HSM 監視が障害の回避に役立つ理由トップ 10

www.ncipher.co.jp

インスタントアラート

1. 手作業によるチェックを繰り返す必要性を排除

アラートとステータス情報が各種インターフェイスを介して自動的に配信されるため、HSM が設置されている場所にいる必要はありません。nShield Monitor の Web ベースのダッシュボード、SNMP、承認済みユーザーの E メールアカウント、nShield Monitor の syslog データ出力を使用する外部の SIEM（セキュリティ情報およびイベント管理）システムなど、情報を受信するためのオプションが複数あります。

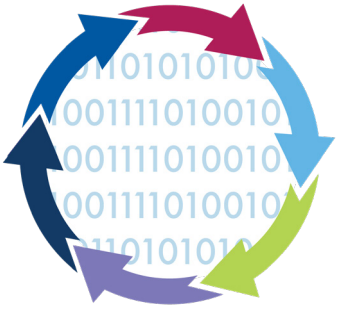
2. 予防的な修正措置を実現

nShield Monitor には 3 つの異なるユーザーロールがあります。管理者（Administrator）は他のユーザー（特にグループマネージャーと他の管理者）の作成を含むシステム構成を管理します。グループマネージャー（Group Manager）は特定の HSM および HSM のグループの管理を担当します。監査役（Auditor）はダッシュボードとレポートを監視します。これらのユーザーのいずれかがインスタントアラートを受信することにより、障害のある HSM が発見された場合、HSM に容量の過負荷が発生する可能性が高い場合や不正な改変が行われた場合などに迅速な措置が可能になります。

3. 業務の役割に応じてステータスデータをフィルタリングすることで情報の過負荷を回避

HSM に関連付けられたセキュリティドメイン内のどこかにアラームがある場合は、すべてのユーザーがハイレベルで素早く確認できます。グループマネージャーは、平均使用率、1 秒あたりのトランザクション数、タイプごとのアクティブなアラーム数を示すハイレベルのグループレポートを使用できます。グループマネージャーは、自分の管理下にある HSM の情報とアラートのみを受信します。E メール通知イベントはグループレベルで構成できるため、情報、通知、警告、エラー、クリティカル、アラート、緊急ステータスをフィルタリングすることができます。

継続的な追跡



4. 個別の HSM および HSM のグループのパフォーマンスを監視

ユーザーが期間を選択してグループのパフォーマンスを監視することができます。必要に応じて、任意のデバイスを複数のグループに関連付けることが可能です。ステータス、使用率、ホストの TPS、未確認のアラームなど、特定のグループ内のすべての HSM の統計情報を素早く確認する機能があります。60 秒ごとに更新されるダッシュボードを使用して、上位 5 つのデバイスを簡単に確認できます。

5. 容量の過負荷を事前に警告

「使用率の過負荷」と「使用率ピークイベント」のしきい値をユーザーが個別に設定でき、グループごとに設定可能な警告レベル、クリティカルレベル、ピークレベル、およびピーク期間のパラメータによって制御できます。アラームは、グループごとにオン/オフの切り替えが可能です。警告のしきい値を超えると重大度「警告」のイベントが生成され、クリティカルのしきい値を超えると重大度「クリティカル」のイベントが生成されます。サンプリングは 10 分ごとに行われ、過去 10 分間のアクティビティがカバーされます。

6. HSM の健全性と重大イベントの継続的な監視を実行

各 HSM の監視は平均で 60 秒ごとに更新されます。グループに関係なく、システムで定義されているすべての HSM がカバーされます。健全性の情報には、HSM の動作状態、アラーム/改竄ステータス、不正検出分析、過負荷ステータス、ネットワークステータス、通信/管理ポート情報が含まれます。

包括的なデータ

7. 分析と比較用に HSM 構成のバンドルビューを提供

グループマネージャーと監査役は、担当するグループのすべてのデバイスを素早く表示でき、個々の HSM をクリックすることで、デバイス名、所属グループ、シリアル番号、IP アドレス、健全性チェックの詳細な統計情報、LMK 情報などの情報を確認できます。この表示から、HSM とグループ両方の関連する使用率グラフとホストコマンドグラフに簡単に移動できます。

8. HSM の使用率とパフォーマンスに関する詳細なレポートを生成

ダッシュボードのパフォーマンスグラフは、現在の使用率の「スナップショットビュー」を表します。グループマネージャーは、担当するすべてのグループの時間を前後に移動できます。グラフをクリックするとより詳細な情報が表示されます。外部での処理や分析のため、CSV 形式での印刷またはエクスポートもサポートしています。データフィルタリングでサポートされる時間範囲は非常に柔軟性が高く、過去 1 時間、過去 24 時間、過去 7 日間、過去 30 日間、またはユーザー定義の範囲を設定することができます。

9. パフォーマンス、エラーなどの重要データの詳細分析のためのドリルダウンが可能

個別の HSM およびグループの一部としての HSM の暗号化パフォーマンスは、個々のコマンドに至るまで、さまざまな期間にわたって分析が可能です。デバイスおよびグループのログは、改竄や nShield Monitor システムに追加された新しい HSM デバイスなどの情報を記録し、日付と時刻、重大度、メッセージ内容でデータをフィルタリングする各種オプションがサポートされています。アクティブアラーム、オフライン HSM、過負荷の HSM などの問題は常に強調表示され、グループマネージャーが必要に応じて修正措置を採れるようになっています。

10. HSM 使用率に関する詳しい情報を特定の機能にまで掘り下げて提供

瞬時、短期、長期の傾向を確実に評価するため、ユーザーが期間を選択できます。期間中のアクティブなホストコマンドすべてが呼び出し頻度とともに表示されます。これにより、予期しないホストコマンド処理などの潜在的な不正イベントを簡単に識別できます。

nShield Monitor は nShield HSM に不可欠な監視ツールです。詳細については www.ncipher.co.jp をご覧ください。

nCipherSecurity をフォロー