CSIRC REPORTS

Monthly Analytic Synopsis

March 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
2.3 (b) (5) [redacted] 13
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 US-CERT Incident Report | PMC 33
5.2 Successful Incident Attack Report | PMC 34
5.3 PII Incident Report | OBM Memorandum M-07-16 34
6 (b) (5) [redacted] 35
6.1 (b) (5) [redacted] 35
7 **Appendix: Acronyms, Abbreviations, and Definitions** 35

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]

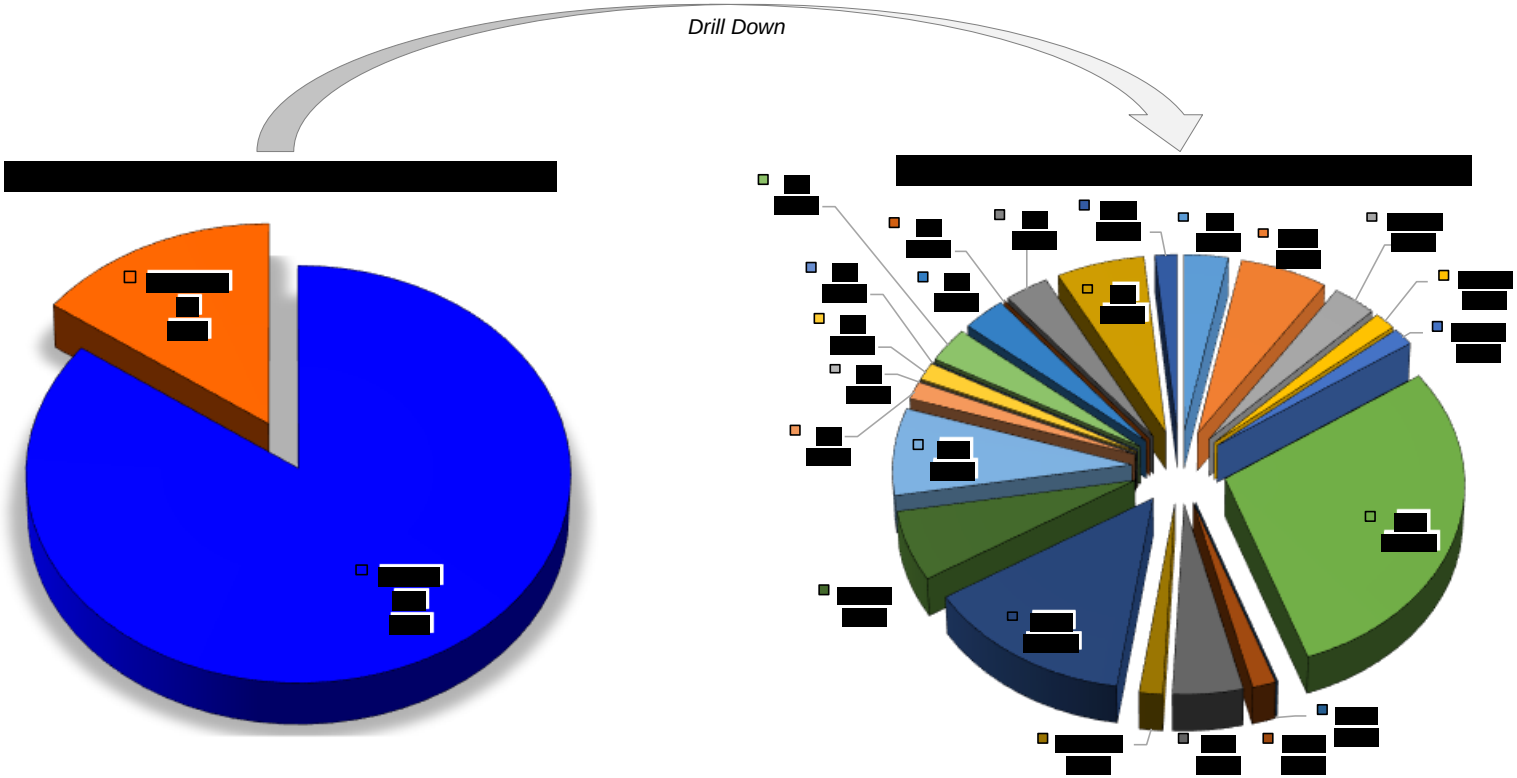
Revision Log

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
TBA	4.0	Version 4.0	(b) (6) [redacted]	[redacted]	TBA

1 Executive Summary

1.1 (b) (5) [redacted]

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



1.2 (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]	[redacted]	[redacted]	[redacted]	[redacted]

2 BigFix Based Reports

2.1 (b) (5) [redacted]

[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]

2.3 (b) (5) [redacted]

[redacted]

- [redacted]

3 Remedy Based Reports

3.1 (b) (5) [redacted]

[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.

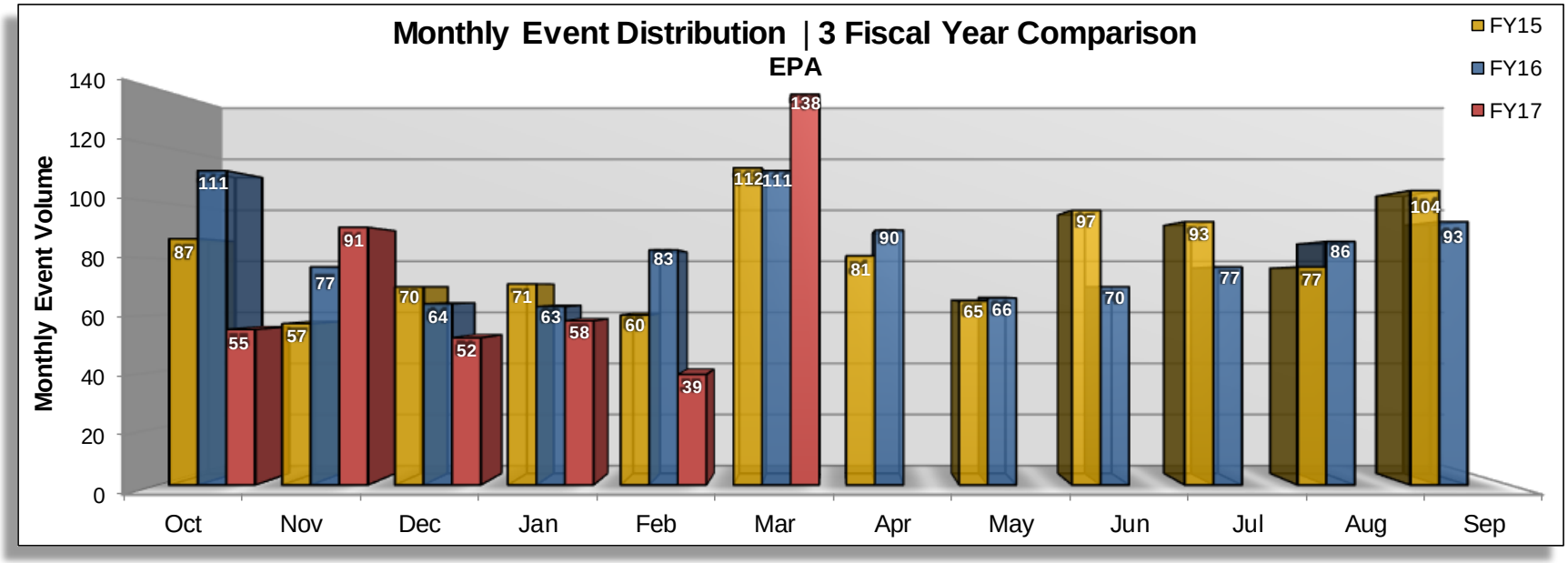
Examples of **Incidents** include the following:

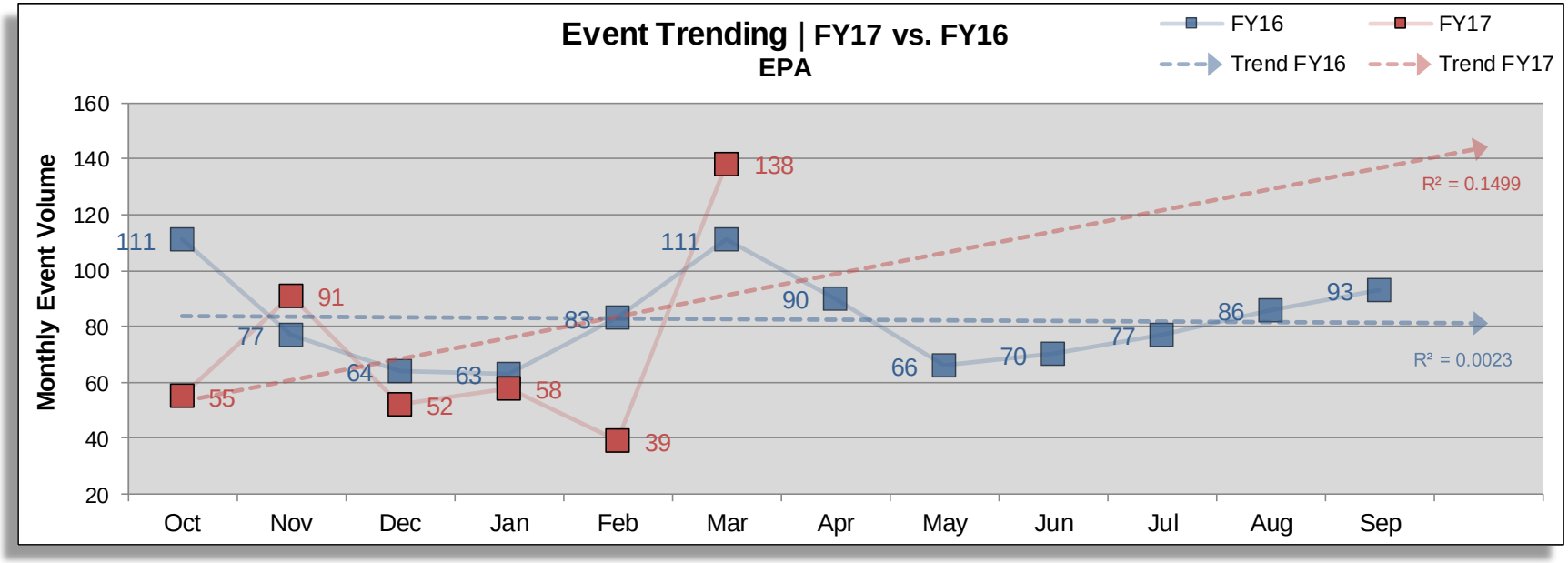
- User receives a phishing email & clicks on the link, which takes the user to a fake Microsoft website. LAN & password information is provided.
- While browsing the Internet, a user receives a pop-up from Microsoft support stating their system has a virus and to call a 1-800 number to help resolve the 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 **72** computer security related events **per month** in FY17.
Average (daily):	The agency is incurring an average of **3.5** computer security related events **per business day** in FY17.
High Month:	**March** is currently the most active month in FY2017 with **138** events. This represents **31.9%** of all events in FY17.
Low Month:	**February** is currently the least active month in FY2017 with **39** events. This represents **9.0%** of all events in FY17.
(b) (5) [redacted]	(b) (5) [redacted]
[redacted]	[redacted]
Trend (slope):	Events for FY17 (Oct 2016 through Sep 2017) have an **upward trend** ▲ (i.e. slope of linear regression) with a value of **0.0198.**

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

Exhibit 15: Event Report | Volume and Trending





« Return to Table of Contents

(b) (5)

[redacted]

(b) (5)

[redacted]

3.3 (b) (5) [redacted]

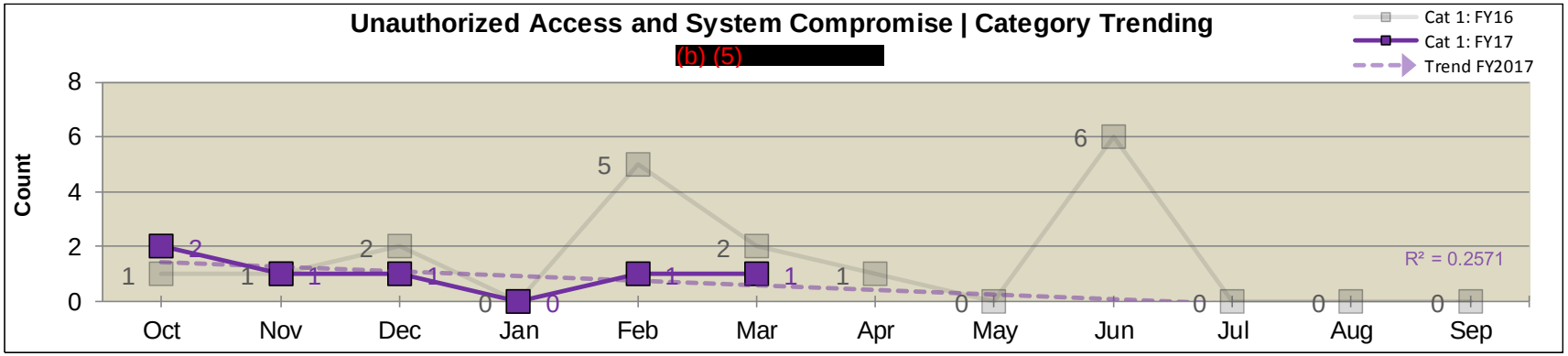
[redacted]

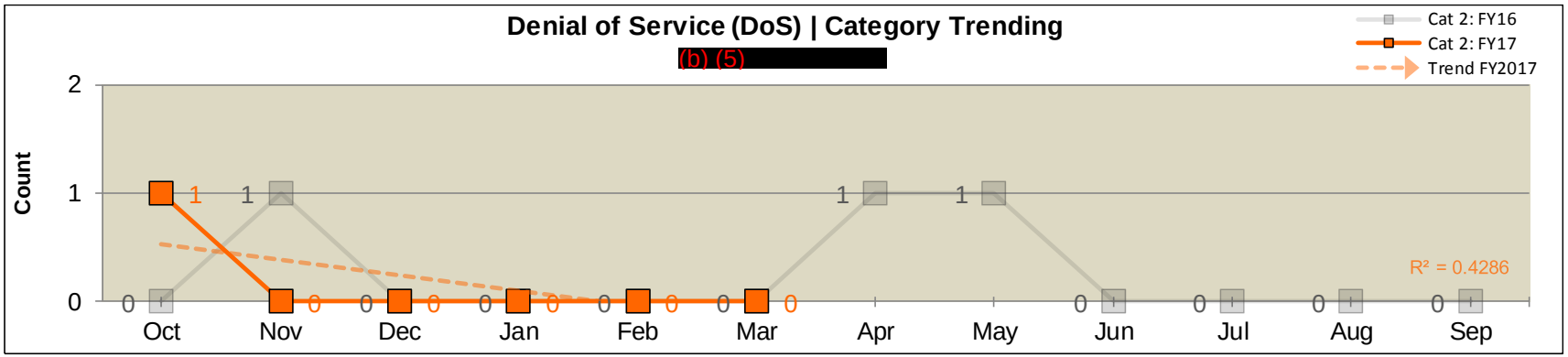
(b) (5) [redacted]

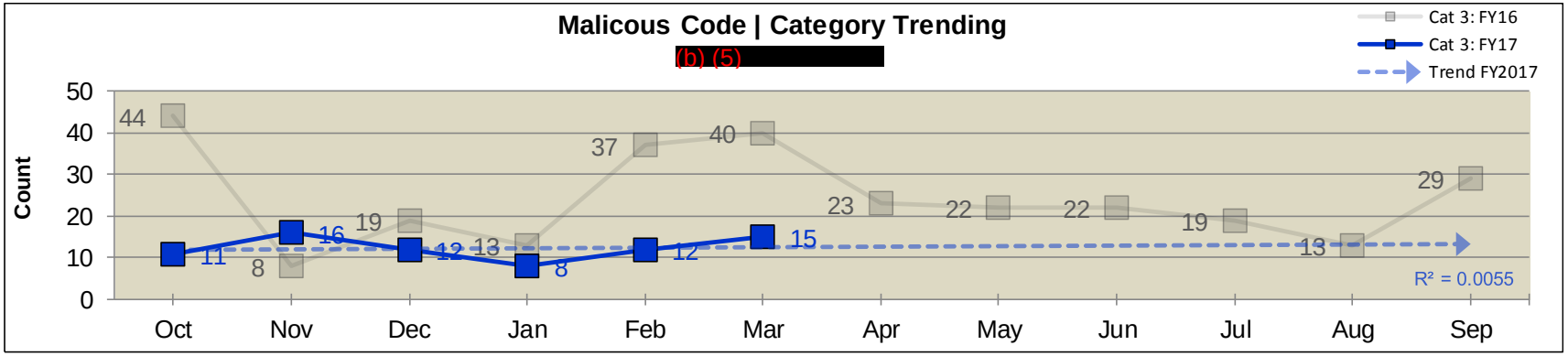
Cat 0	**Exercise / Network Defense Testing** | Default Criticality: Defined by exercise | US-CERT Reporting Requirement: n/a
Cat 1	**Unauthorized Access & System Compromise** | Default Criticality: High | US-CERT Reporting Requirement: 1 hour
Cat 2	**Denial of Service (DoS)** | Default Criticality: High | 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)

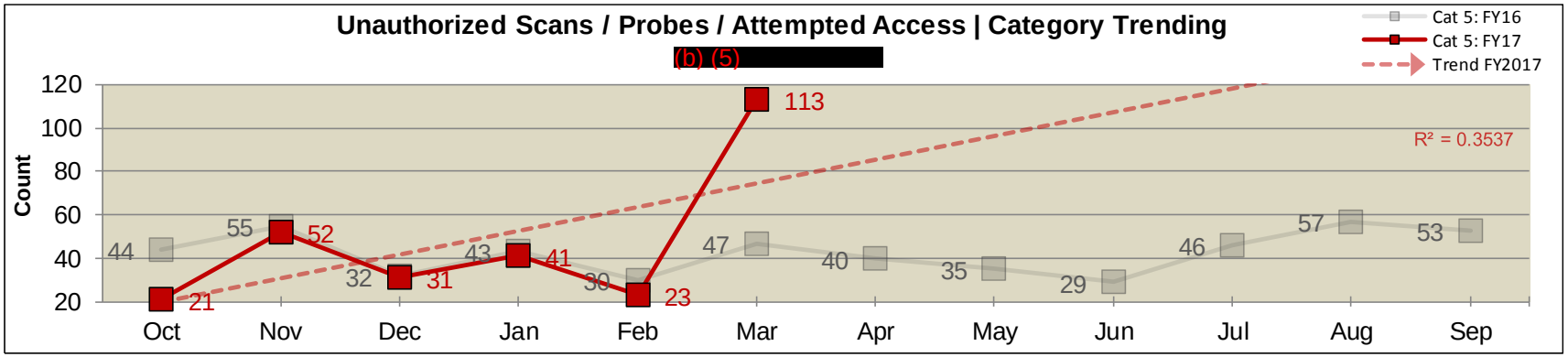
[redacted]


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 = 0.2571


Denial of Service (DoS) | Category Trending
(b) (5) [redacted]
Cat 2: FY16
Cat 2: FY17
Trend FY2017
Count
2
1
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.4286



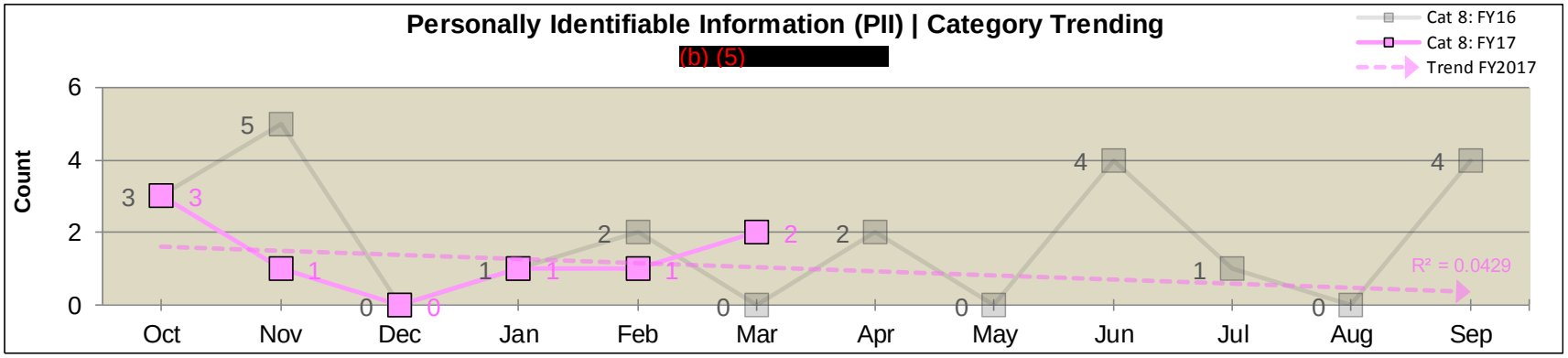
(b) (5) [redacted]



« Return to Table of Contents

(b) (5)

[redacted]


Personally Identifiable Information (PII) | Category Trending
(b) (5)
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
3
3
5
1
0
0
1
1
2
1
0
2
2
0
4
1
0
4
R² = 0.0429

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; for example, a user installs file sharing software, leading to the loss of sensitive 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.

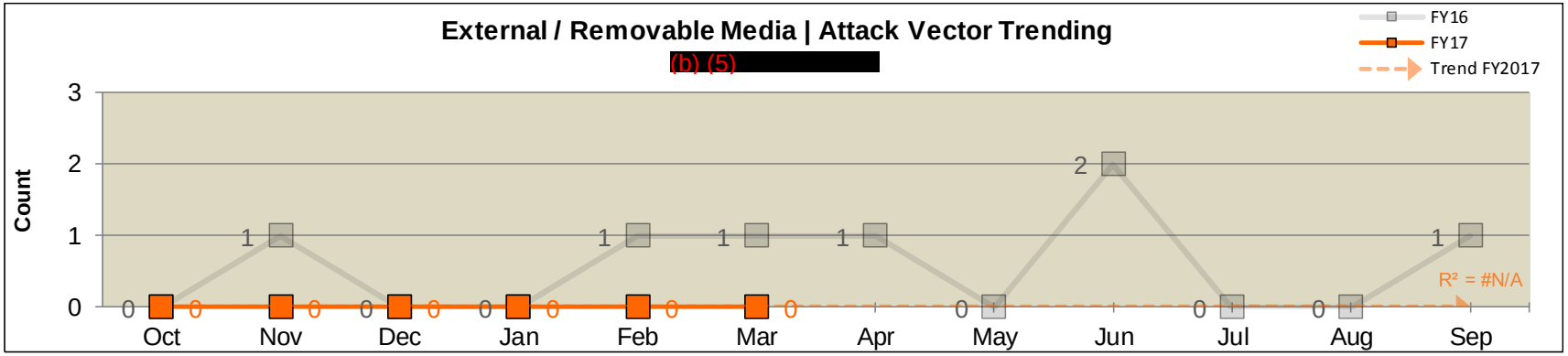
(b) (5)

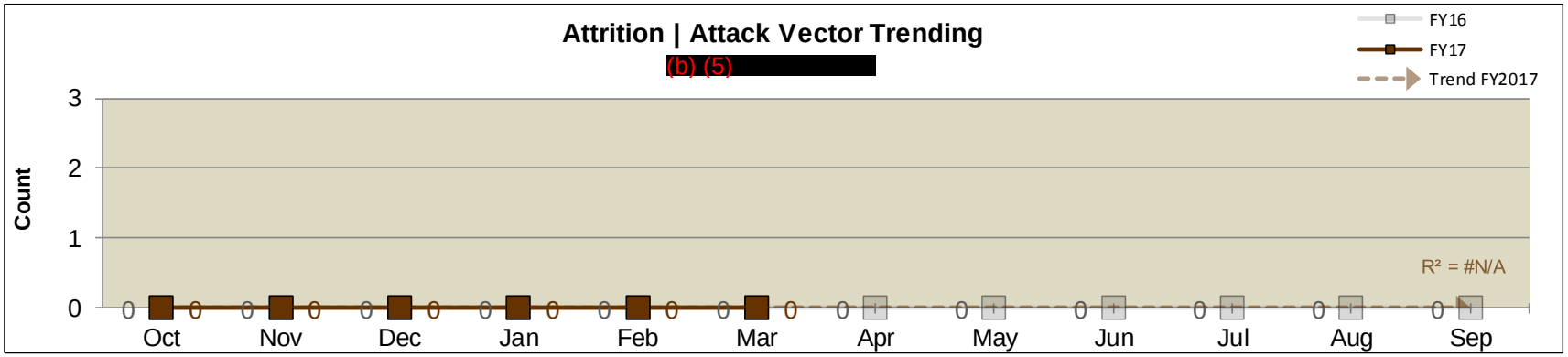
[redacted]

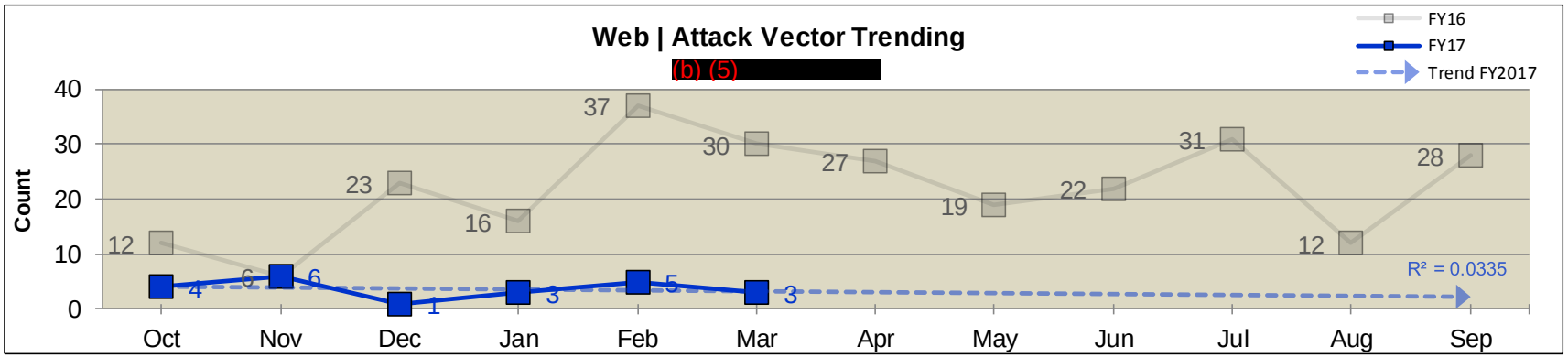
(b) (5)

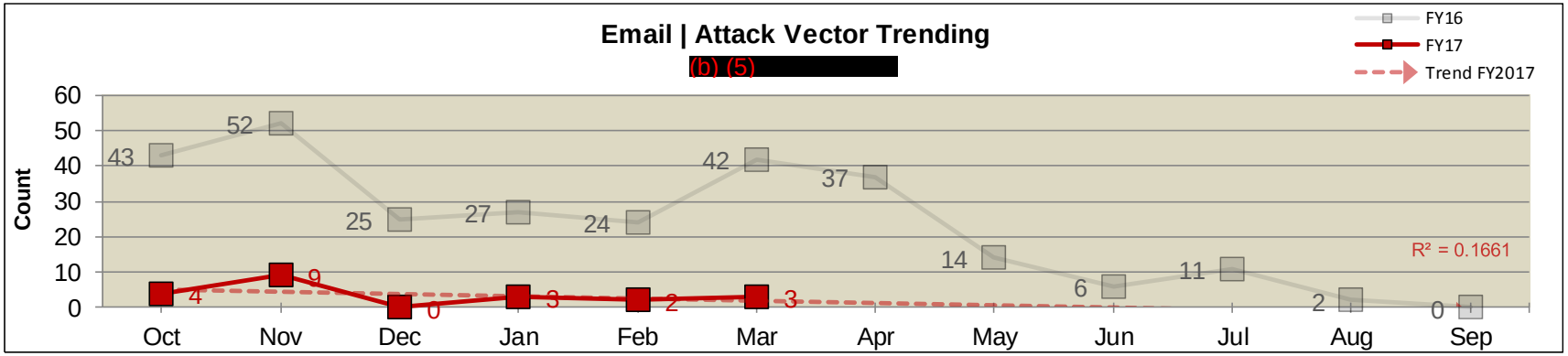
[redacted]

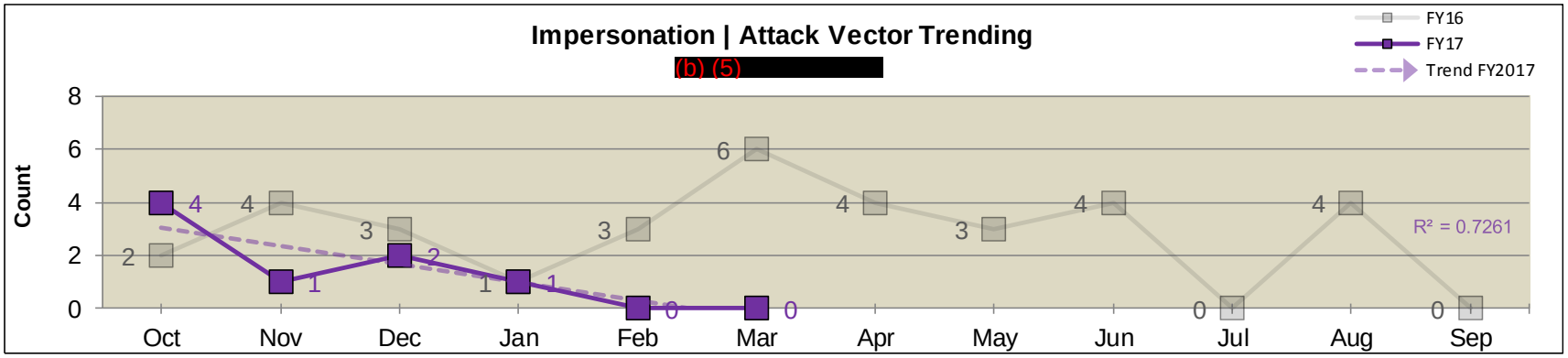
Exhibit 21: Attack Vector Report | Trending







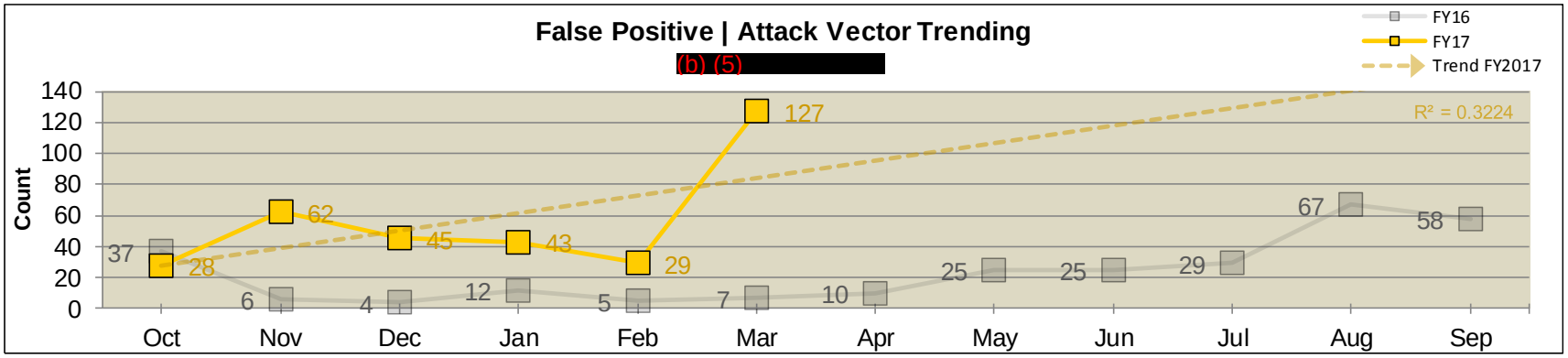

Email | Attack Vector Trending
(b) (5) [redacted]
FY16
FY17
Trend FY2017
Count
60
50
40
30
20
10
0
43
52
25
27
24
42
37
14
6
11
2
0
4
9
0
3
2
3
R² = 0.1661
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep

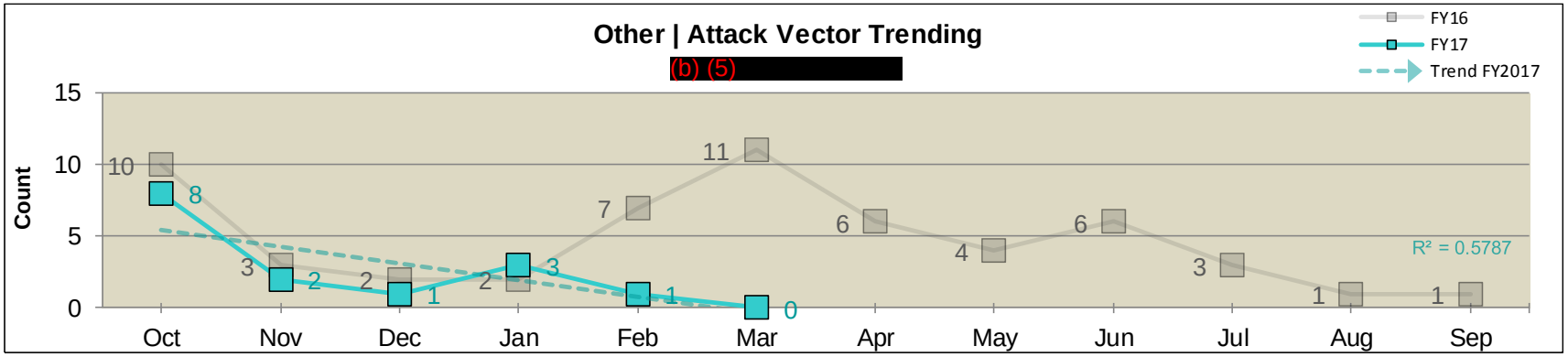

Impersonation | Attack Vector Trending
(b) (5) [redacted]
FY16
FY17
Trend FY2017
Count
8
6
4
2
0
2
4
4
3
3
6
4
3
4
0
4
0
4
1
2
1
1
0
0
R² = 0.7261
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep

(b) (5) [redacted]

(b) (5)

[redacted]


False Positive | Attack Vector Trending
(b) (5) [redacted]
FY16
FY17
Trend FY2017
Count
140
120
100
80
60
40
20
0
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
25
25
29
67
58
R² = 0.3224


Other | Attack Vector Trending
(b) (5) [redacted]
FY16
FY17
Trend FY2017
Count
15
10
5
0
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
4
6
3
1
1
R² = 0.5787

4 (b) (5) MTIPS Based Reports

4.1 (b) (5)

[redacted]

4.1.1 (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]

5 Executive Level Reports

5.1 US-CERT Incident Report | PMC

The purpose of this report is a fulfillment of the Presidential Management Council (PMC) on Cybersecurity reporting requirement. Data is sourced through Remedy and is reported on montly, quarterly, and previous 365 day reporting periods.

US-CERT Related Incidents ► Previous Month
Total US-CERT related incidents: **8**
(b) (5) [redacted]
Total US-CERT related incidents NOT Resolved: **1**
(b) (5) [redacted]
Total False Positives and/or Category 6 (Investigation): **0**
Total phishing incidents with clicking on link: **0**
(b) (5) [redacted]

US-CERT Related Incidents ► Previous Quarter
Total US-CERT related incidents: **36**
Total US-CERT related incidents NOT Resolved: **11**
Total False Positives and/or Category 6 (Investigation): **3**
Total phishing events with clicking on link: **0**
(b) (5) [redacted]

US-CERT Related Incidents ► Previous 365 Days
Total US-CERT related incidents: **117**
Total US-CERT related incidents NOT Resolved: **60**
Total False Positives and/or Category 6 (Investigation): **10**
Total phishing events with clicking on link: **0**
(b) (5) [redacted]

5.2 Successful Incident Attack Report | PMC

The purpose of this report is a fulfillment of Section-E of the PMC Self-Assessment. 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: **Previous Month**
Total Attack Attempts: **14,714**
Total Successful Attacks: **11**
Percentage of Successful Attacks: **0.18%**
(b) (5) [redacted]

CSIRC ► Events ► Incidents ► Successful Attacks
Time Frame: **Previous Quarter**
Total Attack Attempts: **28,245**
Total Successful Attacks: **28**
Percentage of Successful Attacks: **0.01%**
(b) (5) [redacted]

5.3 PII Incident Report | OBM Memorandum M-07-16

The purpose of this report is a fulfillment of OMB Memorandum M-07-16. Incidents involving personally identifiable information (PII) are tracked on a fiscal year-to-date basis. Metrics include total counts, relevance as expressed in whole percentages, and compliance statistics. Data is sourced through Remedy with only duplicates being excluded. This metric is reported on fiscal year to date.

CSIRC ► Events ► Personally Identifiable Information (PII)
Time Frame: **FY2017 to Date** (01 October 2016 - 31 Mar 2017)
Total EPA Events: **368**
Total EPA Events Involving Personally Identifiable Information (PII): **8**
Percent of CSIRC events regarding PII, in the given time frame (whole number): **2%**
Percent of PII related events reported to US-CERT within an hour: **100%**

6 (b) (5) [redacted]

[redacted]

[redacted]

[redacted]

7 Appendix: Acronyms, Abbreviations, and Definitions

Acronym / Abbreviation	Definition
AOR	Area of Responsibility
APT	Advanced Persistent Threat
CSIRC	Computer Security Incident Response Capability
DATA	Data, Analysis, Trending, and Alerting (Team)
DDoS	Distributed Denial of Service
DoD	Department of Defense
DNS	Domain Name System
ECSIM	Enterprise Computer Security Incident Management
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FY2015	Fiscal Year 2015
FY2016	Fiscal Year 2016
FY2017	Fiscal Year 2017
IDS	Intrusion Detection System
ISO	Information Security Officer
MTIPS	(b) (5) Managed Trusted Internet Protocol Service
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
SP	Special Publications
VPN	Virtual Private Network