初期チューニングのご提案

株式会社XXXXX 様
集計期間：yyyy/mm/dd – yyyy/mm/dd
対象デバイス：CESxxx

対象ポリシ：xxxxxxxxxx

■ ホワイトリスト

IPアドレス単位で検知除外を推奨するチューニング内容をご報告します。
なお、ご提案したIPアドレスをホワイトリストへ登録した場合、全ての検知が除外されますことをご了承下さい。

No	IPアドレス	件数	理由	確認事項 / 備考	IPアドレス情報
1	xxx.xxx.xxx.xxx	xxx	検知したシグネチャ27件のうち、左記アドレスのみの通信を検知しているシグネチャが17件で、攻撃を意図していない通信の検知が見受けられます。 ■検知シグネチャNo. 2, 3	xxx.xxx.xxx.xxxからの通信は、想定された通信でしょうか。 その場合、Signature毎の説明にも記載させて頂いておりますが、xxx.xxx.xxx.xxxのIPアドレスをホワイトリストに登録頂く事を推奨いたします。 詳細については、Signature毎の説明をご確認願います。	

■ シグネチャ

これまでに検知したシグネチャについて、推奨するチューニング内容をご報告します。

No	シグネチャ名	signature id	件数	severity level	action	提案	理由	確認事項 / 備考
1	Information Disclosure-HTTP Header Leakage	080200004	xxx	High	Erase	Disable	サーバからのレスポンスヘッダに「X-Powered-By」ヘッダを含む場合に検知します。 本環境では、「X-Powered-By」ヘッダに「PHP/5.3.3」と表示されております。このような情報から攻撃に利用されることがありますので、公開する必要のない情報は非表示にすることを推奨します。 現在の設定では、WAFで該当箇所を削除した上で、レスポンスを返しておりますので、Erase設定のままとすることも可能ですが、大量に検知していますのでサーバ側で非表示にし、本シグネチャはDisableにすることを推奨します。 ■検知例 HTTP/1.1 200 OK Date: Tue, 21 Jun 2016 01:33:16 GMT Server: Apache **X-Powered-By: PHP/5.3.3** Content-Length: 2387 Connection: close Content-Type: text/html; charset=UTF-8	サーバ側で「X-Powered-By」ヘッダを非表示設定にすることは可能でしょうか。 可能である場合 ⇒ Disable 不可の場合 ⇒ Eraseのまま
2	Information Disclosure-ASP/JSP Source Code Leakage	080140017	794	High	Erase	Disable	サーバレスポンスに含まれるJSP(JavaServer Page)のソースコードを検知します。流出した場合、脆弱性等を調査され、攻撃に悪用される可能性があります。 本環境では、xxx.xxx.xxx.xxxから「/test/js_css/GlobalS.js」や「/t-test/js_css/GlobalS.js」等への通信や、xxx.xxx.xxx.xxxから「/test/js_css/GlobalS.js」等への通信に対するサーバからのレスポンスに含まれる「wscript.shell」を検知しております。「wscript.shell」はJavascriptのプログラムから他のプログラムを実行するためのActiveXオブジェクトです。 現在の設定では、該当文字列を削除してレスポンスを送信するため、検知内容が意図したもので、正規内容である場合はシグネチャのDisable、もしくはAlertにすることを推奨します。 ■検知例 HTTP/1.1 200 OK Date: Thu, 23 Jun 2016 01:03:26 GMT Server: Apache Last-Modified: Sun, 25 Oct 2015 15:00:00 GMT Content-Length: 17346 Content-Type: text/javascript (中略、以下レスポンスボディの一部)	
3	SQL Injection	030000078	50	High	Alert_Deny	検知IPアドレスの ホワイトリスト登録 (シグネチャはAlert_Denyのまま)	SQLインジェクション攻撃を検知します。 本環境では、xxx.xxx.xxx.xxxから「/test/manager/admin/SQL_TEST.php」や「/demo-test/manager/admin/SQL_TEST_ALL.php」等へ対する通信に含まれる文字列を検知しております。 xxx.xxx.xxx.xxxからの通信が想定される場合は、該当のIPアドレスをホワイトリストに登録することにより、xxx.xxx.xxx.xxxからの通信は検知しませんので、シグネチャは現在の設定のまま(No.4：Alert_Deny/No.5：Alert)とすることを推奨します。 ホワイトリストに登録しない場合は、本通信が想定される通信でしたら誤遮断/誤検知の原因となりますので、Disableにすることを推奨します。 ■検知例 POST /test/manager/admin/SQL_TEST.php HTTP/1.1 Referer: https://www.test.com/test/manager/admin/SQL_TEST.php User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.test.com (中略、以下POSTデータ)	
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								