定期報告会のレポート例となります。

下記の通り、シグネチャ検出状況 Top10イベントとCriticalイベントのサマリをご報告し、さらに各アラート種類（シグネチャ）毎に、以下の内容をまとめてご報告いたします。
・イベントの概要、攻撃の内容
・影響を受けるソフトウェア／バージョン情報
・お客様のシステム構成を考慮、確認した上での推奨方針
・送信元IP／宛先IP、ポートを日別、時間帯別等で件数の集計　※お客様専用ポータルからも随時参照可

◆シグネチャ検出状況 Top10イベント(2015/01/01-2015/03/31)

設定されているシグネチャで検出したログ件数のTOP10イベントをご提示します。ここでは全プライオリティを対象としています。

アラート名	プライオリティ	アクション	ログ件数	前回ご報告時	推奨
PHP.Remote.File.Inclusion	low	detected	202,312	45,143	現状維持
HTTP.Request.Smuggling	low	detected	11,147	615	現状維持
ZmEu.Vulnerability.Scanner	low	detected	6,678	1,299	遮断
TCP.Overlapping.Fragments	low	detected	5,404	1,436	現状維持
HTTP.URI.SQL.Injection	high	detected	4,372	6	要確認
Cross.Site.Scripting	low	detected	4,133	39	要確認
TCP.Bad.Checksum	low	detected	3,404	878	現状維持
PHP.CGI.Argument.Injection	high	detected	2,033	202	要確認
LiteSpeed.Web.Server.NullByte.Information.Disclosure	medium	detected	1,677	1	無効化
HTTP.GET.Request.Directory.Traversal	medium	detected	1,556	35	要確認
総合計			**242,716**		

◆シグネチャ検出状況 Criticalイベント(2015/01/01-2015/03/31)

設定されているシグネチャで検出したプライオリティが「critical」レベルのイベントのみを対象にご提示します。

アラート名	プライオリティ	アクション	ログ件数	前回ご報告時	再検知時の対応
OpenSSL.TLS.Heartbeat.Information.Disclosure	critical	detected	75	-	検知のみ
HTTP.Negative.Data.Length	critical	detected	5	-	ご報告
Adobe.ColdFusion.Scheduled.Task.Arbitrary.File.Upload	critical	detected	3	-	検知のみ
DLink.IP.Cameras.rtpd.cgi.OS.Command.Injection	critical	detected	3	-	検知のみ
Cisco.IOS.HTTP.Command.Execution	critical	detected	3	1	検知のみ
HTTP.URI.Overflow	critical	detected	1	3	ご報告
総合計			**90**		

各アラート種類（シグネチャ）毎の詳細な報告内容例です。
下記はZmEu.Vulnerability.Scannerについての例です。

◆1：ZmEu.Vulnerability.Scannerについて

【イベント概要】
ZmEu.Vulnerability.Scannerとは、phpmyadmin（PHPに実装されているMySQLの管理ツール）の脆弱性を突くための前準備として、
サーバにphpmyadminがインストールされているかを調査する探索系行動を示すものとなります。

【影響を受けるバージョン等】
phpmyadminを導入している環境

【本イベントへのコメント】
本イベントの検出傾向を見る限りでは、検知の大半は海外からの通信によるものとなっております。
お客様環境にてphpmyadminを導入されているかは、念の為ご確認頂きたく存じますが、余計な脆弱性調査を防ぐ観点から、
本イベントに関しては検知時の動作を遮断とすることに関しても、併せてご検討頂ければと存じます。

◆2：ZmEu.Vulnerability.Scannerの検出状況詳細（検出通信Top20 [送信元IPと宛先IPの組み合わせ]）

検知数順位	送信元IPアドレス	宛先IPアドレス	宛先ポート番号	サービス	ログ件数
1	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8013	8013/tcp	208
2	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8001	8001/tcp	104
3	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8010	8010/tcp	104
4	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8009	8009/tcp	104
5	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8008	8008/tcp	104
6	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8007	8007/tcp	104
7	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8002	8002/tcp	104
8	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8011	8011/tcp	104
9	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8012	8012/tcp	104
10	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8016	8016/tcp	104
11	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.77.103	8090	8090/tcp	104
12	94.102.49.31 (Ecatel[オランダ])	10.246.77.103	8001	8001/tcp	72
13	94.102.49.31 (Ecatel[オランダ])	10.246.77.103	8008	8008/tcp	72
14	94.102.49.31 (Ecatel[オランダ])	10.246.77.103	8011	8011/tcp	72
15	94.102.49.31 (Ecatel[オランダ])	10.246.77.103	8012	8012/tcp	72
16	94.102.49.31 (Ecatel[オランダ])	10.246.77.103	8013	8013/tcp	72
17	94.102.49.31 (Ecatel[オランダ])	10.246.77.103	8016	8016/tcp	72
18	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.85.161	8002	8002/tcp	55
19	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.85.162	8011	8011/tcp	54
20	184.107.252.18 (iWeb Technologies Inc[カナダ])	10.246.85.164	8014	8014/tcp	53

◆3：ZmEu.Vulnerability.Scannerの検出状況詳細（検出通信Top20 [送信元IPと検出時間帯の組み合わせ]）

検知数順位	時間帯	送信元IPアドレス	ログ件数
1	12	184.107.252.18 (iWeb Technologies Inc[カナダ])	2,495
2	11	94.102.49.31 (Ecatel[オランダ])	1,152
3	4	89.248.162.170 (Ecatel[オランダ])	207
4	10	89.248.162.170 (Ecatel[オランダ])	207
5	7	94.102.52.10 (Ecatel[オランダ])	207
6	1	69.174.245.163 (アメリカ)	138
7	20	94.244.139.199 (NashNet[ウクライナ])	138
8	18	61.19.246.190 (CAT TELECOM Data Comm. Dept[タイ])	138
9	17	94.75.228.26 (leaseweb.com[オランダ])	138
10	17	69.174.245.163 (アメリカ)	138
11	17	46.105.110.43 (OVH[フランス])	138
12	12	94.75.228.26 (leaseweb.com[オランダ])	138
13	12	65.111.180.205 (Serverpronto[アメリカ])	138
14	12	23.236.126.45 (C3 Networks Inc[アメリカ])	138
15	8	220.181.152.196 (CHINANET Beijing province network[中国])	137
16	10	60.191.252.55 (Jinhua Telecom Co[中国])	127
17	3	60.191.252.55 (Jinhua Telecom Co[中国])	115
18	21	61.47.61.67 (PACNET-BKK-HUB[タイ])	108
19	20	123.125.219.67 (China Unicom[中国])	83
20	6	61.147.67.88 (中国)	66

※お客様専用ポータル画面イメージ

クローズアップ分析レポート作成対象データを選択してください。 | 全件表示 | 一部表示 |

選んだ項目でクローズアップ分析レポート作成

	送信元ゾーン名	宛先ゾーン名	ログ件数		送信元(ユニーク数)		宛先(ユニーク数)		サービス(ユニーク数)		ユニークアラート数	
1	trust	untrust	2	40.00%	2	40.00%	2	66.67%	2	66.67%	2	50.00%
2	untrust	DMZ	2	40.00%	2	40.00%	1	33.33%	1	33.33%	2	50.00%
3	trust	DMZ	1	20.00%	1	20.00%	1	33.33%	1	33.33%	1	25.00%
合計			**5**	**100.00%**	**5**	**100.00%**	**3**	**100.00%**	**3**	**100.00%**	**4**	**100.00%**

選んだ項目でクローズアップ分析レポート作成

集計項目、集計方法を左リストから選択し、「追加→」ボタンをクリックし、右リストに反映します。
Ctrlキーを押しながら項目をクリックすることにより、複数の項目を選択できます。右リストの項目は、検索優先順に「↑」「↓」ボタンで並べ替えます。

集計項目

デバイス
アプリケーション名
デバイスIPアドレス
ログ種別
ログ種別詳細
送信元ポート番号
宛先ポート番号
アプリケーション名称
送信元ゾーン名
宛先ゾーン名
送信元インターフェース名

追加→ / ←削除

送信元IPアドレス
宛先IPアドレス
アラート名
CVE番号

↑ / ↓

集計方法

送信元(ユニーク数)
宛先(ユニーク数)
サービス(ユニーク数)
ユニークアラート数
ユニーク攻撃実施日

追加→ / ←削除

ログ件数

↑ / ↓

ソート条件 ○ 集計項目 を 昇順▲ ○ 集計項目 を 降順▼ ◉ 集計方法 を 降順▼ ○ 集計方法 を 昇順▲

表示件数 1000 件

レポート再作成 ☐ ※過去の検索結果を破棄し、再度レポートを作成します

クローズアップ分析レポート作成

日付別攻撃件数集計レポート

期間	2011年03月07日 00時00分00秒 ～ 2011年03月07日 23時59分59秒
条件1	

前画面に戻る | ログ表示 | CSVダウンロード | PDFダウンロード

グラフ件数: 60 件 グラフ1 グラフ2 閉じる

クローズアップ分析レポート作成対象デ

レポート作成情報

提出先: 内部監査室
カバータイトル: 不正侵入検知ログレポート
作成者: 情報システム部 ○○ ○○

作成 | 取消

	日付	ログ件数		アラート数
1	2011-03-07	5	100.	100.00%
合計		5	100.	100.00%

選んだ項目でクローズアップ分析レポート作成