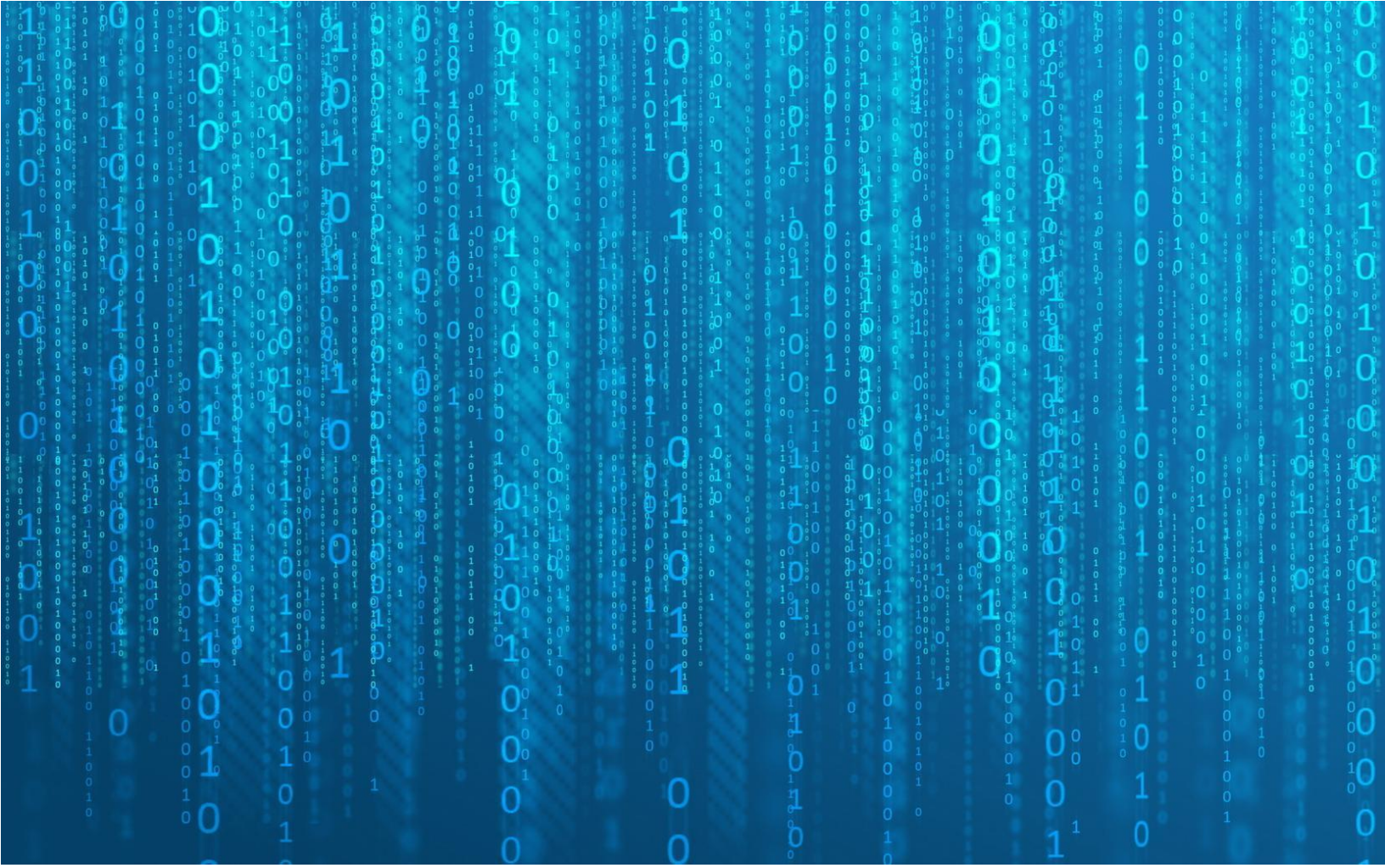


# CSIRC REPORTS

Monthly Analytic Synopsis

August FY17

EPA Computer Security Incident Response Capability

# Table of Contents

**Revision Log** ..... ii
1 **Executive Summary** ..... 1
1.1 (b) (5) [redacted] ..... 1
1.2 (b) (5) [redacted] ..... 2
2 **BigFix Based Reports** ..... 2
2.1 (b) (5) [redacted] ..... 2
2.2 (b) (5) [redacted] ..... 12
3 **Remedy Based Reports** ..... 14
3.1 (b) (5) [redacted] ..... 14
3.2 Event Report ..... 15
3.3 Event Category Report ..... 19
3.4 Attack Vector Report | NIST SP 800-61 (rev 2) ..... 23
4 (b) (5) **MTIPS Based Reports** ..... 28
4.1 (b) (5) [redacted] ..... 28
4.1.1 (b) (5) MTIPS Blocked Category Definitions ..... 28
5 **Executive Level Reports** ..... 33
5.1 Successful Incident Attack Report | PMC ..... 33
6 (b) (5) [redacted] ..... 33
6.1 (b) (5) [redacted] ..... 33

# List of Exhibits

(b) (5) [redacted]

(b) (5) [redacted]

Exhibit 15: Event Report | Volume and Trending ..... 16

(b) (5) [redacted]

(b) (5) [redacted]

Exhibit 21: Attack Vector Report | Trending ..... 25

(b) (5) [redacted]

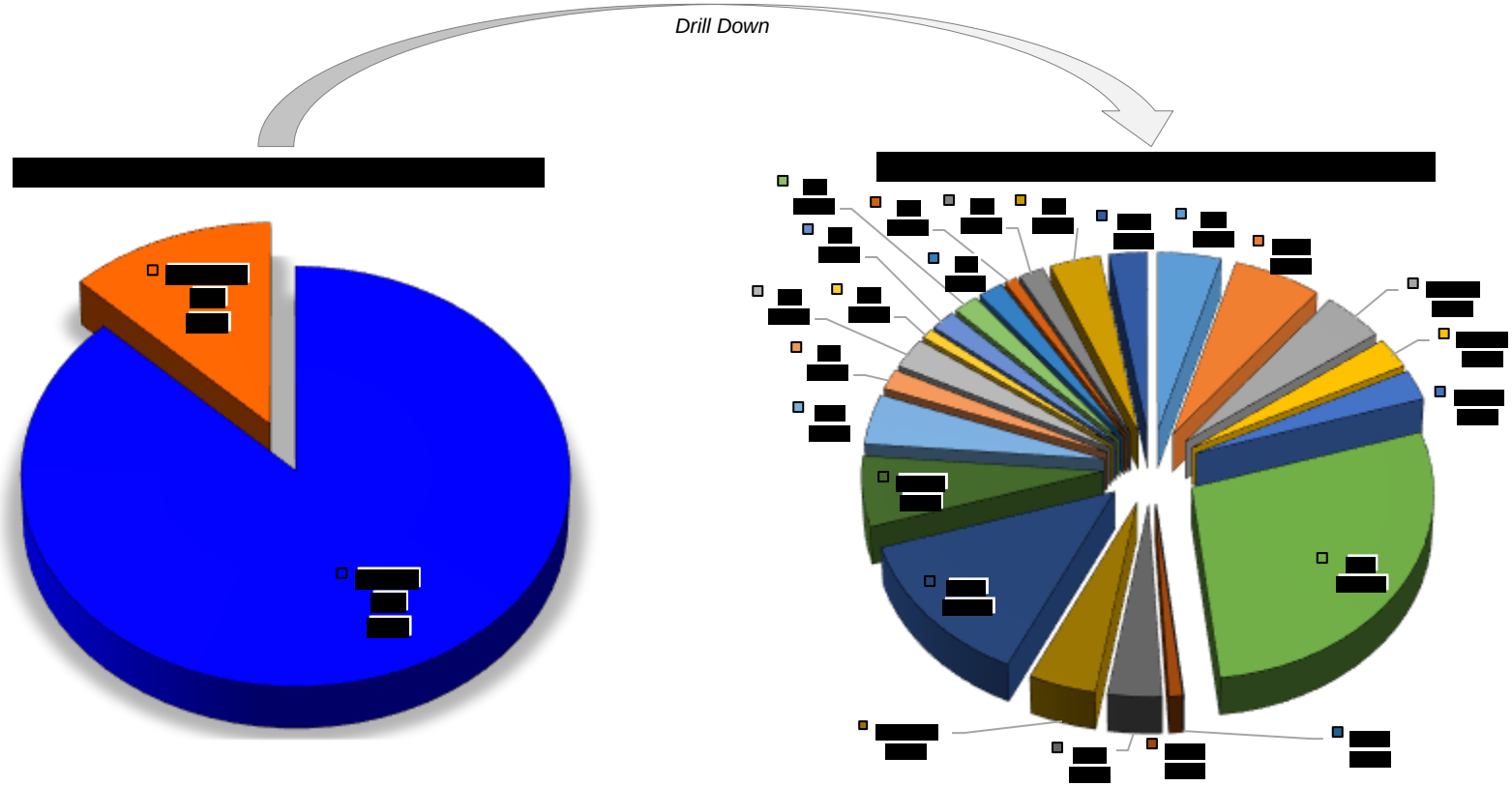
# Revision Log

| Date | Version No. | Description | Author | Reviewer | Review Date |
|---|---|---|---|---|---|
| 08/05/2013 | 1.0 | Release Version | (b) (6) [redacted] | [redacted] | 08/02/2013 |
| 08/05/2014 | 2.0 | Version 2.0 | (b) (6) [redacted] | [redacted] | 08/01/2014 |
| 10/05/2015 | 3.0 | Version 3.0 | (b) (6) [redacted] | [redacted] | 10/02/2015 |
| 03/07/2017 | 4.0 | Version 4.0 | (b) (6) [redacted] | [redacted] | 03/03/2017 |

# 1 Executive Summary

## 1.1 (b) (5) [redacted]

- (b) (5) [redacted]



## 1.2 (b) (5) [redacted]

(b) (5) [redacted]

| [redacted] | [redacted] | [redacted] | [redacted] |
|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |

# 2 (b) (5) [redacted]

## 2.1 (b) (5) [redacted]

(b) (5) [redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

## 2.2 (b) (5) [redacted]

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

# 3 Remedy Based Reports

## 3.1 (b) (5) [redacted]

(b) (5) [redacted]

(b) (5) [redacted]

## 3.2 Event Report

Per NIST SP 800-61 (rev 2), an **Event** is any observable occurrence in a system or network. An **Incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Examples of **Events** include the following:

- User receives a phishing email and does not click on the link.
- While browsing the Internet, a user receives a pop-up from Microsoft support stating their system has a virus and to call a 1-800 number to help resolve the issue. The request is ignored and the pop-up is simply closed.
- User attempts to access a particular webpage, but is inadvertently redirected to another webpage. The user is prompted to click on a link for a Flash Player update. No clicking takes place.

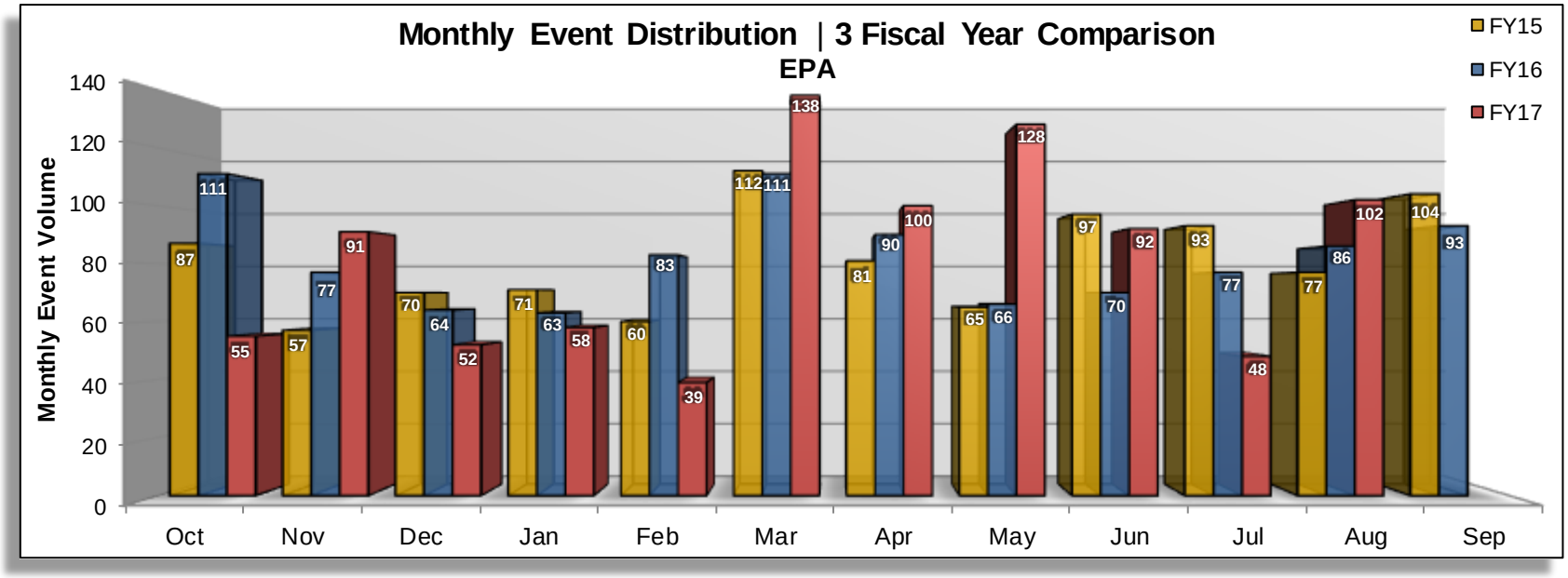
Examples of **Incidents** include the following:

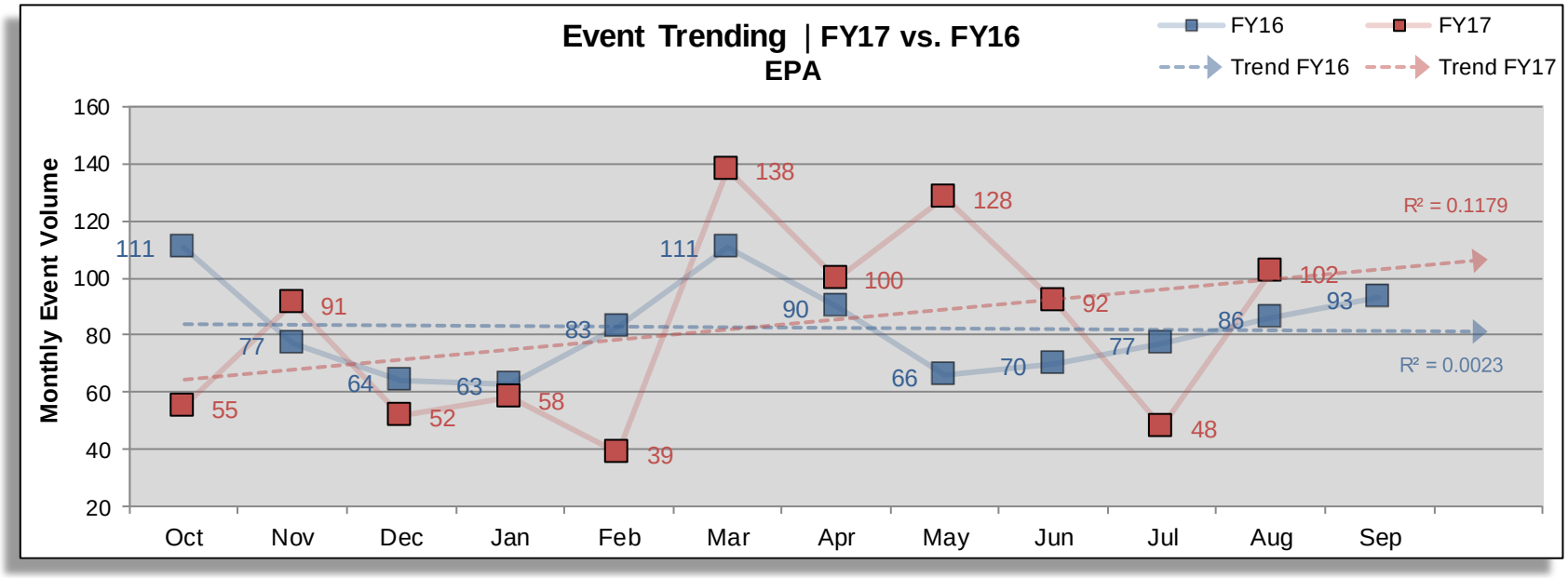
- User receives a phishing email & clicks on the link, which takes the user to a fake Microsoft website. LAN & password information is provided.
- While browsing the Internet, a user receives a pop-up from Microsoft support stating their system has a virus and to call a 1-800 number to help resolve the issue. The user calls the listed phone number and gets deceived into providing PII, CBI, or through a series of downloads allows the fake Microsoft technician unauthorized access to the system.
- User attempts to access a particular webpage, but is inadvertently redirected to another webpage. The user is prompted to click on a link for a Flash Player update. Upon clicking the link, a trojan horse is downloaded and a compromise takes place.

| FY17 | Corresponding Statistics for Computer Security Events |
|---|---|
| **Average (monthly):** | The agency is incurring an average of **82.1** computer security related events/incidents **per month** in FY17. |
| **Average (daily):** | The agency is incurring an average of **3.9** computer security related events/incidents **per business day** in FY17. |
| **High Month:** | **March** is currently the most active month in FY17 with **138** events/incidents. Represents **15.3%** of all events/incidents in FY17. |
| **Low Month:** | **February** is currently the least active month in FY17 with **39** events/incidents. Represents **4.3%** of all events/incidents in FY17. |
| (b) (5) [redacted] | (b) (5) [redacted] |
| [redacted] | [redacted] |
| **Trend (slope):** | Events/Incidents for FY17 (Oct 2016 through Sep 2017) have an **upward trend** ▲ (i.e. slope of linear regression) of **0.0338.** |

| FY16 | Corresponding Statistics for Computer Security Events |
|---|---|
| **Average (monthly):** | The agency incurred an average of **82.6** computer security related events/incidents **per month** in FY16. |
| **Average (daily):** | The agency incurred an average of **4.0** computer security related events/incidents **per business day** in FY16. |
| **High Month:** | **October** was the most active month in FY2016 with **111** events/incidents. Represented **11.2%** of all events in FY16. |
| **Low Month:** | **January** was the least active month in FY2016 with **63** events/incidents. Represented **6.4%** of all events in FY16. |
| (b) (5) [redacted] | (b) (5) [redacted] |
| [redacted] | [redacted] |
| **Trend (slope):** | Events/Incidents for FY16 (Oct 2015 through Sep 2016) had a **downward trend** ▼ (i.e. slope of linear regression = **-0.0104**). |

Exhibit 15: Event Report | Volume and Trending






« Return to Table of Contents

(b) (5)

[redacted]

(b) (5)

[redacted]

## 3.3 Event Category Report

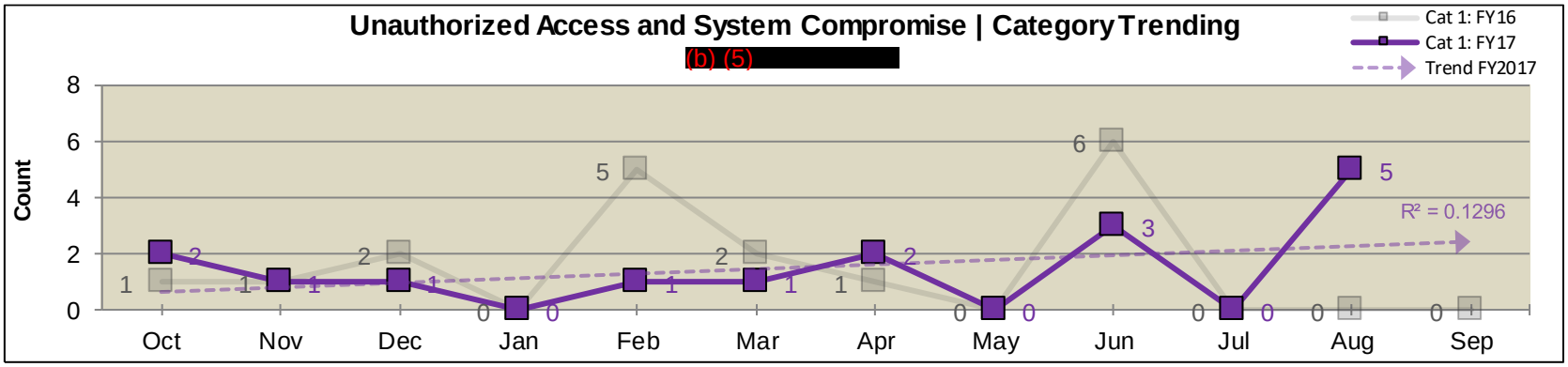
(b) (5) [redacted]

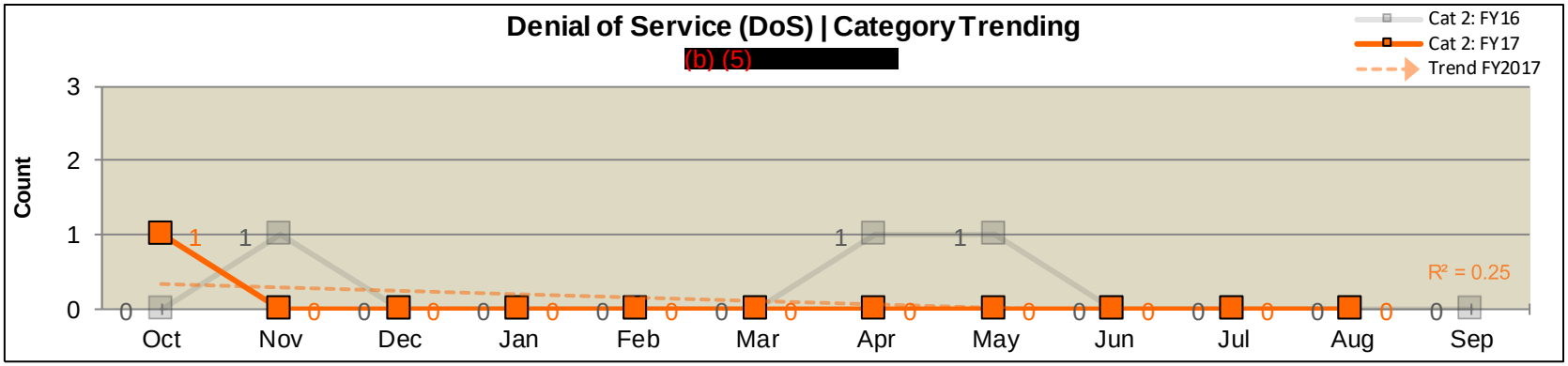
(b) (5) [redacted]

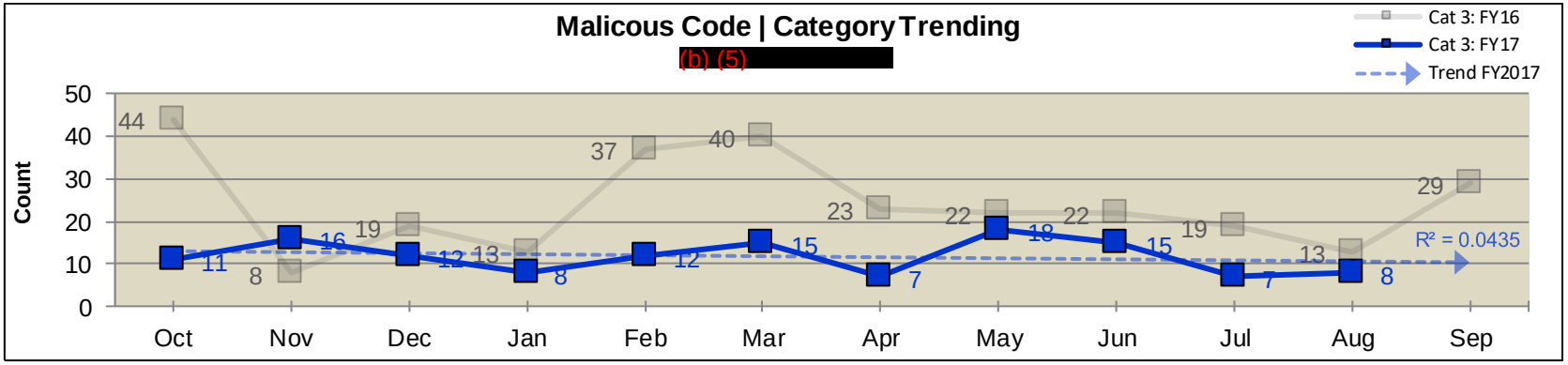
| | |
|---|---|
| Cat 0 | **Exercise / Network Defense Testing** \| Default Criticality: Defined by exercise \| US-CERT Reporting Requirement: n/a |
| Cat 1 | **Unauthorized Access & System Compromise** \| Default Criticality: High \| US-CERT Reporting Requirement: 1 hour |
| Cat 2 | **Denial of Service (DoS)** \| Default Criticality: High \| US-CERT Reporting Requirement: 2 hours |
| Cat 3 | **Malicious Code** \| Default Criticality: Medium \| US-CERT Reporting Requirement: 2 hours |
| Cat 4 | **Improper Usage** \| Default Criticality: Medium \| US-CERT Reporting Requirement: Weekly |
| Cat 5 | **Unauthorized Scans / Probes / Attempted Access** \| Default Criticality: Medium \| US-CERT Reporting Req: Monthly |
| Cat 6 | **Investigation** \| Default Criticality: Medium \| US-CERT Reporting Requirement: n/a |
| Cat 7 | **Currently Unused** |
| Cat 8 | **Personally Identifiable Information (PII)** \| Default Criticality: Medium \| US-CERT Reporting Requirement: 1 hour |

(b) (5)

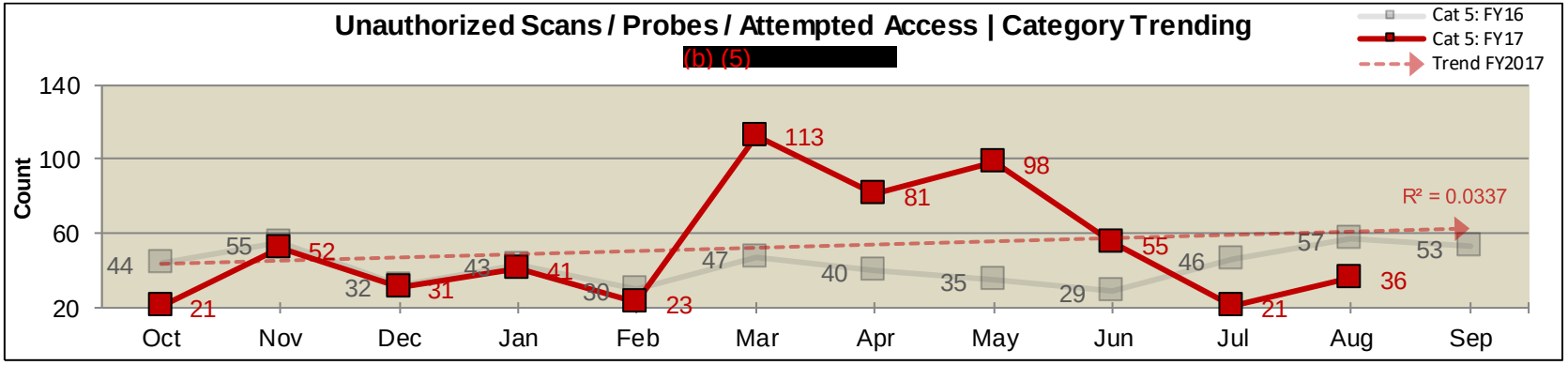
[redacted]


Unauthorized Access and System Compromise | Category Trending
(b) (5) [redacted]
Cat 1: FY16
Cat 1: FY17
Trend FY2017
Count
8
6
4
2
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.1296


Denial of Service (DoS) | Category Trending
(b) (5) [redacted]
Cat 2: FY16
Cat 2: FY17
Trend FY2017
Count
3
2
1
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.25

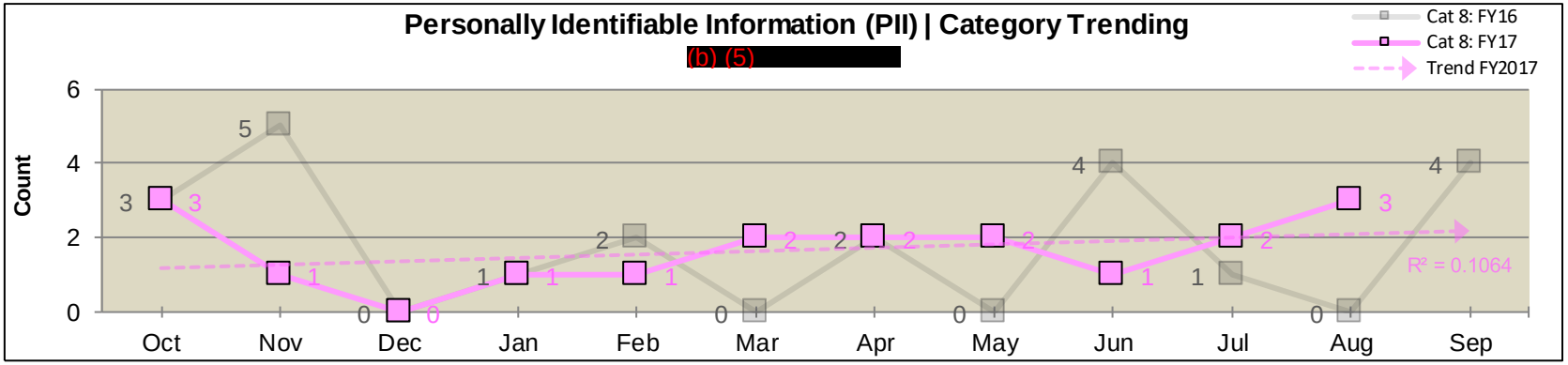

Malicous Code | Category Trending
(b) (5) [redacted]
Cat 3: FY16
Cat 3: FY17
Trend FY2017
Count
50
40
30
20
10
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
44
8
19
13
37
40
23
22
19
13
29
11
16
12
8
12
15
7
18
15
7
8
R² = 0.0435

(b) (5) [redacted]


Unauthorized Scans / Probes / Attempted Access | Category Trending
(b) (5) [redacted]
Cat 5: FY16
Cat 5: FY17
Trend FY2017
Count
140
100
60
20
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
44
55
32
43
30
47
40
35
29
46
57
53
21
52
31
41
23
113
81
98
55
21
36
R² = 0.0337

(b) (5)

[redacted]


Personally Identifiable Information (PII) | Category Trending
(b) (5) [redacted]
Cat 8: FY16
Cat 8: FY17
Trend FY2017
Count
6
4
2
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.1064

## 3.4 Attack Vector Report | NIST SP 800-61 (rev 2)

The purpose of this report is to show how attacks are occurring, the volume of each, trending, and annual comparisons. Data for this report is derived from a monthly Remedy data extraction (i.e. Remedy Tier 3). Remedy Tier 3 adheres to the official NIST SP 800-61 (rev 2) attack vectors. Event data includes incidents unless otherwise noted. The report reflects exactly how the data is recorded in Remedy. Data is updated by the 5th business day of each month.

| *Attack Vector* | NIST SP 800-61 (rev 2): Attack Vector Definitions |
|---|---|
| **External / Removable Media:** | An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive. |
| **Attrition:** | An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures). |
| **Web:** | An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware. |
| **Email:** | An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message. |
| **Impersonation:** | An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation. |
| **Improper Usage:** | Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; (Ex) a user installs file sharing software, leading to the loss of data; or a user performs illegal activities on a system. |
| **Loss or Theft of Equipment:** | The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token. |
| **Other:** | An attack that does not fit into any of the other categories. |

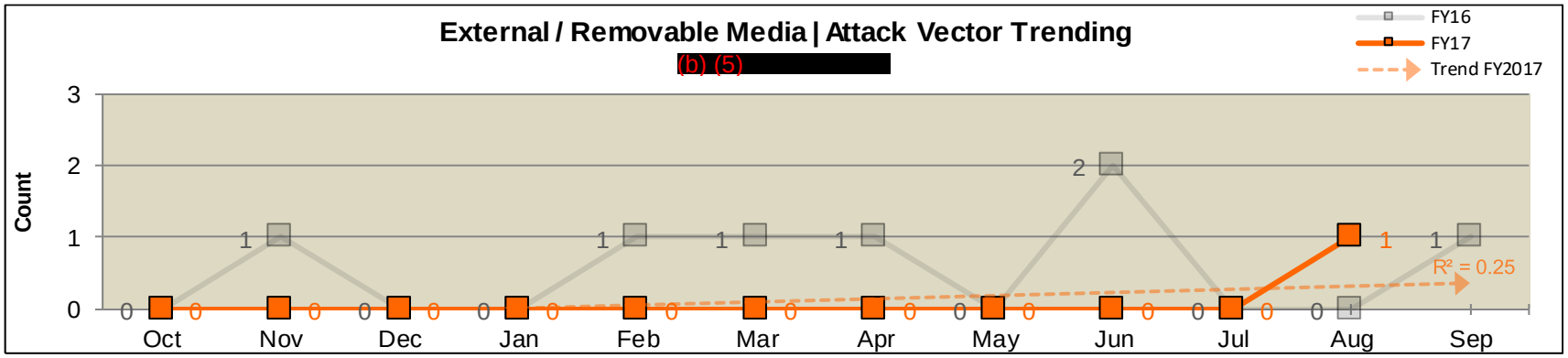
(b) (5)

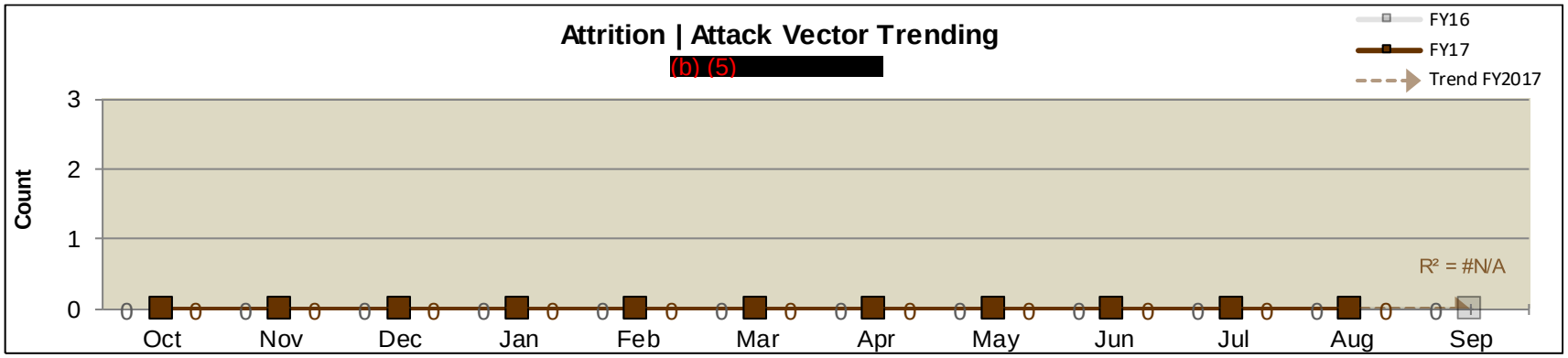
[redacted]

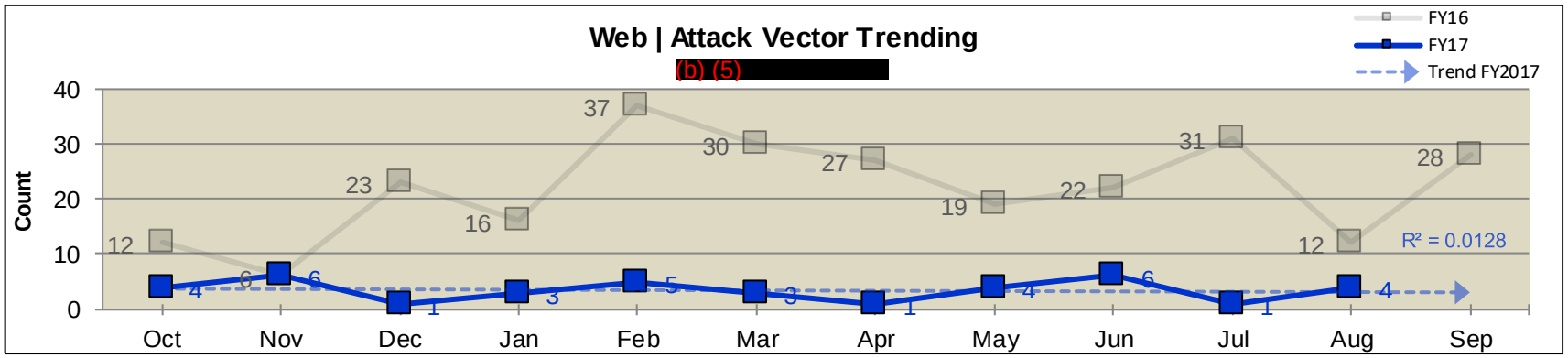
(b) (5)

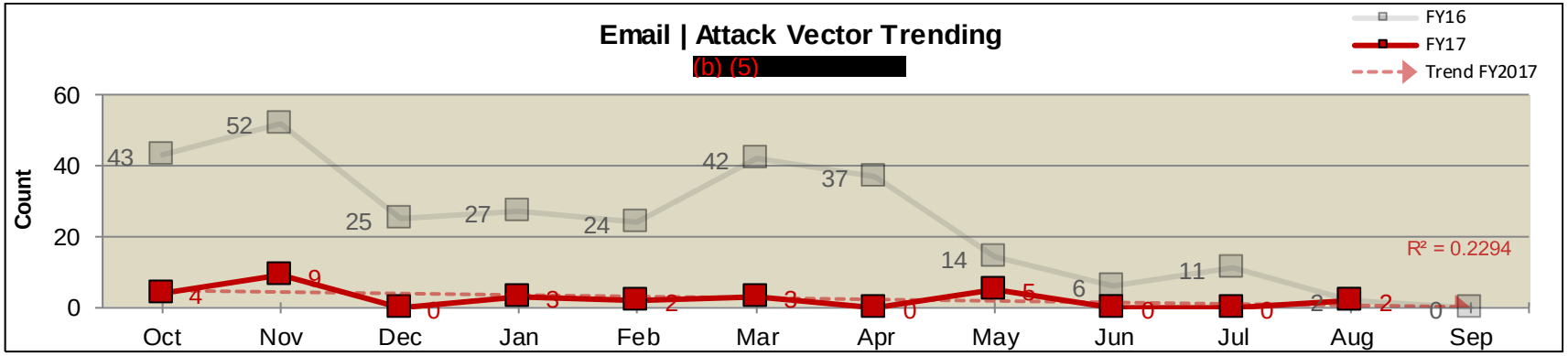
[redacted]

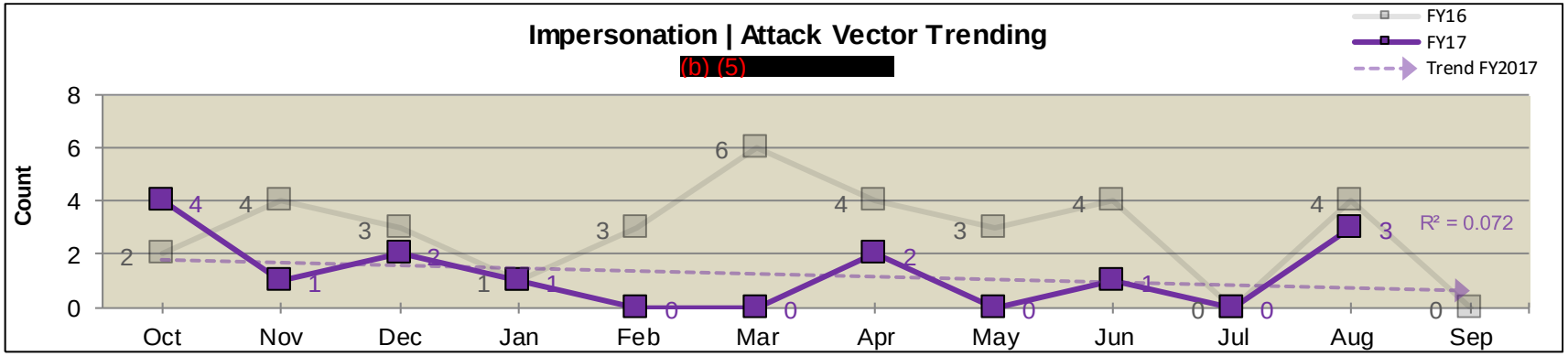
Exhibit 21: Attack Vector Report | Trending



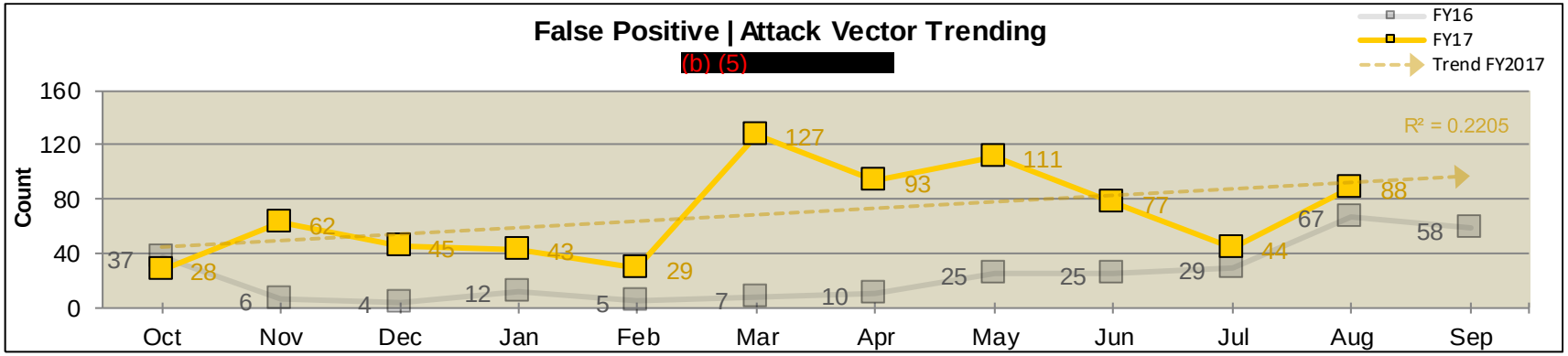

Email | Attack Vector Trending
(b) (5) [redacted]
FY16
FY17
Trend FY2017
Count
60
40
20
0
43
52
25
27
24
42
37
14
6
11
2
0
4
9
0
3
2
3
0
5
0
0
2
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.2294

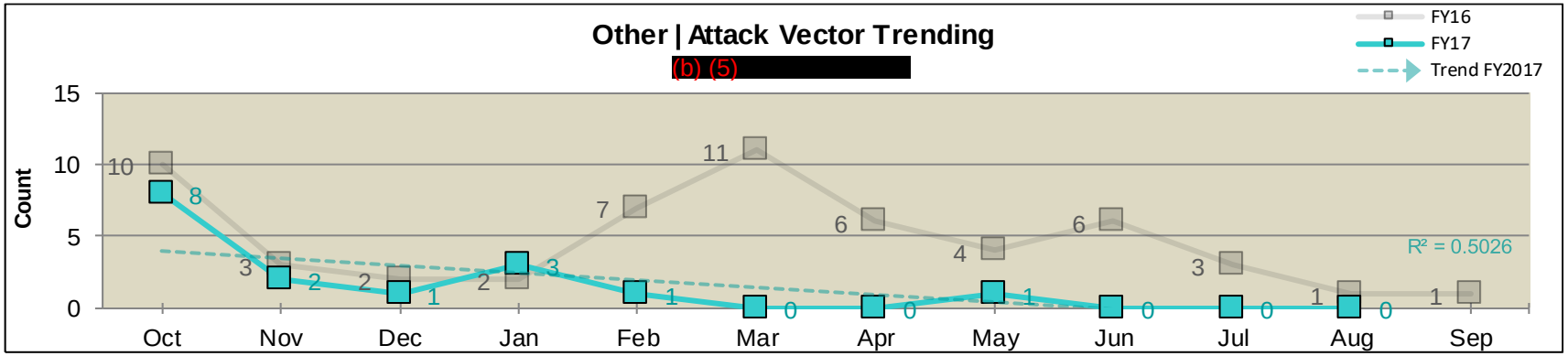

Impersonation | Attack Vector Trending
(b) (5) [redacted]
FY16
FY17
Trend FY2017
Count
8
6
4
2
0
2
4
4
3
1
3
1
1
3
6
0
0
4
2
3
0
4
1
0
0
4
3
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.072

(b) (5) [redacted]

(b) (5)

[redacted]


False Positive | Attack Vector Trending
(b) (5) [redacted]
FY16
FY17
Trend FY2017
Count
160
120
80
40
0
R² = 0.2205
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
37
28
6
62
4
45
12
43
5
29
7
127
10
93
25
111
25
77
29
44
67
88
58


Other | Attack Vector Trending
(b) (5) [redacted]
FY16
FY17
Trend FY2017
Count
15
10
5
0
R² = 0.5026
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
10
8
3
2
2
1
2
3
7
1
11
0
6
0
4
1
6
0
3
0
1
0
1

# 4 (b) (5) MTIPS Based Reports

## 4.1 (b) (5)

(b) (5)

(b) (5)

- (b) (5)
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(b) (5)

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

# 5 Executive Level Reports

## 5.1 Successful Incident Attack Report | PMC

The purpose of this report is the fulfillment of Section-E of the PMC (Presidential Management Council on Cybersecurity) reporting requirement. Metrics include total attack attempts, total successful attacks, and the percentage of successful attacks within a given time period. Total attack attempts are defined as detections observed from Symantec Endpoint Protection, FireEye and the Fortinet IPS system between a unique source IP address and destination address for each hour during the reporting time period (i.e. denominator). Total successful attacks are defined as Remedy logged incidents with definable malware (i.e. numerator). The percentage of successful attacks is defined as the 'Total Successful Attacks' divided by 'Total Attack Attempts'. This metric is reported on monthly and quarterly time periods.

| CSIRC ► Events ► Incidents ► Successful Attacks |
|---|
| Time Frame: **August FY17** |
| |
| Total Attack Attempts: **101,633** |
| |
| Total Successful Attacks: **12** |
| |
| Percentage of Successful Attacks: **0.0118%** |
| (b) (5) [redacted] |

| CSIRC ► Events ► Incidents ► Successful Attacks |
|---|
| Time Frame: **Q3 FY17** |
| |
| Total Attack Attempts: **77,749** |
| |
| Total Successful Attacks: **33** |
| |
| Percentage of Successful Attacks: **0.042%** |
| (b) (5) [redacted] |

# 6 (b) (5) [redacted]

## 6.1 (b) (5) [redacted]

[redacted]

[redacted]

[redacted]