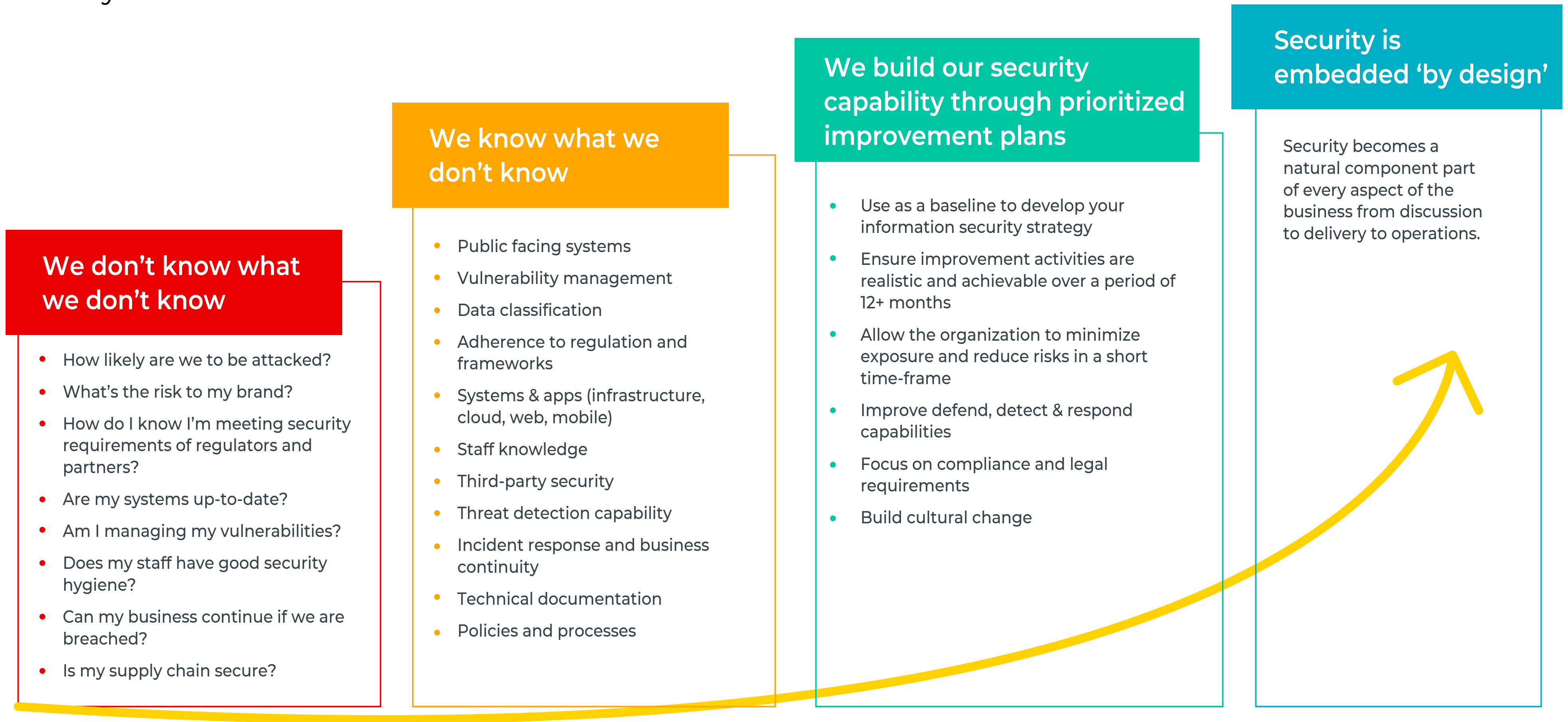
By understanding your attack surface combined with continuous breach simulation, all from one platform, provides a real-world, consistent and configurable view of your vulnerabilities. It delivers built-in risk scoring to give you a straightforward way to understand your current risk levels using a single pane of glass and then measure risk reduction efforts over time.

Skybox risk scores are themselves fully customizable so you can ensure they reflect risks relevant to your organization and can be applied to vulnerabilities, assets and asset groups so you can view risk from the perspective that makes the most sense for you and your team.

Using this platform along with relevant consulting services, CyberProof can provide you with a prioritized remediation process. CyberProof uses the right balance of automated and human input, and guidance that enables you to focus on the exposed vulnerabilities as well as those actively exploited in the wild and where you need to build compensating controls. And because of CyberProof's network insight, remediation options aren’t limited to just patching; you can be informed of IPS signatures and help plan network–based changes that cut off vulnerable assets from attack paths.

GROWING YOUR SECURITY MATURITY

Developing a mature security posture involves a four-step process – and requires continuous assessment and ongoing improvement in order to shift your organization from its initial starting point and reach full security readiness:



We don't know what we don't know

- How likely are we to be attacked?
- What's the risk to my brand?
- How do I know I'm meeting security requirements of regulators and partners?
- Are my systems up-to-date?
- Am I managing my vulnerabilities?
- Does my staff have good security hygiene?
- Can my business continue if we are breached?
- Is my supply chain secure?

We know what we don't know

- Public facing systems
- Vulnerability management
- Data classification
- Adherence to regulation and frameworks
- Systems & apps (infrastructure, cloud, web, mobile)
- Staff knowledge
- Third-party security
- Threat detection capability
- Incident response and business continuity
- Technical documentation
- Policies and processes

We build our security capability through prioritized improvement plans

- Use as a baseline to develop your information security strategy
- Ensure improvement activities are realistic and achievable over a period of 12+ months
- Allow the organization to minimize exposure and reduce risks in a short time-frame
- Improve defend, detect & respond capabilities
- Focus on compliance and legal requirements
- Build cultural change

Security is embedded 'by design'

Security becomes a natural component part of every aspect of the business from discussion to delivery to operations.

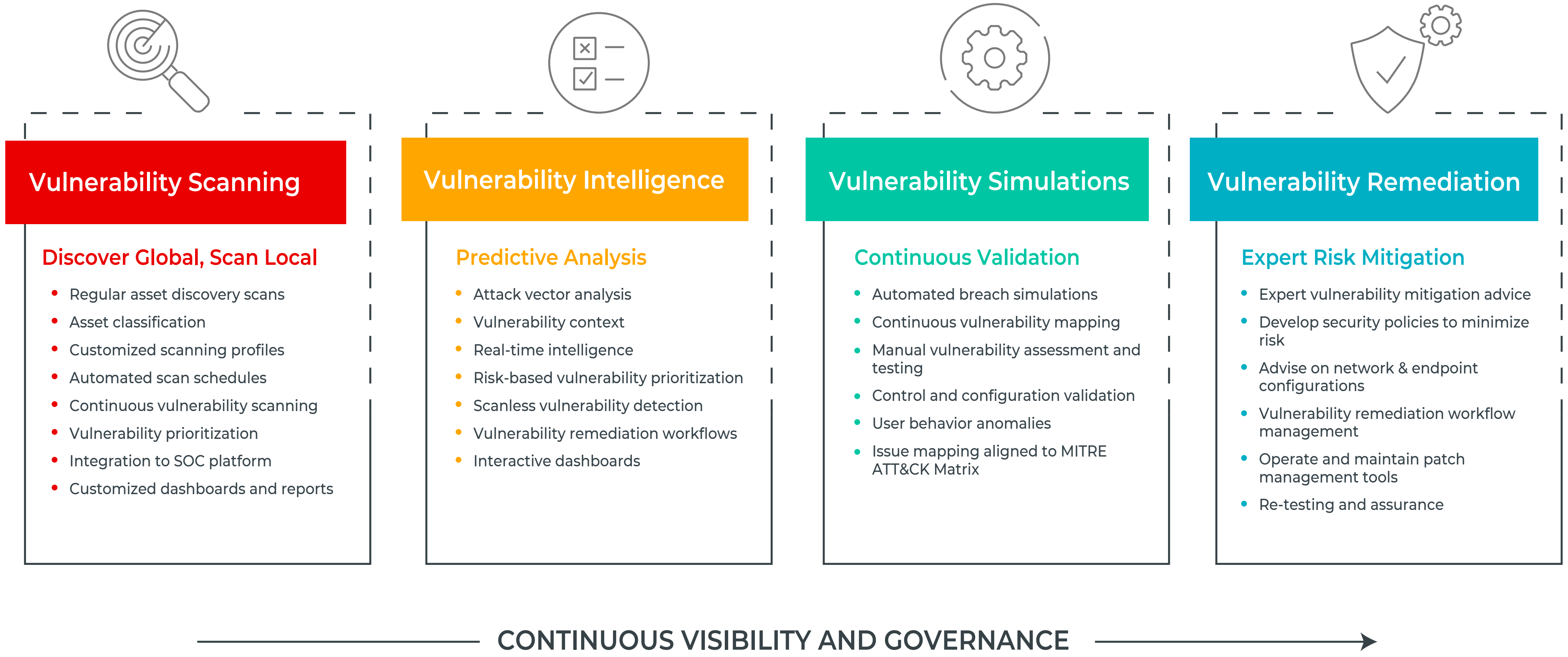
Good risk-based vulnerability management is a thread that runs through this approach and serves to continuously underpin your knowledge of where to spend time, money and effort in building overall security enhancement and maturity.

A THREAT-CENTRIC APPROACH TO VULNERABILITY MANAGEMENT

A threat-centric approach to vulnerability management helps you get an accurate view of your risk exposure at all times, helping to reduce the chances of a successful attack:

- **Attack Surface Mapping and Discovery –** Visualize attack surface and infrastructures to detect exposed and exploitable vulnerabilities
- **Vulnerability Intelligence –** Enrich vulnerability information with more context, i.e., exploitability, ratings, impact, trends, etc.
- **Breach Simulations –** Continuously test and validate infrastructure against control effectiveness and multiple exploits
- **Vulnerability Prioritization –** Risk-based approach utilizing information gathered during intelligence and breach simulation phase
- **Remediation and Validation –** Cost-effective and low-risk solution to mitigate vulnerabilities & continually validate effectiveness

> **A threat-centric approach to vulnerability management helps you get an accurate view of your risk exposure at all times, helping to reduce chances of a successful attack.**



Vulnerability Scanning

Discover Global, Scan Local

- Regular asset discovery scans
- Asset classification
- Customized scanning profiles
- Automated scan schedules
- Continuous vulnerability scanning
- Vulnerability prioritization
- Integration to SOC platform
- Customized dashboards and reports

Vulnerability Intelligence

Predictive Analysis

- Attack vector analysis
- Vulnerability context
- Real-time intelligence
- Risk-based vulnerability prioritization
- Scanless vulnerability detection
- Vulnerability remediation workflows
- Interactive dashboards

Vulnerability Simulations

Continuous Validation

- Automated breach simulations
- Continuous vulnerability mapping
- Manual vulnerability assessment and testing
- Control and configuration validation
- User behavior anomalies
- Issue mapping aligned to MITRE ATT&CK Matrix

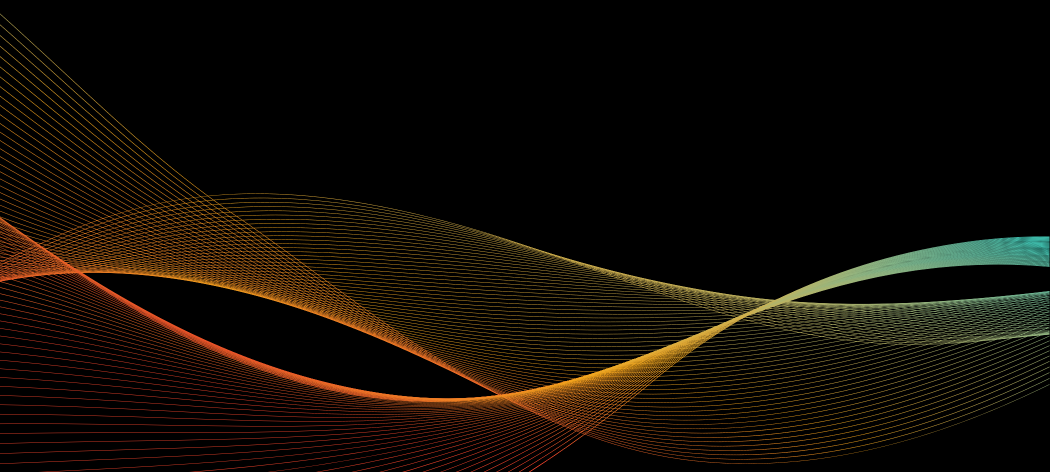
Vulnerability Remediation

Expert Risk Mitigation

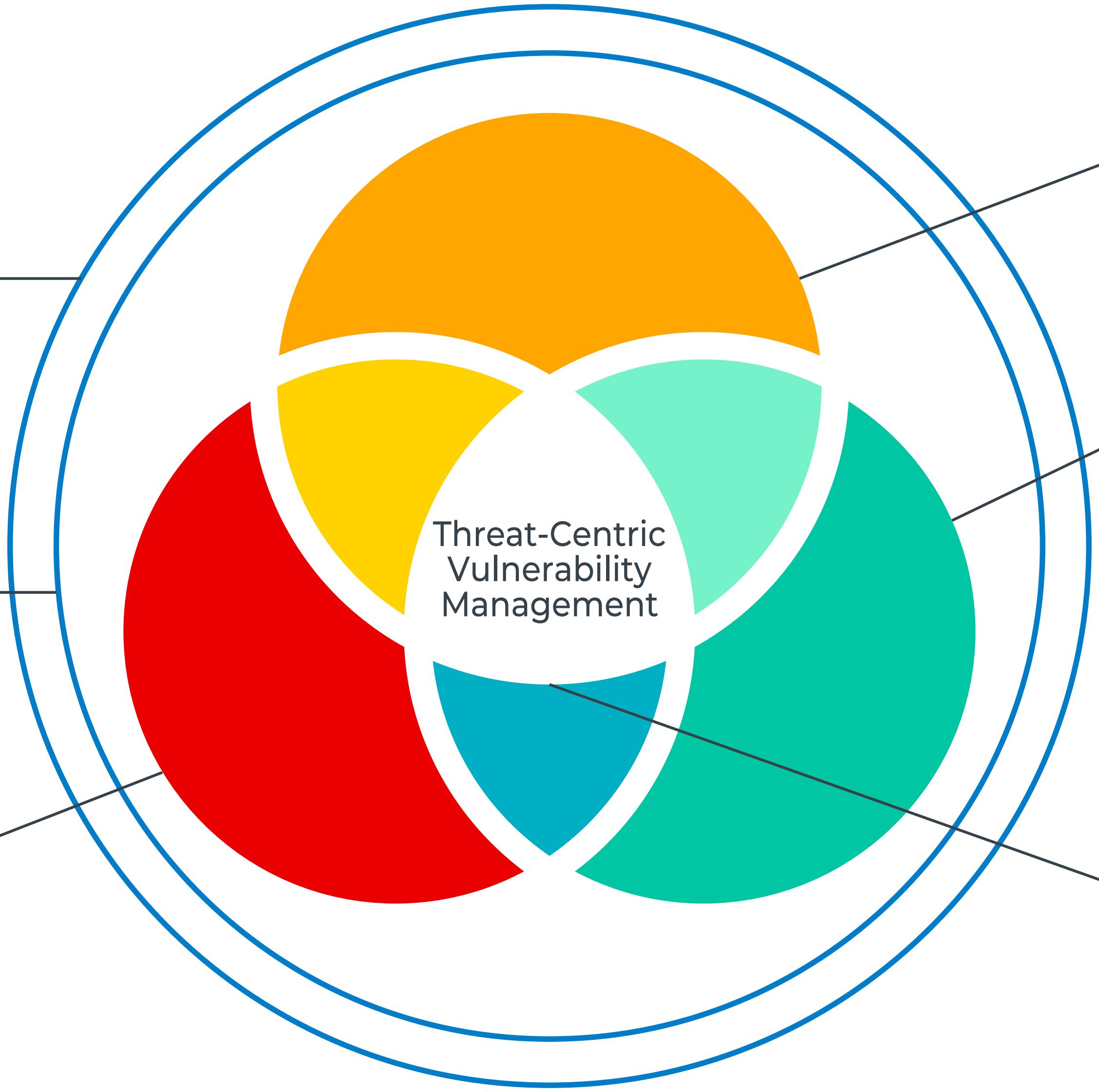
- Expert vulnerability mitigation advice
- Develop security policies to minimize risk
- Advise on network & endpoint configurations
- Vulnerability remediation workflow management
- Operate and maintain patch management tools
- Re-testing and assurance

CONTINUOUS VISIBILITY AND GOVERNANCE

Here is an example of how a threat-centric approach to vulnerability management was able to sift through 1.3 MILLION IDENTIFIED VULNERABILITIES and narrow down to 16 CRITICAL VULNERABILITIES for remediation.



CASE STUDY – FINANCIAL SERVICES



Identified Vulnerabilities

Total Identified: 1.3m
Vulnerability Detector
& Vulnerability Scanner
Potential Threat

Unique Vulnerabilities

Total Identified: 69,000
Advanced Analytics
Potential Threat

Available Exploits

Total Identified: 3055
Real-Time
Threat Intelligence
Imminent Threat

Correlate to CVSS

Total Identified Critical: 416,456
CVSS Scoring
Potential/Imminent Threat

Exposure

Total Identified: 141
Network Monitoring and
Attack Vector Analytics
Imminent Threat

Biggest Risks

Total Identified: 16
Vulnerability Control
Prioritization Center
Imminent Threat

CONCLUSION

Organizations looking to protect themselves from cyber threats get bogged down with heavy security investments and multi-layered tools that frequently generate a lot of noise without necessarily leading to a successful reduction in risk. Traditional management methods are focused on severity rather than risk, and don't prioritize vulnerabilities in alignment with threat exposure and risk.

Successful risk management requires mapping out where your critical data and systems reside and making sure the investment is made in those places first.

CyberProof and Skybox work with you in conducting risk modeling that's focused on the primary threats to your business and allows you to reduce risk while optimizing spend. The first step in this process involves creating a comprehensive model of your infrastructure, and that's where Skybox comes in – giving you the ability to aggregate and normalize data from networking, security, and operational technologies and providing the context that allows you to prioritize where to place the greatest investment. Together, CyberProof and Skybox allow you to develop a threat-centric approach to vulnerability management that successfully reduces the chances of attack.

If you would like to speak to a cyber security expert to find out how CyberProof's integration with Skybox can help you successfully improve your cyber security posture and protect your organization from cyber attacks, contact us today!

ABOUT CYBERPROOF

CyberProof is a security services company that helps organizations to intelligently manage incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact.

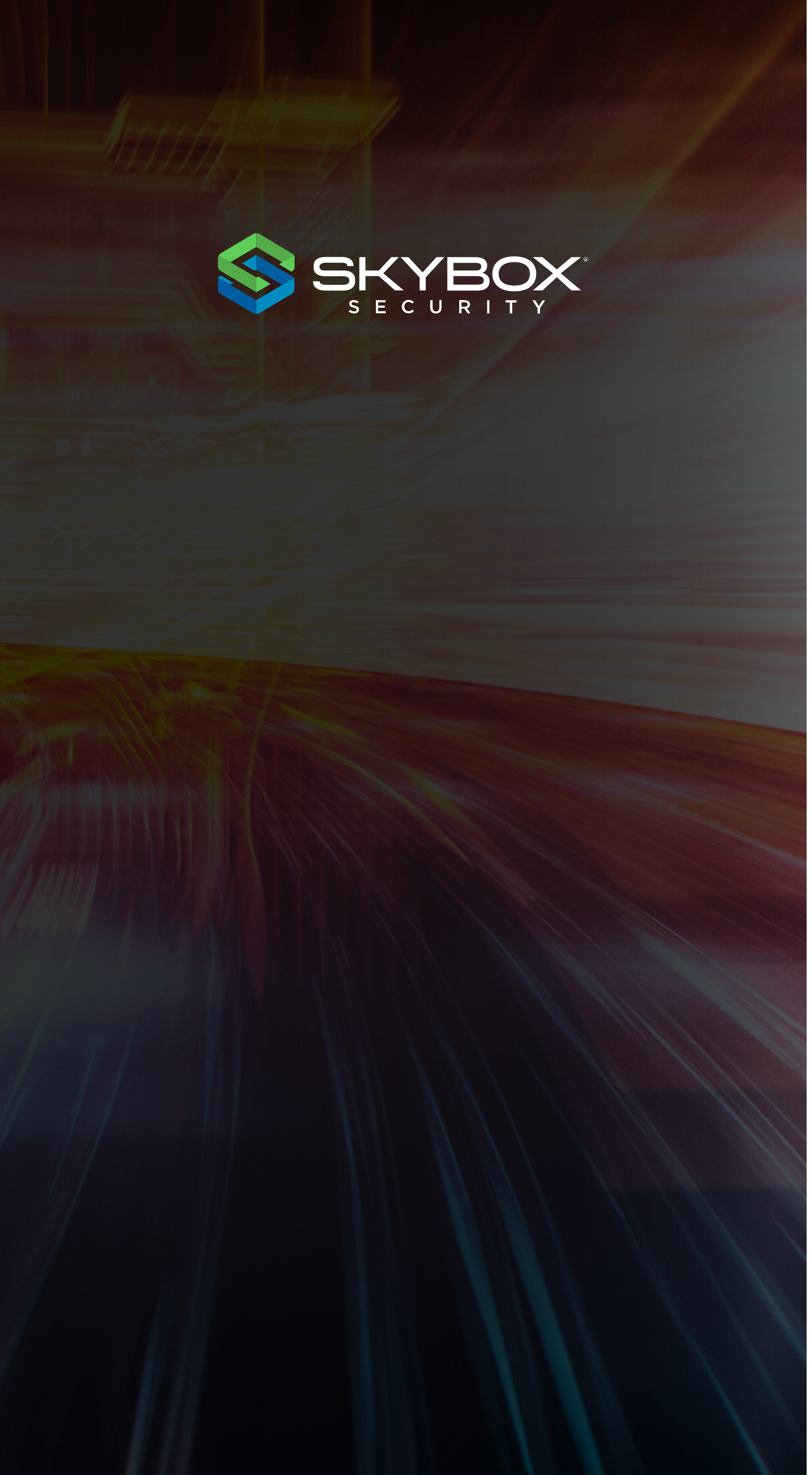
SeeMo, our virtual analyst, together with our experts and your team automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts to prioritize the most urgent incidents and proactively identify and respond to potential threats.

We collaborate with our global clients, academia and the tech ecosystem to continuously advance the art of cyber defense.

CyberProof is part of the UST Global family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services. For more information, see: www.cyberproof.com

LOCATIONS

Aliso Viejo | Barcelona | London | Singapore | Tel Aviv | Trivandrum



ABOUT SKYBOX

At Skybox Security, we provide you with cyber security management solutions to help your organization innovate rapidly and with confidence. We get to the root of cyber security issues, giving you better visibility, context and automation across a variety of use cases. By integrating data, delivering new insights and unifying processes, you're able to control security without restricting operational agility. Skybox's comprehensive solution unites different security perspectives into the big picture, minimizes risk and empowers security programs to move to the next level. With obstacles and complexities removed, you can stay informed, work smarter and drive your organization forward, faster.

For more information, please visit www.skyboxsecurity.com