Visão geral

A Cyber Quant fornece um painel centralizado e estratégico de risco cibernético da sua organização por meio de sua avaliação de risco contextual e recursos de integração de tecnologia.

A Cyber Quant ajuda a responder a perguntas críticas de negócios

- Você sabe quais falhas de segurança representam o maior risco para o seu negócio?
- Qual é o impacto financeiro das violações de segurança na sua organização?
- Como o cenário exclusivo de ameaças cibernéticas da minha organização pode ser incorporado às avaliações de risco?
- Como sua empresa e os líderes de segurança determinam onde investir?

Cyber Quant utiliza uma abordagem de quatro etapas

Cenário de ameaças

Avalie as informações demográficas sobre sua organização para personalizar o impacto do cenário de ameaças para sua empresa com base na localização, no setor e no tamanho da organização.

Questionários

Analise as respostas a questionários personalizados e dinâmicos para identificar a profundidade do risco, o alinhamento aos padrões de segurança e a adequação a outras estruturas importantes do setor.

Análise técnica

Valide o alinhamento das configurações de segurança do seu sistema com suas políticas e as práticas recomendadas do setor, avaliando com segurança mais de 60 tecnologias que abrangem sistemas operacionais, plataformas de nuvem, firewalls, aplicativos de segurança e muito mais.

Avaliar e agir

- ✓ Consolide automaticamente as informações acima para criar painéis e relatórios baseados em funções
- ✓ Calcule a pontuação de risco cibernético e o impacto financeiro de possíveis eventos cibernéticos para sua organização
- ✓ Simule cenários para identificar ações comerciais e técnicas prioritárias com base no ROI das perspectivas de impacto financeiro e redução de riscos

Proposta de valor da Cyber Quant para as principais partes interessadas

CISO

- ✓ Desenvolve estratégias para abordar falhas na segurança e a postura de risco da organização ao longo do tempo
- ✓ Ajusta roteiros de TI e segurança com base em lacunas e avaliações de maturidade tangíveis
- ✓ Justifica as necessidades orçamentárias com ROI quantificado e análises hipotéticas
- ✓ Utiliza a análise de risco quantificada para avaliar a cobertura de seguro cibernético

O Conselho e o CEO

- ✓ Supervisionam relatórios automatizados quantificados e dados de risco cibernético em tempo real por meio de painéis
- ✓ Conduzem com facilidade análises de ROI e hipotéticas antes de qualquer atividade que envolva risco cibernético

Compliance Officer

- ✓ Avalia previamente a qualificação quanto a certificações padrão do setor
- ✓ Aproveita o histórico da avaliação da Cyber Quant para destacar o foco da organização em segurança cibernética e gerenciamento de riscos

CRO

- ✓ Comunica o risco cibernético usando termos que sejam facilmente compreendidos em toda a empresa
- ✓ Mantém a visibilidade do risco cibernético com granularidade por ativos comerciais, divisão e níveis de pilha de tecnologias

CFO

- ✓ Avalia rapidamente os riscos cibernéticos de alienações e atividades de fusão e aquisição
- ✓ Fornece orientação sobre priorização do orçamento controlada por insights de risco quantificados

Tipos de avaliação

A Cyber Quant oferece flexibilidade para utilizar vários elementos para conduzir cinco tipos diferentes de avaliação, desde uma verificação rápida em menos de uma hora até uma avaliação completa que dura algumas semanas. É possível agregar múltiplas avaliações para entender o risco em diferentes departamentos ou em um portfólio de empresas.
Avaliações periódicas permitem que você monitore as tendências em sua postura cibernética para avaliar os contínuos investimentos em proteção contra ameaças cibernéticas e o cenário dinâmico de ameaças. A Cyber Quant fornece efetivamente um painel centralizado e estratégico de risco cibernético da sua organização.

Questionários

Com base na Cyber Quant Security Framework (CQSF) com 47 categorias de controle, a *plataforma oferece flexibilidade no âmbito de avaliação adequada para as necessidades do seu negócio.*

	CQ Um	CQ Dois	CQ Três	CQ Quatro	CQ Cinco
Profundidade do questionário	15 Perguntas	24 Perguntas	47 Perguntas	188 Perguntas	544 Perguntas
Análise do cenário de ameaças (Cyber Insights)	Médio	Médio	Médio	Alto	Alto
Análise técnica (CyMA)	Verificações de tecnologia da CQ Essentials		Amb	Verificações de tecnologia do CQ Essentials	
Avaliação para estruturas do setor	Não habilitada		Disponível	Disponível	Disponível
Impacto financeiro e risco	Sim	Sim	Sim	Sim	Sim
Simulação e análises hipotéticas	Não habilitada		Habilitado	Habilitado	Habilitado
Recomendações de ações de correção	Básico	Básico	Ambos	Detalhado	Detalhado
Nível de confiança	Inicial	Baixo	Médio	Moderada mente	Alto

As avaliações da Cyber Quant que usam os Questionários Cyber Quant Essentials podem ser ainda mais aprimoradas com questionários auxiliares para aumentar a avaliação de várias estruturas e padrões, como:

- ✓ NIST CSF 1.1
- ✓ ISO 27002:2022
- ✓ PCI-DSS 4.0
- ✓ CIS Controls 7-8
- ✓ HIPAA
- ✓ CQSF

Cenário de ameaças

Todos os usuários da Cyber Quant terão informações personalizadas do cenário de ameaças com base no ambiente da organização incluídas automaticamente em suas avaliações. Com base no tipo de avaliação, as informações personalizadas do cenário de ameaças são definidas da seguinte maneira:

Cyber Quant Lite: os ambientes são criados com uma *série de perguntas*. Essas perguntas determinam os ativos de negócios, as tecnologias que os armazenam e o setor e a localização específicos do ambiente.

Cyber Quant Essentials: para cada ambiente, os *profissionais de risco* definem os ativos comerciais armazenados, as tecnologias que armazenam e processam esses ativos, bem como o setor e a localização específicos do ambiente.

Análise técnica

Cyber Quant Lite: os profissionais de risco que realizam avaliações do Cyber Quant Lite podem contar com as seguintes integrações para aumentar e melhorar os resultados das avaliações. Essas verificações podem ser concluídas passivamente com interação mínima do usuário.

- ✓ APIVoid
- ✓ WhatIsMy Browser
- ✓ MyToolbox
- ✓ RiskRecon

Cyber Quant Essentials: os profissionais de risco que realizam as avaliações do Cyber Quant Essentials podem utilizar o módulo Cyber Maturity Analysis (CyMA) para obter uma compreensão mais completa da maturidade dos seus controles. Nesse módulo, é possível importar arquivos de configuração técnica de mais de 60 tecnologias. Alguns exemplos notáveis incluem:

- ✓ AWS
- ✓ Azure
- ✓ Check Point
- ✓ Fortigate
- ✓ McAfee
- ✓ Microsoft Active Directory

Os dois tipos de avaliação têm acesso à integração do Cyber Front para validar e melhorar as classificações de maturidade de controle.

Avaliar e agir

Cyber Quant Lite: visão holística do risco cibernético da organização e do impacto financeiro correspondente para a organização ou o departamento avaliado.

Cyber Quant Essentials: um painel abrangente e interativo está disponível para usuários que optam por essa opção. Além disso, um mecanismo de simulação e vários relatórios estão disponíveis para articular o risco e o impacto financeiro em vários contextos.

A plataforma Cyber Quant capacita a maturidade para padrões e estruturas e avaliações de risco cibernético para atender organizações de pequeno e grande porte

	Avaliação de maturidade		*Avaliação de risco cibernético*	
	Cyber Quant Assessor	**Cyber Quant Lite**	**Cyber Quant Essentials**	**Cyber Quant Ecosystem**
Profundidade dos questionários	• CQSF • NIST CSF • CIS • CRI • PCI DSS • ISO 27002 • GDPR • Brazil Privacy Framework • Outros	• 15 / 24 / 47 perguntas	• 47 / 188 / 500+ perguntas • Combine com o CQ Assessor	• Avalie várias organizações (empresas, departamentos, locais) • Combine várias avaliações Essentials e Lite em uma única visão
Análise técnica	• Verificações passivas [1] • Verificações interativas/integradas [2]	• Verificações passivas	• Verificações passivas [1] • Verificações interativas/integradas[2]	• Verificações passivas[1] • Verificações interativas/integradas[2]
Análise do cenário de ameaças (Cyber Insights [3])	• Combine com a versão Essentials para análise do cenário de ameaças	• Análise baseada no Mastercard Cyber Insights no cenário de ameaças da organização	• Análise baseada no Mastercard Cyber Insights com análises e relatórios adicionais sobre invasores e métodos de ataque	• Combinação do Cyber Insights em todo o ecossistema
Análise de impacto e risco financeiro	• Combine com a versão Essentials para análise de impacto e risco financeiro	• Incluído	• Incluído	• Incluído
Simulação e análises hipotéticas do ROI	• Emparelhe com a versão Essentials para simulações de ROI	• Não incluído	• Incluído	• Incluído
Painéis e relatórios	• Nível intermediário	• Nível baixo	• Nível de detalhe • Avaliar serviços compartilhados	• Painéis individuais e agregados • Priorização entre organizações
Orientação de implementação	• Serviços de consultoria disponíveis	• Serviços de consultoria para análises agregadas para compras em massa	• Serviços de consultoria disponíveis	• Serviços de consultoria disponíveis

1. Verificações passivas são executadas em segundo plano, examinando a segurança do sistema operacional, do navegador, do servidor de e-mail e do site da organização. Elas usam versões leves de soluções da Mastercard, como o Risk Recon e o Cyber Front, além de soluções de terceiros. Pode ser necessário licenciamento adicional.
2. Verificações interativas/integradas da infraestrutura e das tecnologias de aplicação da organização. Elas baseiam-se nas integrações da plataforma com mais de 60 tecnologias de rede, servidor, aplicação, banco de dados e segurança. Pode ser necessário licenciamento adicional para o Risk Recon e o Cyber Front.
3. Está incluída a análise do cenário de ameaças do Cyber Insights para avaliação de risco cibernético da Cyber Quant. É necessária uma licença adicional.

Cyber Insights

Visão geral

As principais partes interessadas ganham visibilidade no cenário de ameaças da sua organização, permitindo que tomem decisões proativas sobre onde investir e quais ações priorizar.

As avaliações de risco cibernético são tradicionalmente centradas no perímetro, ignorando o cenário dinâmico de ameaças adversárias que a organização enfrenta e que é afetado por fatores geopolíticos, econômicos e tecnológicos. Embora a ISO 27002 agora exija que as organizações coletem e analisem a inteligência de ameaças cibernéticas, apenas 30% a incluem como um componente essencial de seu modelo operacional de segurança cibernética. A avaliação do cenário de ameaças fornece visibilidade total das ameaças atuais e futuras previstas, permitindo a tomada de decisões estratégicas e a melhoria da resiliência da segurança cibernética.

Principais benefícios do Cyber Insights

- Maior visibilidade em ameaças externas e fatores de impacto
- Utilização eficiente de recursos para controles alinhados com precisão ao cenário de ameaças
- Redução da probabilidade de um ataque com estratégia de mitigação informada por previsões de tendências de ameaças acionáveis
- Avaliação da resiliência de segurança que identifica áreas em risco de ameaças atuais e emergentes

Como o Cyber Insights funciona

O Cyber Insights fornece rapidamente inteligência estratégica sobre ameaças usando milhares de fontes qualificadas por meio das quatro etapas a seguir:

1

Coleta de dados

A Mastercard integra e gerencia milhares de fontes de inteligência da web claras, profundas e escuras que são rastreadas e processadas pelo sistema Cyber Insights.

2

Processamento de dados

O sistema contém o tesauro multilíngue da Mastercard, o qual consiste em dezenas de milhares de entidades e sinônimos. Cada item de inteligência é processado usando uma ferramenta de análise de texto granular.

3

Análise estatística

O sistema combina e agrega repetições da mesma permutação de entidades, criando estatísticas para cada uma por meio da plataforma Cyber Insights.

4

Resultado

A interface SaaS baseada em consulta gera:

- ✓ Tendências cibernéticas e análise do cenário de ameaças
- ✓ Padrões e previsões de ameaças
- ✓ Relatórios de inteligência personalizados

Vantagem competitiva

Segurança como modelo de negócios

A Mastercard tem experiência prática na proteção de petabytes de seus próprios dados com a estrutura Cyber Insights.

Insights personalizados

A Mastercard analisa os riscos, levando em consideração o cenário de ameaças personalizado para a organização de um cliente.

Ajustes dinâmicos para novas ameaças

Nossa metodologia permite levar em conta o ambiente em constante mudança das ameaças cibernéticas e responder dinamicamente a novos vetores de ataque.

Cyber Quant

Quantificação de risco e impacto financeiro

A Cyber Quant é uma ferramenta de quantificação de risco cibernético que utiliza inteligência estratégica de ameaças aliada a avaliações precisas de maturidade de controle para identificar, avaliar e quantificar sistematicamente os riscos para os ativos de negócios de uma organização em diversas granularidades. Dois resultados importantes da avaliação são a pontuação de risco e o valor da faixa de impacto financeiro para a organização em decorrência de eventos adversos relacionados à segurança cibernética.

Pontuação geral de risco

Com base no seu cenário de ameaças e nos recursos de defesa

16,2 milhões de dólares

Potencial perda financeira

Total geral agregado com base no seu tipo de setor e localização

À medida que você insere informações demográficas, preenche o questionário e carrega arquivos de configuração técnica, a plataforma Cyber Quant usa um processo de nove etapas para entender a organização, gerar insights para correção e calcular o impacto financeiro com base nos custos associados da organização.

1. **Avaliação da maturidade de controle**
2. **Nível da atividade de ameaça**
3. **PoS de métodos de ataque**
4. **Invasor/Níveis de ameaça de ataque**
5. **Nível de risco dos ativos de negócios**
6. **Nível de risco do ambiente**
7. **Nível de risco da organização**
8. **Prioridades de correção**
9. **Cálculo do impacto financeiro**

Etapa 1: Avaliação da maturidade de controle

Os controles mantêm a adesão baseada em parâmetros às práticas recomendadas, às políticas e aos procedimentos estabelecidos pela organização, pelos padrões ou pelo fornecedor do produto para proteger os ativos de negócios. A Cyber Quant utiliza informações humanas e de máquina para atingir um alto nível de confiabilidade ao avaliar a maturidade da postura de segurança.

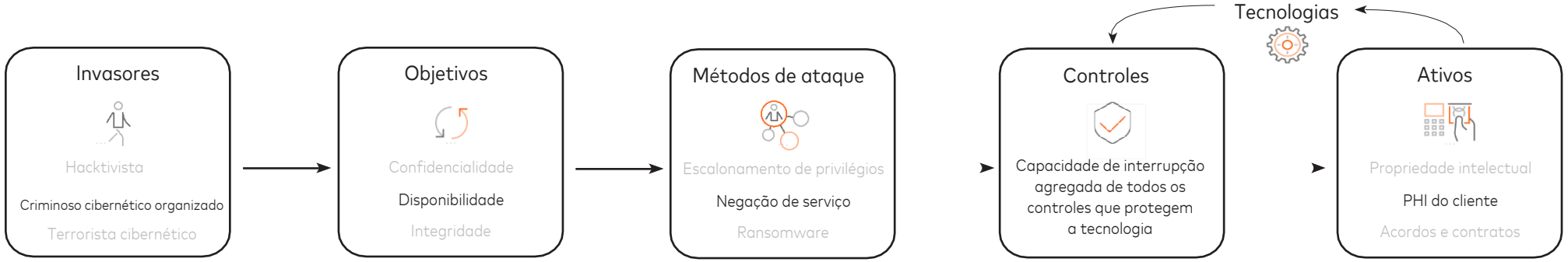
Etapa 2: Nível da atividade de ameaça

O cenário de ameaças à segurança cibernética é compreendido por meio de um modelo estratégico de inteligência de ameaças, adaptado à localização e ao setor da organização. Os métodos, recursos e alvos preferenciais dos agentes de ameaças são examinados e avaliados usando inteligência de todo o mundo, juntamente com a inteligência de propriedade da Mastercard.

Etapa 3: Probabilidade de sucesso (PoS) dos métodos de ataque

Depois que o contexto interno e externo da organização é compreendido com os insights de Maturidade de controle e Nível da atividade de ameaça, a Probabilidade de sucesso (PoS) de cada método de ataque é calculada. PoS é a probabilidade de um método de ataque ter sucesso com base em como ele se compara a um vetor defensivo de controles e seu poder defensivo.

Os métodos de ataque são selecionados com base nas habilidades e no objetivo do invasor.
Para atingir o ativo, o método de ataque deve superar os controles que o protegem.
Os controles que protegem o ativo dependem de quais tecnologias o ativo está armazenado.
É calculada uma PoS para cada possível cenário de ataque. Essa métrica é usada para entender quais ativos estão em maior risco, quais invasores ou métodos de ataque representam o maior risco e quais controles precisam de melhorias.



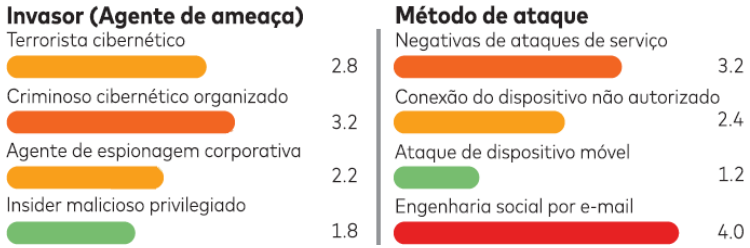
Cyber Quant

Quantificação de risco e impacto financeiro

2 Nível da atividade de ameaça | 3 PoS de métodos de ataque | **4 Invasor/Níveis de ameaça de ataque** | **5 Nível de risco dos ativos de negócios** | **6 Nível de risco do ambiente** | **7 Nível de risco da organização** | **8 Prioridades de correção** | **9 Cálculo do impacto financeiro**

Etapa 4: Invasor/Níveis de ameaça de ataque

Depois de entender a PoS de cada método de ataque em um único ativo, é possível agregar essas informações para cada ativo para calcular o risco de um único método de ataque. Da mesma forma, a PoS para todos os métodos de ataque usados por um invasor pode ser agregada para calcular o risco de um único invasor.



Etapa 5: Nível de risco dos ativos de negócios

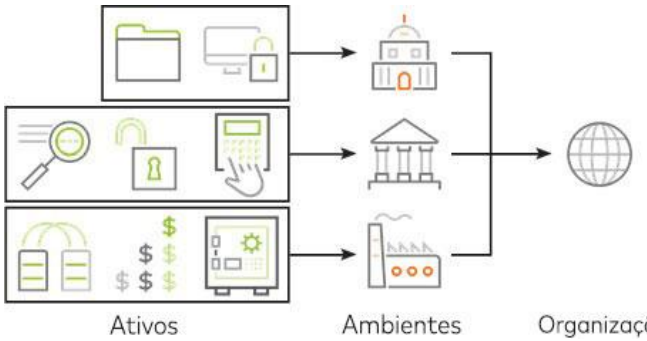
Para entender os ataques a um único ativo de negócios, a plataforma Cyber Quant agrega todos os riscos associados a esse ativo. Isso pode ser ainda mais detalhado pelo objetivo do invasor de entender o risco à confidencialidade, integridade e disponibilidade do ativo.

Etapa 6: Nível de risco do ambiente

Similar ao risco de ativos de negócios, a plataforma Cyber Quant agrega todos os riscos associados a todos os ativos em um ambiente para calcular o nível de risco do ambiente.

Etapa 7: Nível de risco da organização

Para obter uma visão de nível mais alto, a plataforma Cyber Quant agrega todos os riscos associados a todos os ambientes de uma organização para gerar o nível de risco da organização. Isso pode ser ilustrado no gráfico a seguir.



Etapa 8: Prioridades de correção

Com base nos dados gerados em todas as etapas anteriores, a Cyber Quant calcula uma métrica chamada importância de controle, que mede como a melhoria de um controle específico afetará o nível de risco do ambiente. Essa métrica determina a priorização das melhorias de controle para corrigir riscos.

Etapa 9: Cálculo do impacto financeiro

O impacto financeiro desses riscos é calculado usando métodos estatísticos juntamente com dados históricos. Esses dados podem ser usados para articular o risco cibernético à liderança ou a outros funcionários que não sejam necessariamente profissionais de segurança da informação.

Cyber Maturity Analysis - CyMA

O Cyber Maturity Analysis (CyMA) é um componente da Cyber Quant que permite validar e ampliar suas Avaliações da Cyber Quant. Basicamente, o CyMA é uma ferramenta para ajudar você a coletar e analisar:

- ✓ Dados sobre a eficácia do design com base em questionários conduzidos por profissionais de segurança da informação
- ✓ Dados sobre a eficácia operacional com base na análise de arquivos de configuração de várias tecnologias

Fluxo de trabalho do CyMA

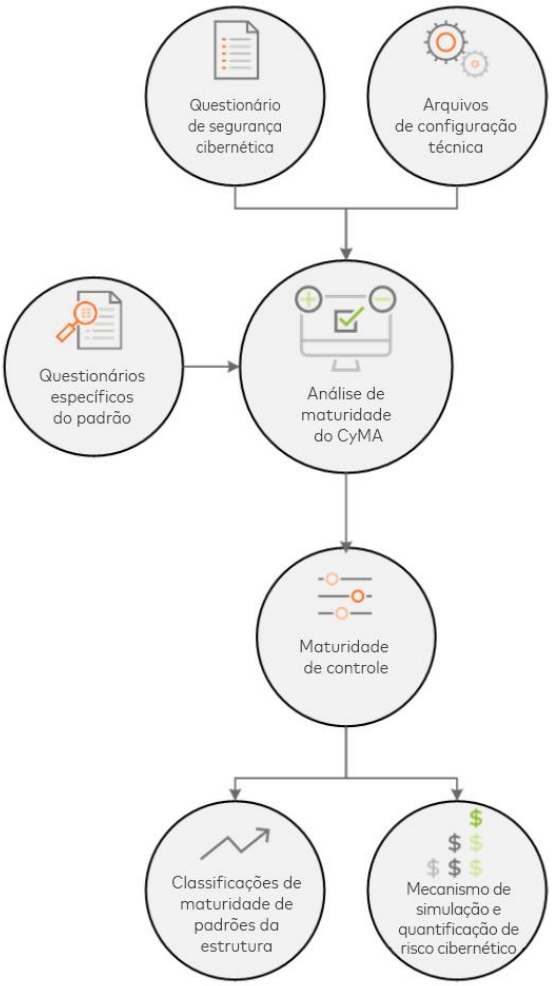
Para avaliar a maturidade de um ambiente, por padrão, a Cyber Quant usa uma lista de 47 controles. O valor exato pode mudar durante a análise da maturidade. Os controles são agrupados com base no padrão ou na estrutura selecionada.

Além disso, cada controle contém indicadores de maturidade coletados de avaliações técnicas de produtos e sistemas de segurança, bem como de questionários que fornecem uma avaliação completa do controle. A incorporação de dados de maturidade de padrões e estrutura de segurança enriquece ainda mais a avaliação de maturidade do controle.

Durante essa avaliação, podem ser necessárias várias amostras de endpoints e servidores. O CyMA está equipado para processar arquivos de configuração técnica de vários endpoints para apresentar uma linha de base para todo o ambiente.

Diferentemente do restante da plataforma Cyber Quant, o CyMA é instalado localmente. Isso faz parte da nossa estratégia de minimização de dados. O CyMA não carrega seus arquivos de configuração técnica para a plataforma Cyber Quant na nuvem, carregando apenas as classificações de maturidade de controle.

Enquanto o sistema host estiver conectado à Internet, o CyMA funcionará no Modo Online e continuará enviando classificações de maturidade dos controles para o painel da Cyber Quant, permitindo que o painel de risco atualize e ajuste continuamente o risco do ambiente. Mudanças nas classificações de maturidade afetarão a classificação de risco em toda a empresa e o impacto financeiro calculado do risco cibernético na organização, dependendo da postura de segurança atual.



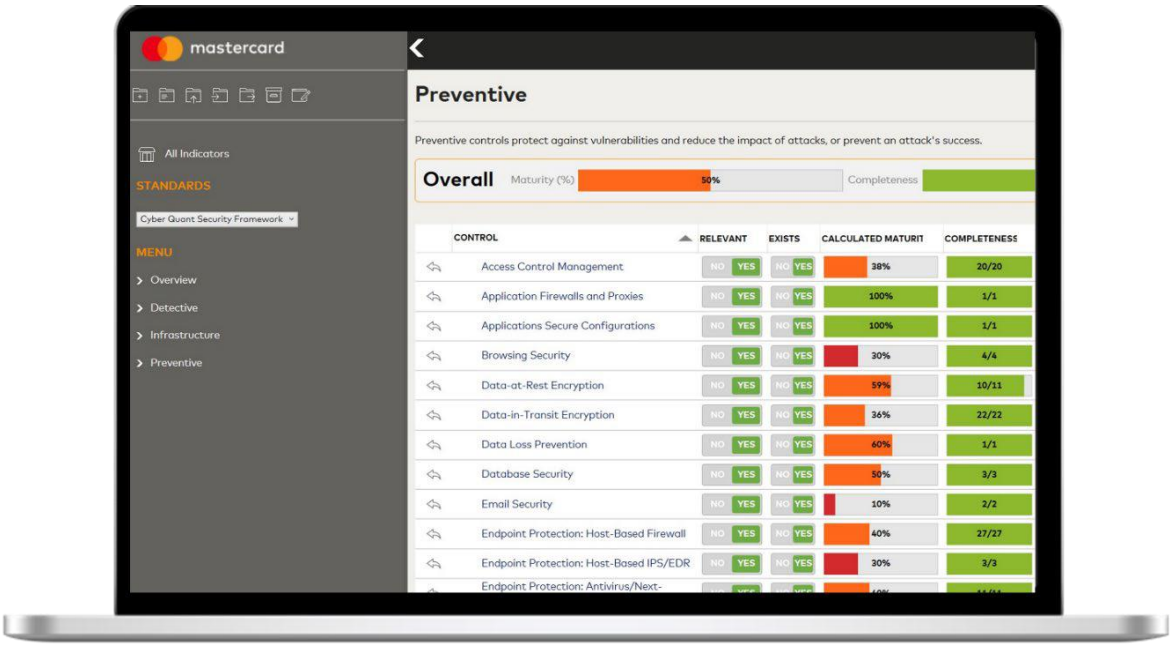
Cyber Maturity Analysis – CyMA

Compatibilidade de padrões

Por padrão, a plataforma Cyber Quant usa um padrão de propriedade chamado **Cyber Quant Security Framework**. Essa estrutura é baseada em diversos padrões e estruturas que formam os padrões e as estruturas de segurança do setor, como ISO 27002, NIST CSF e muito mais.

A Cyber Quant permite que os clientes realizem avaliações de maturidade de vários padrões e estruturas. O CyMA implanta questionários secundários na Cyber Quant para gerenciar isso, permitindo que indicadores específicos do padrão sejam adicionados ao cálculo. O sistema é altamente personalizável e diferentes padrões podem ser adicionados para atender às necessidades específicas da sua organização. O CyMA permite a análise de maturidade em relação a padrões como:

NIST CSF 1.1 | **ISO 27002:2022** | **PCI-DSS 4.0** | **CIS Controls 7-8** | **HIPAA**



Integrações de tecnologia

A validação é obtida importando arquivos de configuração técnica de mais de 60 tecnologias, comparando-os com indicadores de maturidade baseados em práticas recomendadas do ambiente e do setor. Para garantir a segurança dos dados da sua organização, essas atividades de processamento são realizadas no local.

Para garantir maior visibilidade nas tecnologias da informação, o CIS-CAT Pro Assessor foi incorporado ao CyMA com licença para uso. O CyMA utiliza relatórios do CIS-CAT Pro para verificar qualquer sistema na rede em relação a vários benchmarks do CIS.

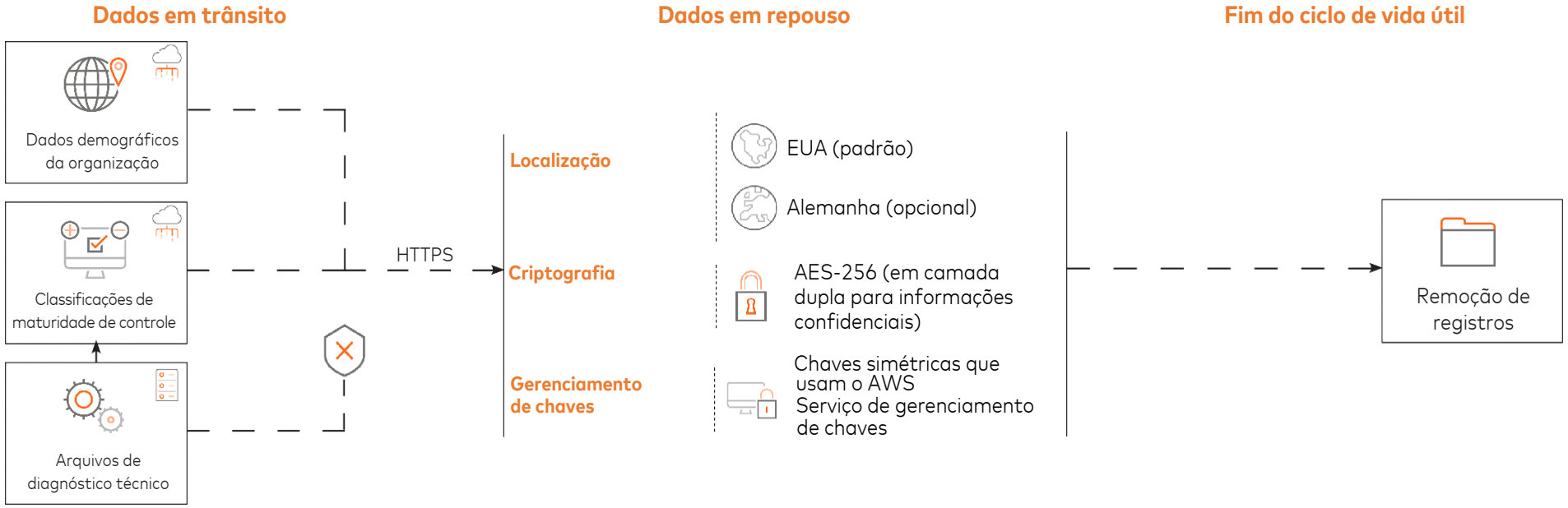
Exemplos notáveis incluem:

- ✓ AWS
- ✓ Microsoft Cloud Security
- ✓ Check Point
- ✓ Crowdstrike
- ✓ Fortigate
- ✓ McAfee
- ✓ Palo Alto
- ✓ Okta
- ✓ Symantec
- ✓ Windows Enterprise
- ✓ Windows Server
- ✓ CentOS Linux
- ✓ Cisco IOS
- ✓ Google Chrome
- ✓ Microsoft Edge
- ✓ Microsoft Exchange
- ✓ Oracle MySQL Enterprise Edition
- ✓ Google Kubernetes Engine
- ✓ Amazon Elastic Kubernetes Service
- ✓ Kubernetes
- ✓ VMWare
- ✓ Palo Alto Firewall

Cyber Quant

Tratamento de dados

A proteção e a privacidade de dados estão incorporadas ao design e à criação de todos os produtos e serviços da Mastercard. Existem procedimentos e processos abrangentes para garantir que apenas os dados necessários sejam processados. Antes que qualquer dado seja considerado para coleta, um extensivo processo de revisão e aprovação é executado pelas equipes de Segurança da Informação e Privacidade da Mastercard para minimizar a coleta, proteger o acesso e gerenciar a retenção.



Pensando em suas necessidades de segurança, a Cyber Quant não processa nenhum dos seus arquivos de diagnóstico técnico na nuvem e mantém esses arquivos estritamente no local.

Somente os dados necessários são retidos para gerenciar o funcionamento da Cyber Quant. Esses dados são mantidos no Amazon Relational Database, o qual garante que os usuários da Cyber Quant estejam em conformidade com todos os padrões de segurança mantidos pela AWS.

Para garantir que os dados sejam transmitidos com segurança para a Cyber Quant, todo o acesso ao banco de dados é concedido via HTTPS. O AWS Key Management Service é usado para criptografar dados em todos os estágios do processamento.

Por padrão, os clientes são integrados a uma zona de disponibilidade nos EUA. Se algum cliente preferir hospedar suas informações na Europa devido a razões, como requisitos regulatórios, é possível hospedar informações em uma zona de disponibilidade na Alemanha.

De acordo com as políticas da Mastercard, diferentes categorias de dados têm diferentes requisitos de retenção. O período total de retenção desde o primeiro contrato de trabalho até a exclusão da documentação do projeto é de 84 meses.

Mediante solicitação, a Mastercard removerá as informações do cliente de todos os dispositivos ou mídias de armazenamento, a menos que a retenção seja necessária para cumprir com as regulamentações ou os procedimentos aplicáveis.

Quando todos os requisitos de retenção forem atendidos, a Mastercard certificará que as informações do cliente foram removidas, fisicamente destruídas, apagadas com segurança ou devolvidas ao cliente usando uma técnica aceita pelo setor para tornar as informações do cliente irrecuperáveis de todos os dispositivos ou mídias de armazenamento.

Cyber Quant

Recursos de geração de relatórios

A Cyber Quant vem com um painel interativo, por meio do qual você pode monitorar riscos e postura cibernética.

A Cyber Quant também oferece uma variedade de relatórios que podem ser gerados mediante solicitação, os quais fornecem as informações necessárias para entender, articular e corrigir riscos tanto no nível empresarial quanto nas partes constituintes da organização.

9 Tipos abrangentes de relatórios

1. Relatório técnico detalhado da Mastercard

Uma avaliação baseada no Cyber Quant Security Framework (CQSF) com 47 categorias de controle. A plataforma oferece flexibilidade para você escolher o âmbito de avaliação adequada para as necessidades do seu negócio.

2. Relatório completo

Uma visão detalhada da maturidade do controle, do risco, do impacto financeiro, do cenário de ameaças e das prioridades de correção por meio de múltiplas avaliações em nível do ambiente.

3. Relatório do CQ Lite

Uma visão holística do risco cibernético de uma organização e do impacto financeiro correspondente para toda a empresa, bem como para cada ativo de negócios.

4. Relatório de gerenciamento

Uma visualização da pontuação de risco, importância do controle, impacto financeiro e cenário de ameaças de toda a empresa, abrangendo múltiplas avaliações.

5. Diagnóstico técnico versus questionário

Uma comparação entre os níveis de maturidade dos controles conforme percebidos pela organização e os níveis de maturidade dos controles calculados por meio de configurações técnicas.

6. Relatório de maturidade de padrões e estruturas

Informações detalhadas sobre a maturidade dos controles, detalhadas por um indicador para cada padrão

7. Detalhamento da maturidade de controle

Dados de maturidade de controle coletados de questionários e análises técnicas de um único ambiente

8. Detalhamento das fontes por controle

Este relatório contém todos os indicadores coletados por controle de todas as fontes disponíveis.

9. Relatório de instâncias

Dados de maturidade brutos e calculados coletados de questionários e análises técnicas.

Legenda do caso de uso

Destinado à liderança | Destinado à equipe técnica | Informações de impacto financeiro | Informações específicas do padrão | Maturidade de controle

Agradecimentos

Para obter mais informações sobre a Cyber Quant, visite-nos em
https://cyberquant.zendesk.com/hc/en-us

Como alternativa, você pode entrar em contato com
a equipe da Cyber Quant em support@cyberquant.com