Programa de Segurança e Operações

Como a Cyber Crucible opera o seu programa de segurança — gestão de mudanças, gestão de patches e vulnerabilidades, recuperação de desastres e continuidade de negócio, resposta a incidentes e violações, e controlo de endpoints — descrito para avaliadores de risco de fornecedores. Declara claramente o que está documentado e o que é fornecido sob NDA, e não reivindica quaisquer certificações.

- A Cyber Crucible possui um processo de gestão de mudanças?
- A Cyber Crucible possui um programa de gestão de patches?
- A Cyber Crucible possui um plano de recuperação de desastres e continuidade de negócios?
- A Cyber Crucible possui um processo de resposta a incidentes e notificação de violações?
- Como a Cyber Crucible protege e controla os endpoints?
- Quais políticas de segurança a Cyber Crucible mantém e como posso solicitá-las?

A Cyber Crucible possui um processo de gestão de mudanças?

Resposta curta: Sim. As mudanças em produção seguem um processo documentado de gestão de mudanças, com revisão, testes e aprovação. Como o produto opera no nível do kernel, a disciplina de mudanças é tratada como um controle de segurança, e não apenas como uma prática de engenharia.

O que o processo abrange

As mudanças no código da aplicação, nos drivers do kernel, nas configurações de servidores e na infraestrutura de suporte passam por estágios definidos do ciclo de vida: os requisitos de segurança são estabelecidos na fase de design; o código-fonte é controlado por versão e segredos nunca são incorporados em texto claro; testes automatizados validam as mudanças antes da promoção; e as mudanças em produção recebem revisão e aprovação formais. A segregação de funções é mantida, de modo que o autor de uma mudança não é seu único aprovador. As configurações-base dos servidores seguem guias de configuração aprovados, e serviços não utilizados são desativados sempre que possível.

Mudanças emergenciais e de drivers

As mudanças emergenciais seguem um caminho acelerado que, ainda assim, requer autorização, testes direcionados e uma revisão pós-implementação. Os drivers de kernel do Windows passam por controle de qualidade interno e são submetidos à certificação do Windows Hardware Compatibility Program (WHCP) da Microsoft antes do lançamento — uma verificação externa e independente do componente com maior nível de privilégio.

Alinhamento com frameworks e o limite honesto

O processo está alinhado ao NIST SP 800-53 (família CM) e à ISO/IEC 27001:2022 A.8.32. A Cyber Crucible não reivindica nenhuma certificação. O procedimento detalhado de gestão de mudanças e

as evidências de suporte são fornecidos aos revisores sob acordo de confidencialidade (NDA).

A Cyber Crucible possui um programa de gestão de patches?

Resposta curta: Sim. Um programa de gestão de patches e vulnerabilidades baseado em risco mantém softwares, drivers de kernel, servidores e endpoints atualizados, e as constatações são acompanhadas até sua resolução.

Como funciona

Testes de segurança automatizados contínuos são executados no pipeline de desenvolvimento, testes de penetração manuais baseados em risco são realizados com um piso anual, e testes acionados por eventos são executados a cada alteração significativa, cobrindo tanto redes internas quanto externas. Patches de segurança e hot-fixes são aplicados conforme recomendação do fornecedor, e os grupos responsáveis devem manter-se atualizados quanto aos patches aplicáveis. Mídias removíveis e portáteis são submetidas ao mesmo nível de proteção e verificação que as mídias fixas.

Priorização e implantação

As constatações são priorizadas por severidade e explorabilidade, com vulnerabilidades ativamente exploradas tratadas por meio de um caminho expedito e fora de banda. Os patches seguem o processo de gestão de mudanças — validados antes da promoção para produção — e as atualizações de drivers de kernel são revalidadas por meio do Microsoft WHCP antes do lançamento.

Alinhamento a frameworks e o limite honesto

O programa está alinhado ao NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7 e ISO/IEC 27001:2022 A.8.8. Nenhuma certificação é reivindicada. Janelas específicas de remediação-alvo e evidências de remediação são fornecidas aos avaliadores sob NDA.

A Cyber Crucible possui um plano de recuperação de desastres e continuidade de negócios?

Resposta curta: Sim. A Cyber Crucible mantém um plano de recuperação de desastres testado, de responsabilidade da gestão de TI, e uma arquitetura construída para alta disponibilidade. Como a prevenção de ameaças é executada localmente no endpoint, a proteção do endpoint continua mesmo durante uma interrupção do backend de gestão.

Resiliência por arquitetura

O backend de gestão é construído com armazenamento redundante e replicado, de modo que a perda de um nó individual não causa perda de dados ou indisponibilidade. O Acordo de Nível de Serviço publicado compromete-se com 99,9% de disponibilidade mensal para o backend de gestão e relatórios, excluindo manutenções programadas e causas fora de controle razoável. A proteção do endpoint em si não é afetada por uma interrupção do backend.

Backups e planejamento de contingência

Os dados são continuamente replicados e copiados para armazenamento externo seguro, utilizando credenciais privilegiadas distintas, com os backups protegidos contra ransomware por meio de tratamento offline ou imutável, e testados regularmente. O plano mantém um plano de resposta a emergências informáticas, um plano de sucessão, um estudo de criticidade de dados e uma lista de criticidade de serviços, e incorpora análise de impacto nos negócios, estratégias de recuperação, um plano de comunicação que inclui notificação aos clientes, e objetivos de recuperação definidos. Os testes incluem exercícios de simulação (table-top) e simulações de recuperação.

Alinhamento com frameworks e o limite honesto

O plano está alinhado com a NIST SP 800-34 e com a ISO/IEC 27001:2022 A.5.29–A.5.30. A Cyber Crucible define objetivos de ponto de recuperação e tempo de recuperação para o backend; os valores-alvo específicos, bem como o plano em si, são disponibilizados aos avaliadores sob acordo de confidencialidade (NDA). Como a proteção é executada localmente, a defesa do endpoint continua com praticamente nenhuma lacuna de tempo de recuperação durante uma interrupção do backend ou em uma implantação isolada (air-gapped).

A Cyber Crucible possui um processo de resposta a incidentes e notificação de violações?

Resposta curta: Sim. Um processo documentado de resposta a violações de dados define as funções e as etapas para responder a um suspeito de furto, violação ou exposição de dados protegidos, incluindo a notificação ao cliente. Um prazo de notificação comprometido pode ser estabelecido por contrato para clientes regulados.

O processo de resposta

Um suspeito de incidente é reportado imediatamente por meio de canais internos monitorados pela função de Segurança da Informação. Após a identificação, o acesso ao recurso afetado é removido e é convocada uma equipe de resposta a incidentes presidida pela alta administração. Investigadores forenses e especialistas, disponibilizados por meio do seguro cibernético e tecnológico da Cyber Crucible, determinam como o incidente ocorreu, os dados envolvidos, as partes afetadas e a causa raiz. Um plano de comunicação é desenvolvido em conjunto com os departamentos Jurídico, de Comunicações e de Recursos Humanos para notificar a equipe, o público e as partes afetadas conforme apropriado — incluindo a notificação ao cliente por meio de um canal mutuamente acordado — seguido de uma revisão pós-incidente.

Resposta de suporte e notificação

Os incidentes voltados ao cliente são acompanhados de acordo com os níveis de gravidade publicados no SLA (SEV1 a SEV4), e um prazo de notificação de violação ou incidente pode ser comprometido contratualmente para clientes regulados.

Alinhamento com frameworks e o limite honesto

O processo está alinhado ao NIST SP 800-61 e à ISO/IEC 27001:2022 A.5.24–A.5.26. Nenhuma certificação é reivindicada. O procedimento completo de resposta a incidentes e notificação de violações é fornecido aos avaliadores mediante acordo de confidencialidade (NDA).

Como a Cyber Crucible protege e controla os endpoints?

Resposta curta: De duas formas. O próprio produto é uma prevenção autônoma de endpoints que opera na camada de kernel, e a Cyber Crucible controla seus próprios endpoints corporativos e de engenharia sob um programa formal. Ambos se baseiam na construção interna do código com maior nível de privilégio.

Proteção de endpoints do produto

O produto oferece prevenção autônoma contra ransomware, ataques em memória (fileless) e injeção de processos, aplicada na camada de kernel. Ele é deliberadamente desacoplado das bibliotecas do sistema operacional, de modo que, quando invasores comprometem ou sequestram essas bibliotecas em memória, o produto continua a executar, aplicar controles e reportar. Como a detecção e a resposta são executadas localmente, a proteção continua durante uma interrupção do back-end de gerenciamento ou em uma implantação deliberadamente isolada (air-gapped).

Integridade da cadeia de suprimentos e validação independente

Os algoritmos de descoberta, heurísticas de kernel, sensores e drivers são projetados e mantidos internamente; nenhuma biblioteca de terceiros não verificada ou gancho de telemetria oculto é incorporado ao software. Como o componente de mais alto privilégio é proprietário, uma classe inteira de exposição da cadeia de suprimentos de terceiros é eliminada, e não apenas gerenciada. Todos os drivers de kernel do Windows são validados e assinados sob o Windows Hardware Compatibility Program (WHCP) da Microsoft.

Controles de endpoints corporativos

Os endpoints gerenciados seguem linhas de base de configuração segura aprovadas, executam proteção e varredura de endpoints, e aplicam os mesmos controles a mídias removíveis e portáteis que a mídias fixas, com o uso não autorizado de mídias restrito. A instalação de software é regida por política, os dados em repouso nos endpoints são criptografados, e os endpoints são mantidos atualizados sob o programa de gerenciamento de patches.

Alinhamento com frameworks e o limite honesto

Os controles de endpoints estão alinhados aos CIS Critical Security Controls (v8) e ao NIST SP 800-53 (SI-3, CM-2, MP-7). Nenhuma certificação é reivindicada. Padrões de configuração detalhados e evidências são fornecidos a revisores sob NDA.

Quais políticas de segurança a Cyber Crucible mantém e como posso solicitá-las?

Resposta breve: A Cyber Crucible mantém um conjunto completo de políticas de segurança da informação — abrangendo uso aceitável, acesso e autenticação, criptografia, gestão de mudanças, recuperação de desastres, resposta a incidentes e violações, retenção e destruição de dados, entre outros. As políticas e as evidências de apoio estão disponíveis a avaliadores sob NDA.

Áreas representativas das políticas

O conjunto de políticas abrange uso aceitável e ética; acesso, autenticação e acesso remoto; criptografia e proteção de chaves; desenvolvimento seguro e gestão de mudanças; segurança de servidores e endpoints; recuperação de desastres e continuidade de negócios; resposta a incidentes e violações; e retenção de dados, destruição e retenção de e-mails. Resumos de programas de conformidade, auditoria e governança de IA/SDLC são mantidos junto com as políticas.

O que é público e o que está sob NDA

As páginas públicas da base de conhecimento descrevem a existência, os princípios e o alinhamento com estruturas de referência de cada programa, para que um avaliador possa compreender a postura em um nível geral. Os documentos específicos das políticas, os padrões de configuração, os valores exatos (como cronogramas de retenção e objetivos de recuperação) e as evidências de auditoria são confidenciais e fornecidos sob um NDA mútuo, juntamente com o pacote preparado de due diligence para fornecedores.

Como solicitá-las

Os avaliadores podem solicitar o conjunto de políticas de segurança, o pacote preparado para fornecedores e as evidências de apoio pelo e-mail **dpo@cybercrucible.com**. O NDA mútuo padrão da Cyber Crucible está disponível caso ainda não exista um em vigor. Não é reivindicada certificação para nenhuma estrutura; a documentação explica como a arquitetura e os controles atendem a cada obrigação.