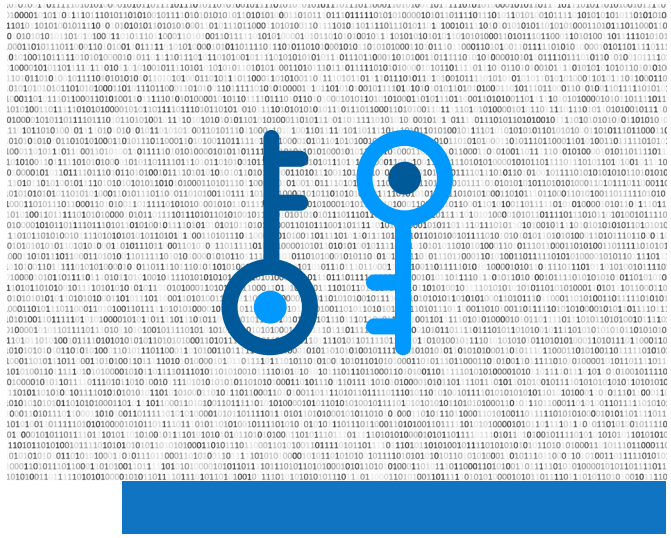
最高情報セキュリティ責任者(CISO)が DEVOPS部門に(これから)聞くべき10の質問

digicert®

01

組織全体で署名鍵へのアクセスを追跡、管理するための管理体制は整っているか?

管理に穴があれば、正当な鍵が悪意のある攻撃者の手に渡って、マルウェアに感染したソフトウェアの署名に使われてしまい、危殆化したソフトウェアを信頼すべきソフトウェアとしてお客様の顧客に通知してしまう危険性があります。すべての署名鍵とその場所を追跡していなければ、組織の顧客、評判、**財政状況**をリスクにさらすことになるのです。



02

ソフトウェアに署名をする権限、署名鍵の使用を管理する権限の保有者を把握しているか?

署名は鍵の使用ポリシーに厳密に従う必要があります。管理が甘く、**透明性**に欠けていると、組織または法律上の規制をすり抜けて署名できてしまいます。 鍵の使用を追跡し監視することで、管理者は権限ベースでの鍵アクセスを設定できるようになり、悪用を検出した場合に介入することができます。

03

自社の署名鍵によって生成されたコードサイニング証明書がどれかを把握しているか?

署名済みのソフトウェアは、組織とエンドユーザー間の信頼に基づく合意を示しています。管理者が署名鍵による証明書の発行者を追跡していなければ、悪意のある者が侵害されたソフトウェアや不正なソフトウェアリリースに署名することを目的として、組織の信用を利用して正当な証明書を生成する可能性があります。

04

何らかの活動、例えばユーザcの役割が変わったとき、またはユーザーが退社したときに、鍵と証明書からユーザーのアクセスを削除できているか?

ユーザーが退社したときは必ず、そのユーザーの署名権限を失効させなければなりません。ユーザーの役割が変わったときは、新しい役割の署名要件に合うようにアクセス権を変更する必要があります。ユーザー管理を徹底すれば、役割、責任、プロジェクトなどに応じて署名権限を設定できるようになるので、鍵と証明書の使用を適切なタイミングで適切な人に許可できます。

05

ユーザーが署名、鍵ペアの生成、証明書の作成を行う際、多要素認証を要求しているか?

署名、鍵ペアの生成、証明書の作成は、セキュリティを保つ必要のある極めて重要な活動です。不正なユーザーがこうした活動を行った場合、セキュリティ侵害が発生する可能性があります。また、マルウェアに感染したソフトウェアに署名してリリースすることにより、サプライチェーンへの攻撃を引き起こす可能性もあります。多要素認証は、個人が身元を偽っていないことを確認することで、署名ツールへのアクセスを認証済みのユーザーのみに制限できます。

06

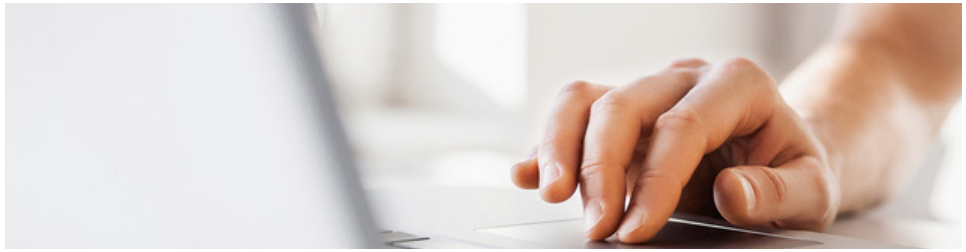
物理トークン、USB、HSMアクセスを追跡し保護しているか?

家の鍵や車の鍵と同じです。コードに署名するための物理鍵をなくしたり、共有したり、盗まれたりしてはなりません。鍵は常に追跡し、どこにあるか、いつ使用されたか、誰が使用したかを把握できるようにしておきます。

07

開発者はコードサイニング証明書を共有しているか?

鍵の共有はDevOpsでは珍しいことではありません。多くの主要なレポジトリが実際にユーザーガイドでこの危険な習慣を推奨しているほどです。開発者が鍵を共有すると、誰が署名したのか、いつ署名したのかという視認性や管理性が失われてしまいます。証明書を失効させなければならない場面でも、その鍵を使用して過去に署名されたすべてのソフトウェアが危険だとユーザーにみなされる可能性があります。



08

ビルドプロセス中にマルウェアに挿入されないようにするため、再現可能なコードを作成しているか?

原則として再現可能なコードにしておくことで、ビルドプロセスを複製してリリースを比較できるようになります。同じバイナリ出力であれば、マルウェアに感染している確率はまずないと判断されるため、自信をもってソフトウェアに署名し、リリースできます。これは、サプライチェーン攻撃に対する最高の防衛策のひとつで、特に、オープンソースのコードやサードパーティのライブラリを使用しているときに有効です。

09

組織内のすべての署名イベントを監視し監査しているか?

セキュリティは外部リリースだけの話ではありません。内部のCI/CDプロセスにも、サプライチェーンや外部エンドユーザーにリリースされるソフトウェアと同レベルの精査と信頼が必要です。社内でしか使用しないソフトウェアであっても、他のリリースと同様に、署名者、署名した内容、署名日時を把握しておく必要があります。アクシデントや悪意ある攻撃からの保護につながるだけでなく、コンプライアンスを維持し、セキュリティプロファイルを強化するのに役立つからです。

10

コードやソフトウェアリリースに署名されているかどうかを確実に追跡しているか?

署名済みのソフトウェアの役目は、それが信頼できる真正なコードおよびソフトウェアであることをパートナーと顧客に伝えることです。コードとDockerコンテナが、適切に管理された鍵と鍵署名ユーザーのアクセスによってビルド中にスキャンされ保護されていれば、納入前にソフトウェアに署名できます。これにより、転送中のソフトウェアが保護され、監査レコードが作成されて、パートナーや顧客にそのソフトウェアの真正性が納入前に検証済みであることが伝わります。この署名プロセスは管理されたコードサイニングサービスと自動化ツールを利用することで大幅に効率化できるため、俊敏なCI/CDパイプラインの中断や遅延を避けることができます。

DevOpsのセキュリティは決して後回しにしてはなりません。適切な質問をすることで、CI/CDパイプラインとサプライチェーン全体の保護を事前に検討できます。

セキュリティギャップを解消し、DevOpsのループの穴を埋めるお手伝いを致します。詳しい方法についてはお問い合わせ下さい。jpn-info-pki@digicert.com