EARLY WARNING system

The Next Generation of Threat Management

powered by IntelliShield™

PRODUCT SHEET

In der vernetzten IT-Welt wird es immer mehr zu einer Herausforderung, mit den Schwachstellen Schritt zu halten, die die kritischen Systeme bedrohen. Traditionelle Scanning- und Alarmierungsdienste leisten gute Arbeit bei der Identifizierung von Schwachstellen. Aber die Informationen, die sie liefern, lassen die Zusammenhänge vermissen, so dass es viel Zeit und Geld braucht herauszufinden, welche Prioritäten bei den Abwehrmaßnahmen zu setzen sind.

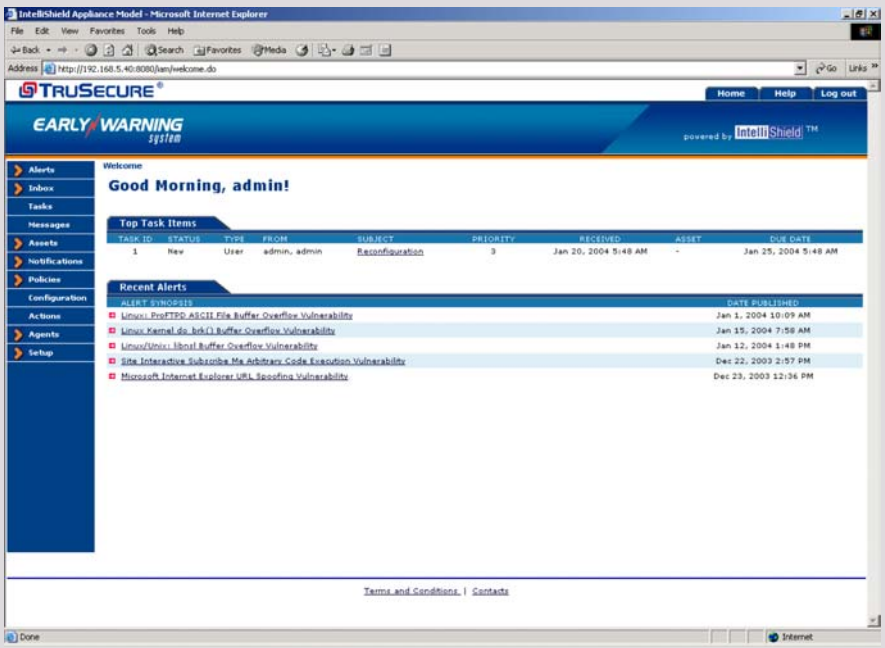
Der Schlüssel zur Schadensbegrenzung für Ihr Business liegt in der Vergrößerung des Zeitfensters, das sich zwischen dem Auftauchen einer neuen Schwachstelle und der Entscheidung für Gegenmaßnahmen auftut. Sobald ein Exploit freigesetzt ist, wird aus der Schwachstelle eine reale Bedrohung und das Zeitfenster schmilzt zusammen.

Das Entdecken der Schwachstelle ist nur der erste Schritt. Sodann müssen Sie Ihre Kenntnisse über die Schwachstelle mit den Informationen verbinden, die Sie über die möglicherweise gefährdeten Systeme besitzen. Danach Gegenmaßnahmen recherchieren, die verfügbaren Ressourcen ermitteln und die notwendigen Aufgaben verteilen. Und schließlich müssen Sie sicherstellen, dass die notwendigen Maßnahmen getroffen wurden und die gewünschte Wirkung tatsächlich erzielen. Dies beschreibt den durchgehenden Prozess des Bedrohungsmanagements.

IntelliShield™ Early Warning System™ (EWS) ist eine neuartige Lösung, die den gesamten Prozess des Bedrohungsmanagements automatisiert, angefangen mit der Identifizierung einer Schwachstelle bis zur Prüfung der Gegenmaßnahmen. EWS basiert auf den Informationsgütern, den sog. Assets. Es ordnet diesen Assets Größen zu, die deren Bedeutung für die Geschäftsprozesse widerspiegeln und verbindet diese Informationen mit Scanning-Ergebnissen und Echtzeit-Alarmmeldungen.

Features

- Modularer und skalierbarer Aufbau, damit eine rasche Installation und Integration in bestehende Sicherheitsinfrastrukturen möglich ist.
- Neue Schwachstellenmeldungen lösen gezielte „Assessments“ aus, um die Assets zu bestimmen, die aktuell bedroht sind.
- Flexible Optionen zur gezielten Benachrichtigung
- Empfehlungen für Abwehrmaßnahmen sind Bestandteil der Benachrichtigungen.
- Automatische Überprüfungen bestätigen, dass bedrohte Systeme nicht länger gefährdet sind.



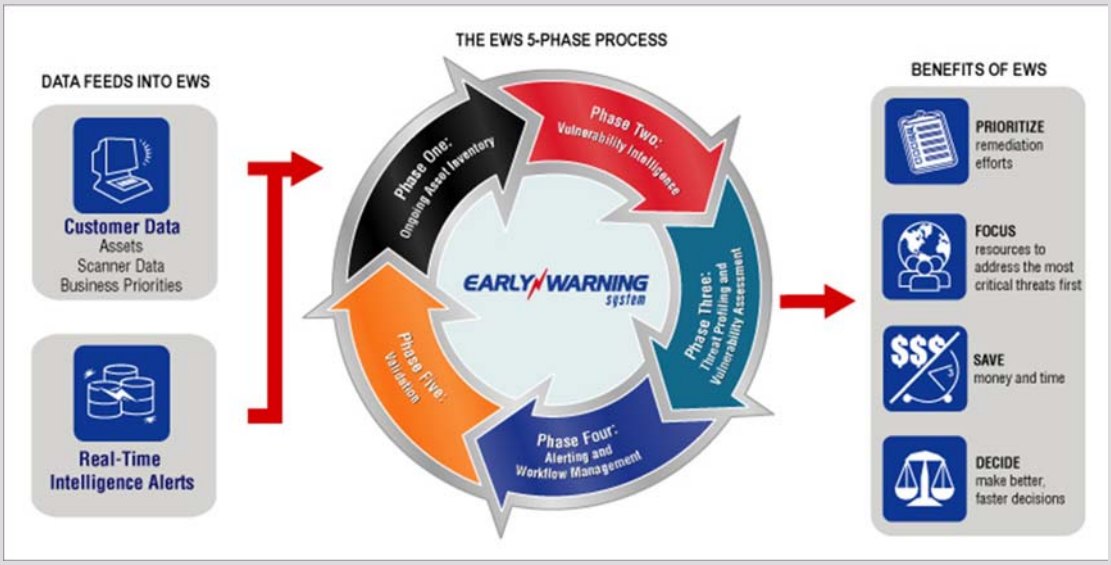
TRUSECURE
Intelligent Risk Management

Benefits

- *Asset-basierte Alarme* – EWS meldet, wenn ein spezifisches System in Ihrem Netzwerk bedroht ist. Die Benachrichtigungen sind angepasst auf die Schwere der Bedrohung, die Wahrscheinlichkeit des Eintritts und die Kritikalität des betroffenen Systems. Die Alarme sagen Ihnen, was wichtig ist, und zwar wichtig für Sie. Neue Schwachstellenmeldungen lösen gezielte „Assessments“ aus, um die Assets zu bestimmen, die aktuell bedroht sind.
- *Entscheidungshilfe* – Detaillierte, umsetzbare Aufklärung („Intelligence“) erlaubt es Ihnen, bessere und schnellere Entscheidungen über Abwehrmaßnahmen zu treffen: Welche sind am wichtigsten, welchen Aufwand bedeuten sie und wie lange dauert deren Umsetzung?
- *Kostengünstige Gefahrenabwehr* – Meldungen über Schwachstellen in Echtzeit ermöglichen es Ihnen, die Kosten für die Gegenmaßnahmen zu verringern, weil Sie die Gefahren nach Ihrem Zeitplan beseitigen, bevor sie sich zu einer Krise zuspitzen. Dadurch können Sie Ihre Team-Ressourcen zuerst auf den Schutz der wirklich kritischen Systeme konzentrieren.
- *Zugang zum TruIntelligence™ Security Knowledge Network™* - TruSecure verfügt über ein Vielzahl von Ressourcen, die rund um die Uhr Schwachstellen und Bedrohungen entdecken, analysieren und kategorisieren.
- *Fortlaufende Discovery Scans* – EWS unternimmt regelmäßige Scans der sich in der Regel schnell ändernden Netzwerkumgebung, die sog. Discovery Scans. Diese helfen Ihnen, neue Systeme zu erkennen oder Änderungen an der technischen Konfiguration bestehender Systeme nachzuvollziehen.

EWS – Fünf Phasen des Bedrohungsmanagements

Das Bedrohungsmanagement des Early Warning Systems basiert auf einem Prozess aus fünf Phasen, der automatisiert und angepasst werden kann.



Phase 1: Fortlaufende Systembestandsaufnahme – EWS führt laufende Bestandsaufnahmen der Systeme in vorher festgelegten IP-Bereichen durch. Gefundene Veränderungen werden im Asset-Bestand erfasst.

Phase 2: Schwachstellenaufklärung – Alarmierungen in Echtzeit durch das TruIntelligence-Netzwerk geben Details über neue Bedrohungen und veranlassen spezifische Aktionen, die in der Konfiguration der sog. EWS „smart filter“ festgelegt werden.

Phase 3: Bedrohungsprofilierung und Schwachstellenbewertung – EWS bestimmt die Systeme, die von einer neuen Schwachstellenmeldung betroffen sind.

Phase 4: Risikoalarm und Workflow – EWS benachrichtigt den Verantwortlichen für ein System („asset owner“), dass eine Gefährdung besteht und liefert die notwendigen Informationen, um Schutz- oder Gegenmaßnahmen zu ergreifen. Benachrichtigungen und Abwehrmaßnahmen werden im EWS-eigenen Workflow-System festgehalten.

Phase 5: Bestätigung – EWS überprüft automatisch, ob die erforderlichen Maßnahmen zur Risikobegrenzung ergriffen wurden und auch tatsächlich wirksam sind.

TruSecure Deutschland
Kaiserswerther Str. 115
D-40880 Ratingen
Tel: +49 (0)2102 420 765

TRUSECURE
Intelligent Risk Management
www.trusecure.com