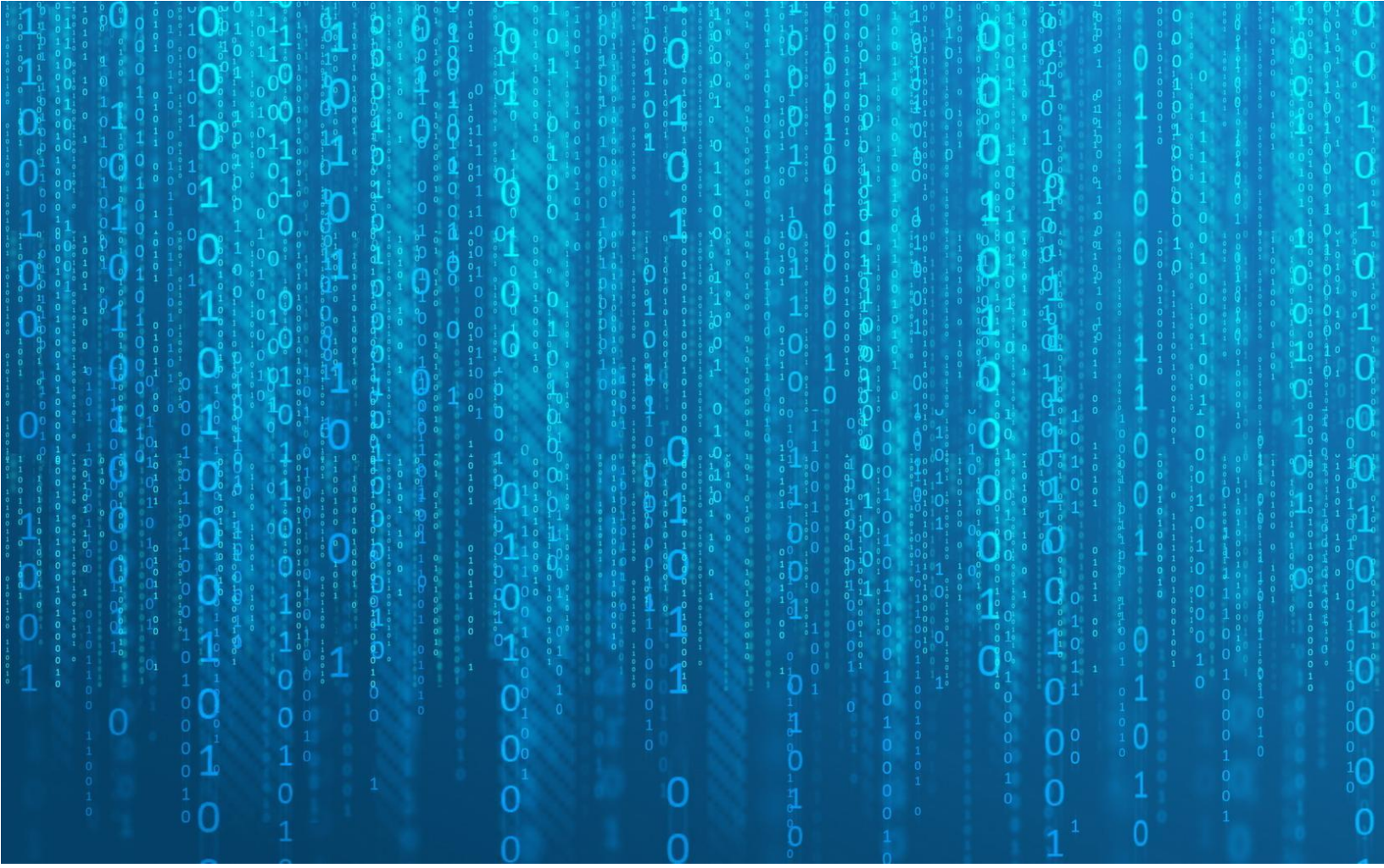


CSIRC REPORTS

Monthly Analytic Synopsis

January 2017

EPA Computer Security Incident Response Capability

TABLE OF CONTENTS

REVISION LOG iii
1 EXECUTIVE SUMMARY 1
2 BIGFIX BASED REPORTS 2
2.1 (b) (5) [redacted] 2
2.2 (b) (5) [redacted] 7
2.3 (b) (5) [redacted] 9
2.4 (b) (5) [redacted] 9
3 REMEDY BASED REPORTS 17
3.1 Open Ticket Trending and Distribution 17
3.2 Event / Incident Volume, Trending, and Distribution 19
3.3 Event Correlating Metrics 24
3.4 Event Category Trending and Distribution 27
3.5 Attack Vector Trending and Distribution 33
4 AT&T MTIPS BASED REPORTS 40
4.1 MTIPS Trending 40
4.1.1 MTIPS Blocked Category Definitions 40
5 EXECUTIVE LEVEL REPORTS 48
5.1 US-CERT Incident Report 48
5.2 Personally Identifiable Information (PII) Incident Report 51
5.3 Successful Incident Attack Report 52
6 FEEDBACK 53
6.1 CSIRC REPORTS Feedback eForm 53
7 PIPELINE 53
7.1 TBD 53
APPENDIX: ACRONYMS, ABBREVIATIONS, AND DEFINITIONS 54

LIST OF EXHIBITS

(b) (5) [redacted]

(b) (5)

(b) (5)

Exhibit 16: Event Volume | Annual Comparisons 20
Exhibit 17: Event Volume | Monthly Distribution (FY2017 vs. FY2016) 21

(b) (5)

Exhibit 22: Event Category Distribution | Annual Comparison 27

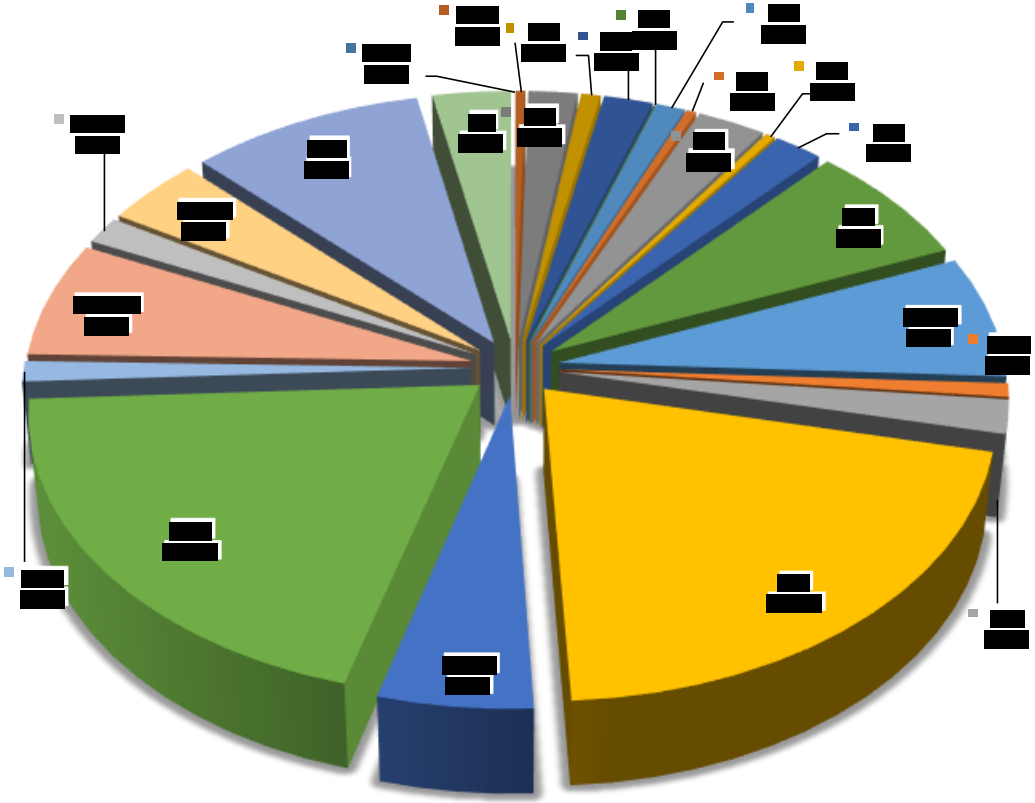
(b) (5)

REVISION LOG

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

1 EXECUTIVE SUMMARY

(b) (5)



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]

2.2 (b) (5) [redacted]

[redacted]

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5)

[redacted]

2.3 (b) (5) [redacted]

[redacted]

2.4 Installed (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]

3 REMEDY BASED REPORTS

3.1 (b) (5) [redacted]

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

3.2 Event / Incident Volume, Trending, and Distribution

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.

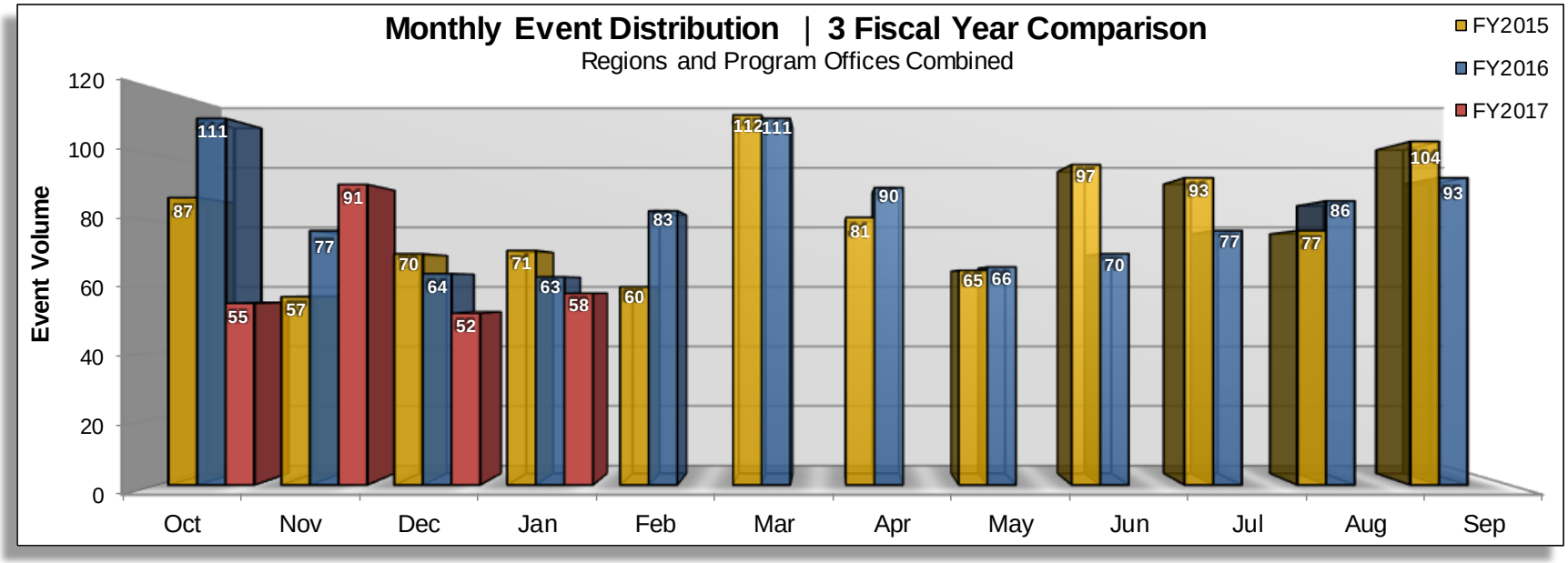
Examples of **Incidents** include the following:

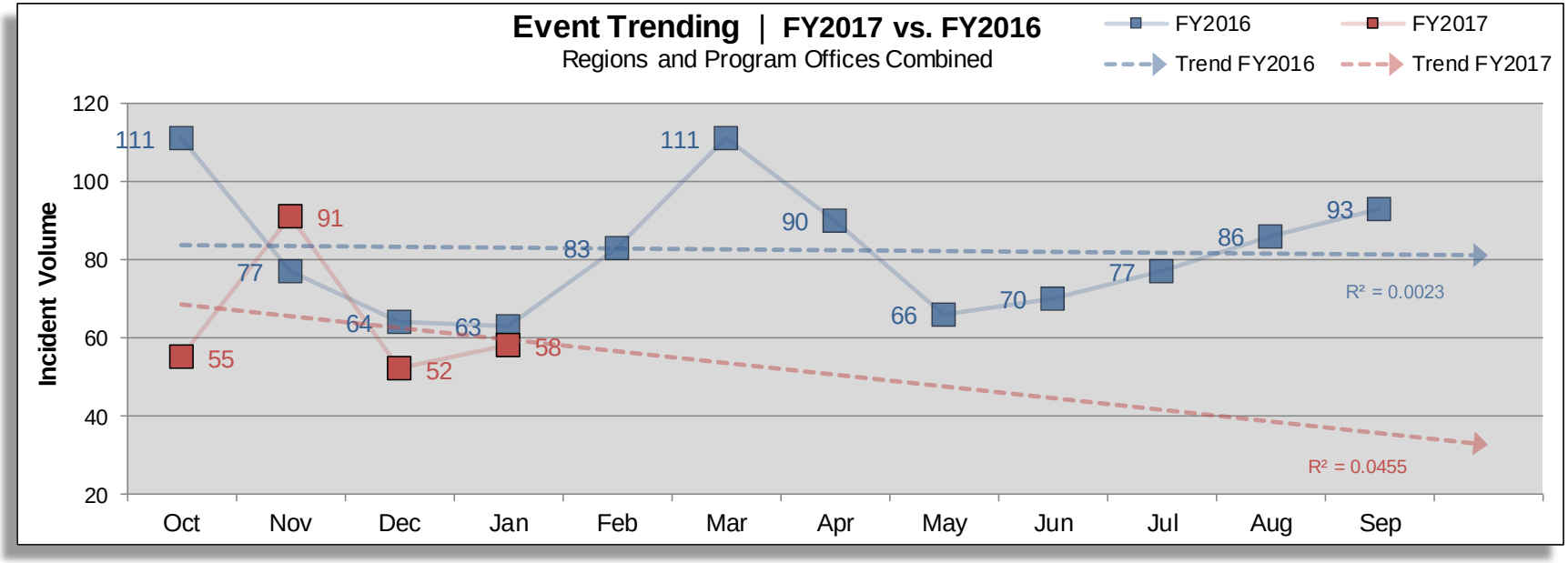
- User receives a phishing email & clicks on the link, which takes the user to a fake Microsoft website. LAN & password information is provided.
- While browsing the Internet, a user receives a pop-up from Microsoft support stating their system has a virus and to call a 1-800 number to help resolve the 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.

FY2017	Corresponding Statistics for Computer Security Events (FY2017)
Average (monthly):	The agency is incurring an average of **64** computer security related events **per month** in FY2017.
Average (daily):	The agency is incurring an average of **3.2** computer security related events **per business day** in FY2017.
High Month:	**November** is currently the most active month in FY2017 with **91** events. This represents **36%** of all events in FY2017.
Low Month:	**December** is currently the least active month in FY2017 with **52** events. This represents **20%** of all events in FY2017.
(b) (5) [redacted]	(b) (5) [redacted]
(b) (5) [redacted]	[redacted]
Trend (slope):	Events for FY2017 (Oct 2016 through Sep 2017) have an **downward trend** ▼ (i.e. slope of linear regression) with a value of **-0.0152.**

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

Exhibit 16: Event Volume | Annual Comparisons

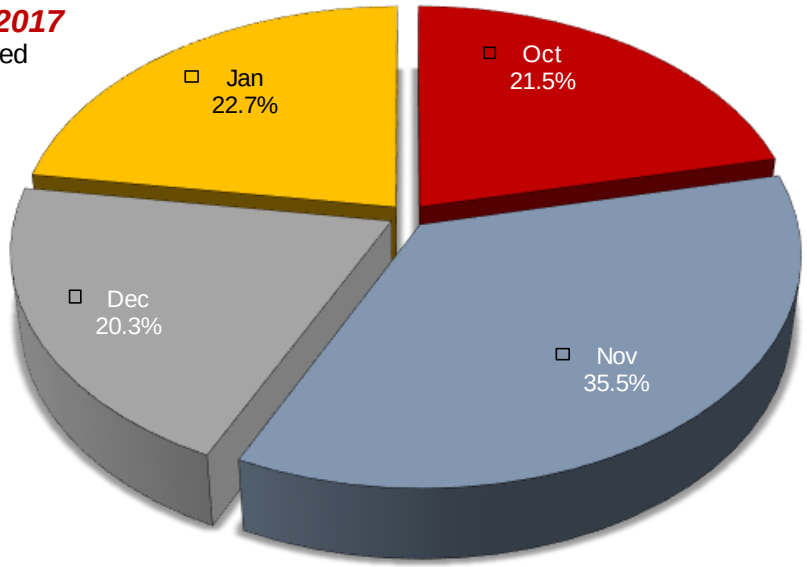




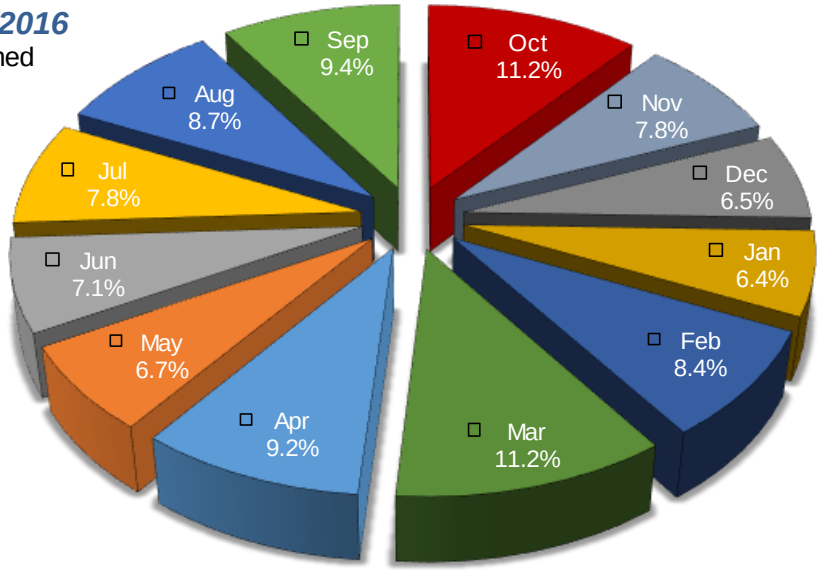
« Return to Table of Contents

Exhibit 17: Event Volume | Monthly Distribution (FY2017 vs. FY2016)

Monthly Event Distribution | *FY2017*
Regions and Program Offices Combined



Monthly Event Distribution | *FY2016*
Regions and Program Offices Combined



(b) (5)

[redacted]

(b) (5)

[redacted]

3.3 Event Correlating Metrics

The purpose of this report is to show correlation between events and contributing factors. Event Urgency Level is a field characterizing the urgency level of the event (low, medium, high, or critical). Reported Source is a metric showing how events are being reported (i.e. phone, email, direct input, or other). Data for this metric is derived from a monthly Remedy data extraction. Event data includes events 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.

FY2017	Statistics for Event Correlating Metrics (FY2017)	
Urgency Level		
Low	**20.3** is the monthly average of low events.	**61** is the total number of low level events for FY2017.
Medium	**65.0** is the monthly average of medium events.	**195** is the total number of mediun level events for FY2017.
High	**0.0** is the monthly average of high events.	**0** is the total number of high level events for FY2017.
Critical	**0.0** is the monthly average of critical events.	**0** is the total number of critical level events for FY2017.
Reported Source		
Email	**60.9%** of the time events are reported by email.	**156** computer security events have been reported by email.
Phone	**28.1%** of the time events are reported by phone.	**72** computer security events have been reported by phone.
Direct Input	**10.9%** of the time events are reported by direct input.	**28** computer security events have been reported direct input.

FY2016	Statistics for Event Correlating Metrics (FY2016)	
Urgency Level		
Low	**26.4** was the monthly average of low events.	**262** was the total number of low level events for FY2016.
Medium	**73.3** was the monthly average of medium events.	**726** was the total number of mediun level events for FY2016.
High	**0.3** was the monthly average of high events.	**3** was the total number of high level events for FY2016.
Critical	**0.0** was the monthly average of critical events.	**0** was the total number of critical level events for FY2016.
Reported Source		
Email	**52.6%** of the time events were reported by email.	**521** computer security events were reported by email.
Phone	**24.6%** of the time events were reported by phone.	**244** computer security events were reported by phone.
Direct Input	**22.8%** of the time events were reported by direct input.	**226** computer security events were reported direct input.

(b) (5)

[redacted]

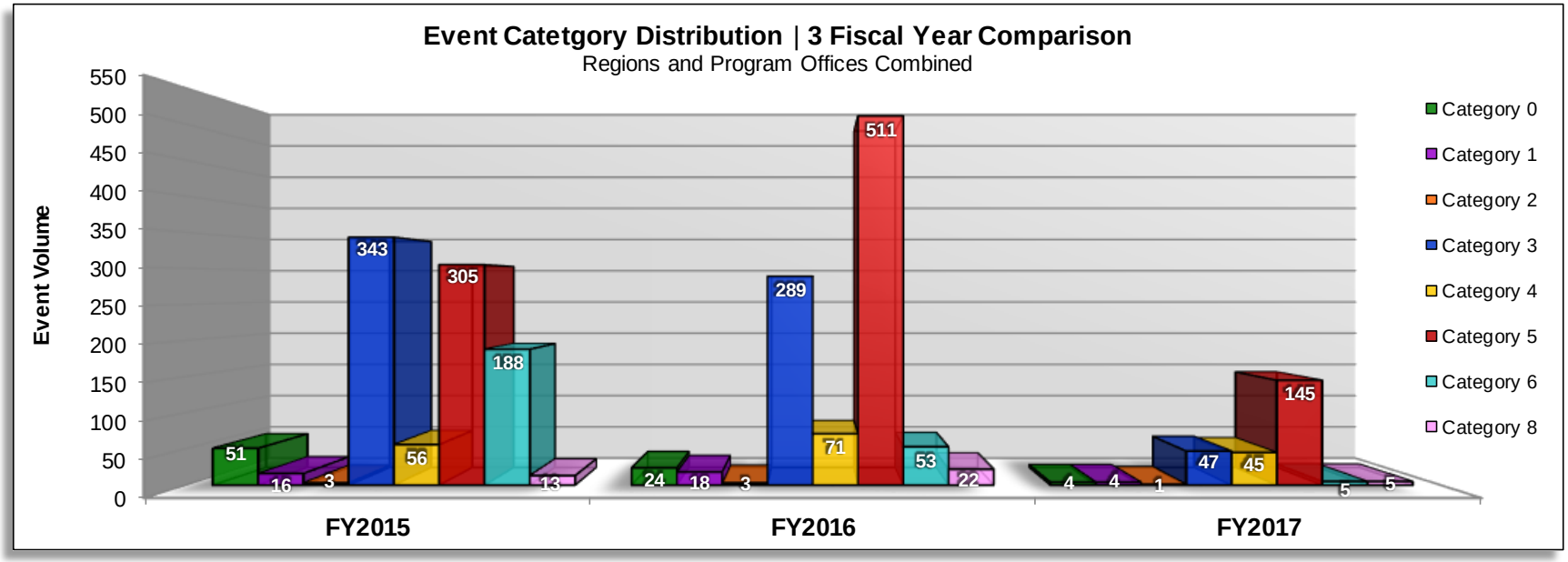
(b) (5)

[redacted]

3.4 Event Category Trending and Distribution

The purpose of this report is to show what attacks are occurring, the volume of each, and associated trending. Data for this report is derived from a monthly Remedy data extraction (i.e. Remedy Tier 2). Remedy Tier 2 adheres to the CSIRC Incident Categorization Matrix. 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.

Exhibit 22: Event Category Distribution | Annual Comparison



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

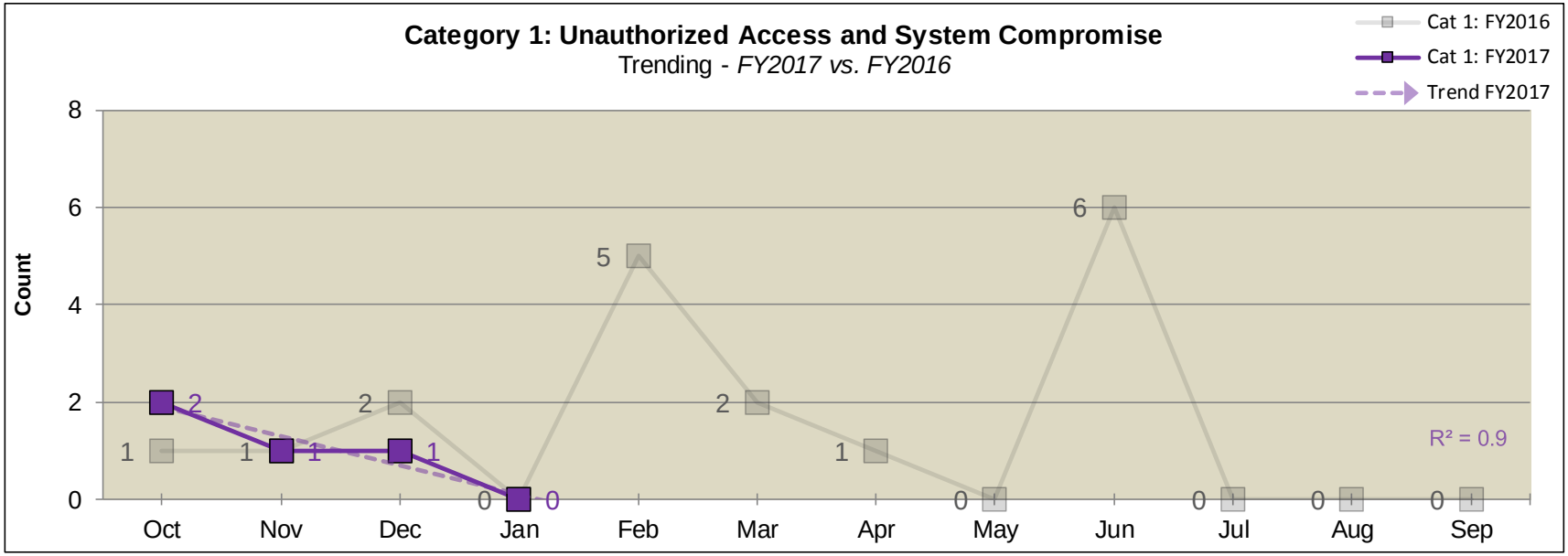
(b) (5)

[redacted]

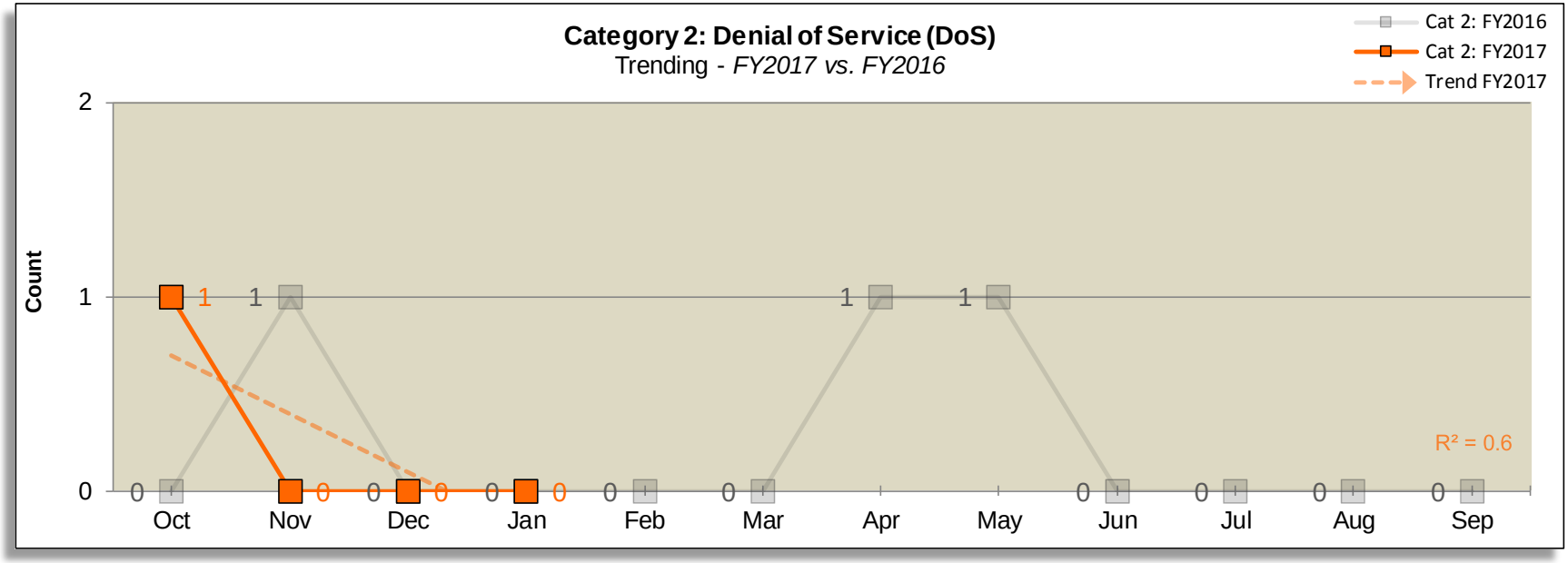
Cat 0	**Exercise / Network Defense Testing** | Default Criticality: Defined by exercise | US-CERT Reporting Requirement: n/a
Cat 1	**Unauthorized Access & System Compromise** | Default Criticality: High | US-CERT Reporting Requirement: 1 hour
Cat 2	**Denial of Service (DoS)** | Default Criticality: High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

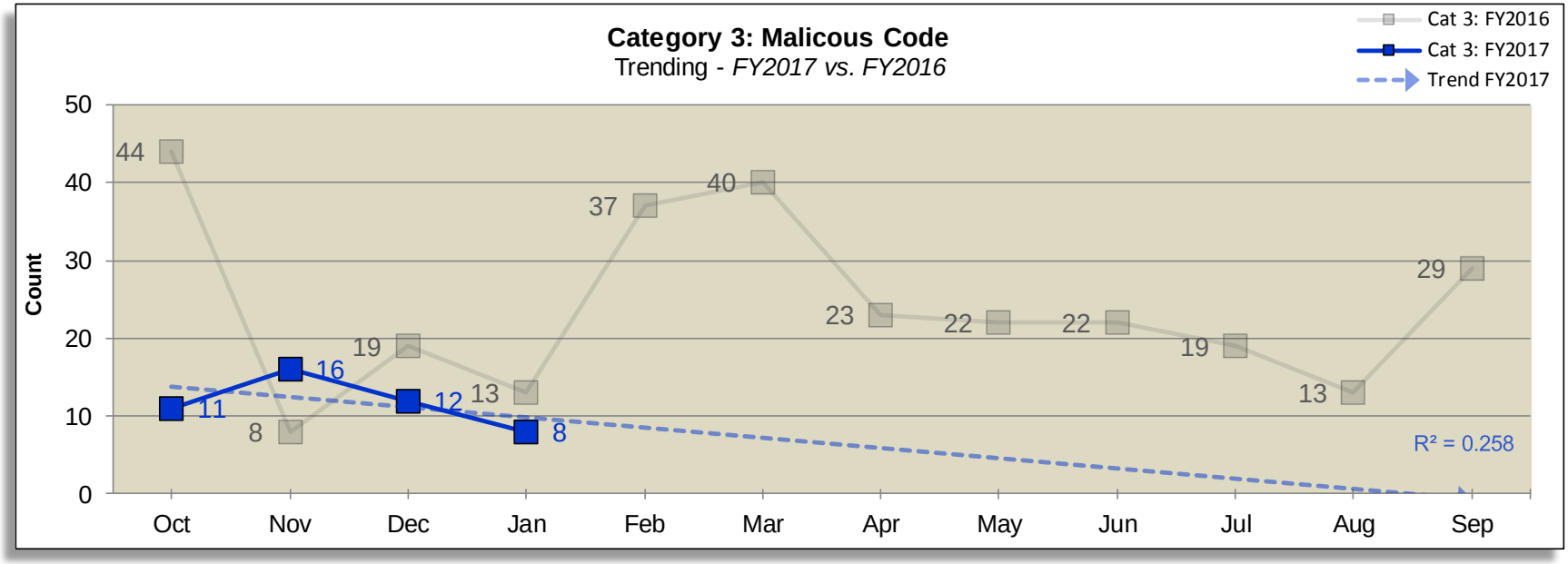
(b) (5)

[redacted]



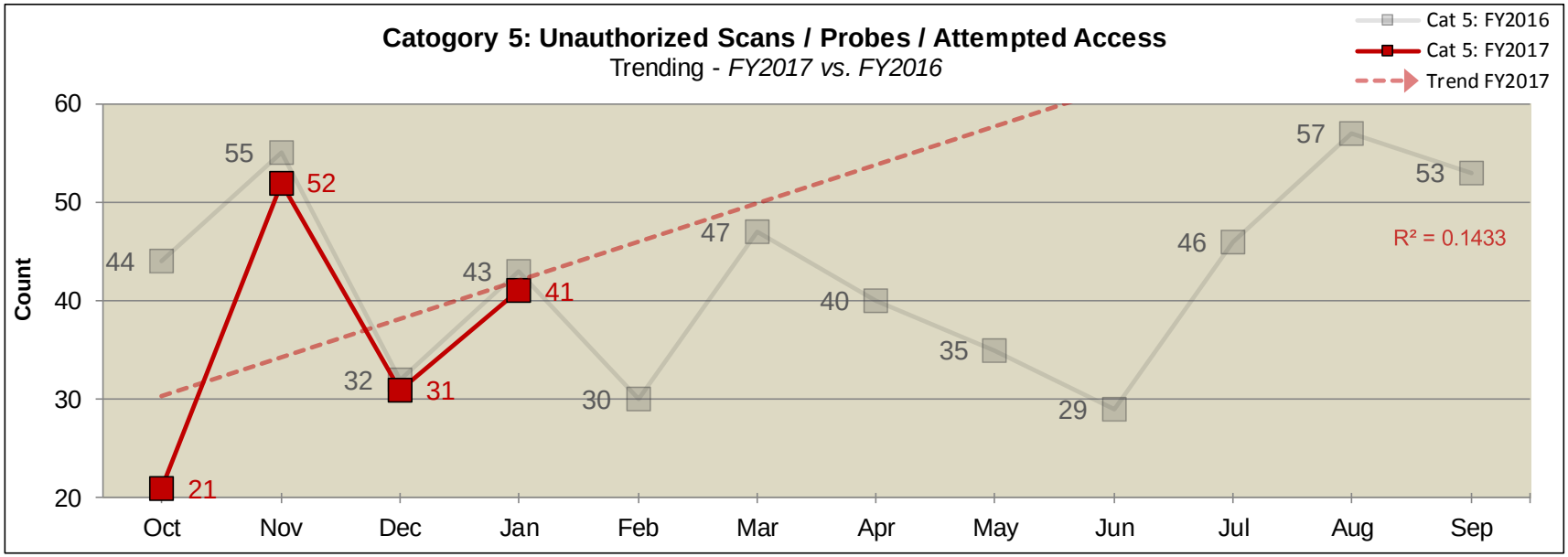
« Return to Table of Contents


Category 2: Denial of Service (DoS)
Trending - FY2017 vs. FY2016
Cat 2: FY2016
Cat 2: FY2017
Trend FY2017
Count
2
1
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.6


Category 3: Malicous Code
Trending - FY2017 vs. FY2016
Cat 3: FY2016
Cat 3: FY2017
Trend FY2017
Count
50
40
30
20
10
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.258

(b) (5)

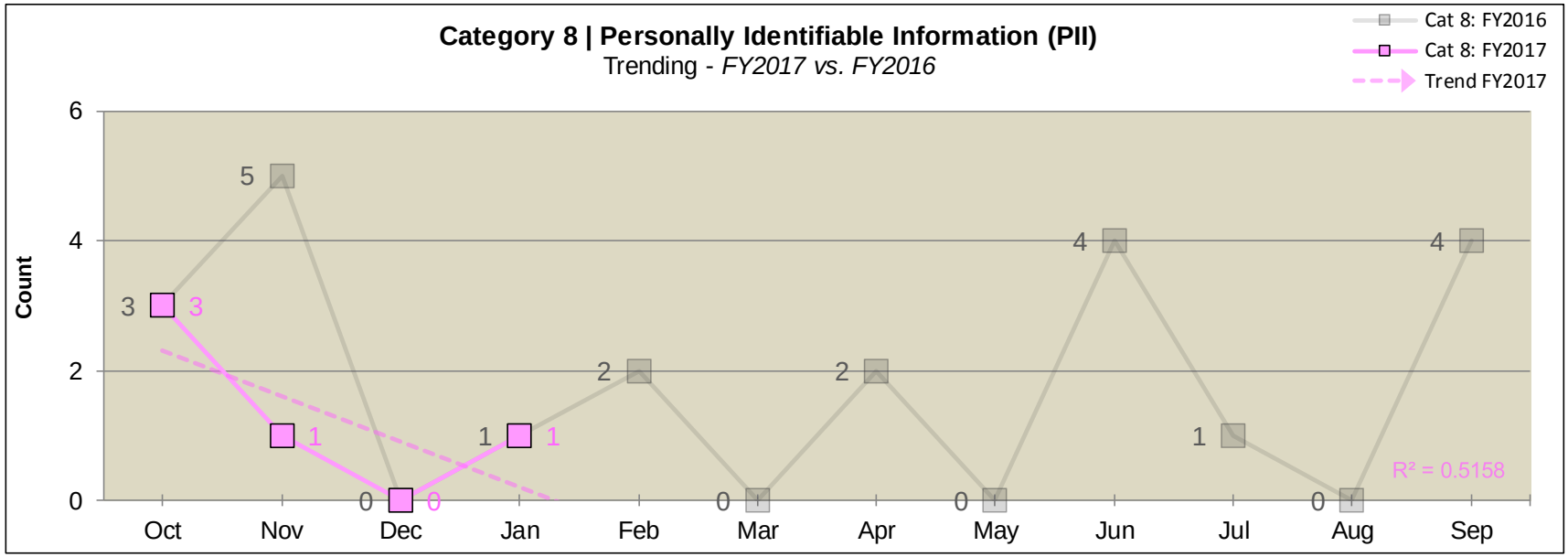
[redacted]



« Return to Table of Contents

(b) (5)

[redacted]



« Return to Table of Contents

3.5 Attack Vector Trending and Distribution

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 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: 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.

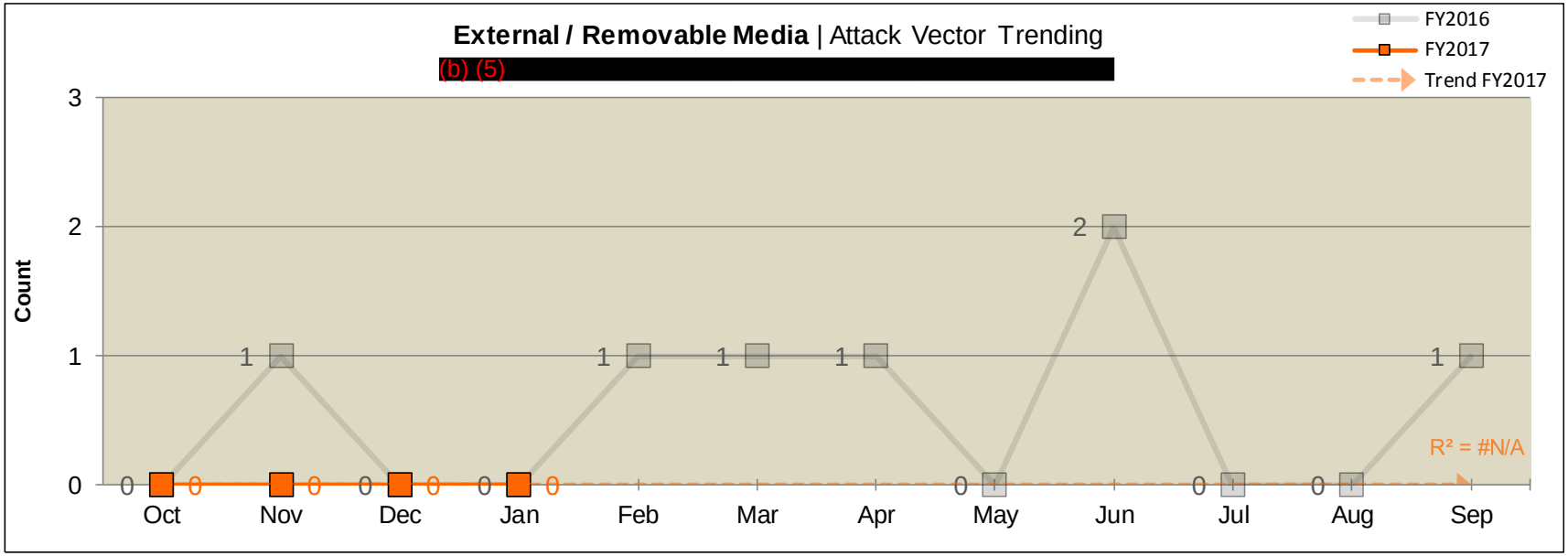
(b) (5)

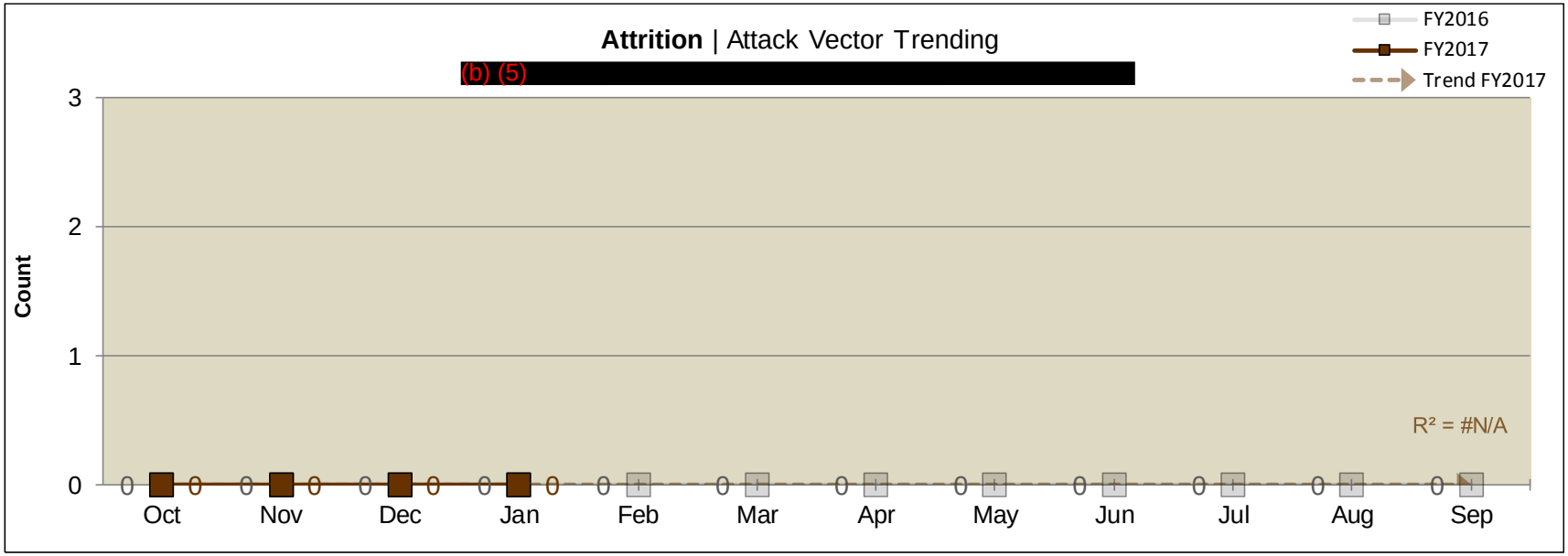
[redacted]

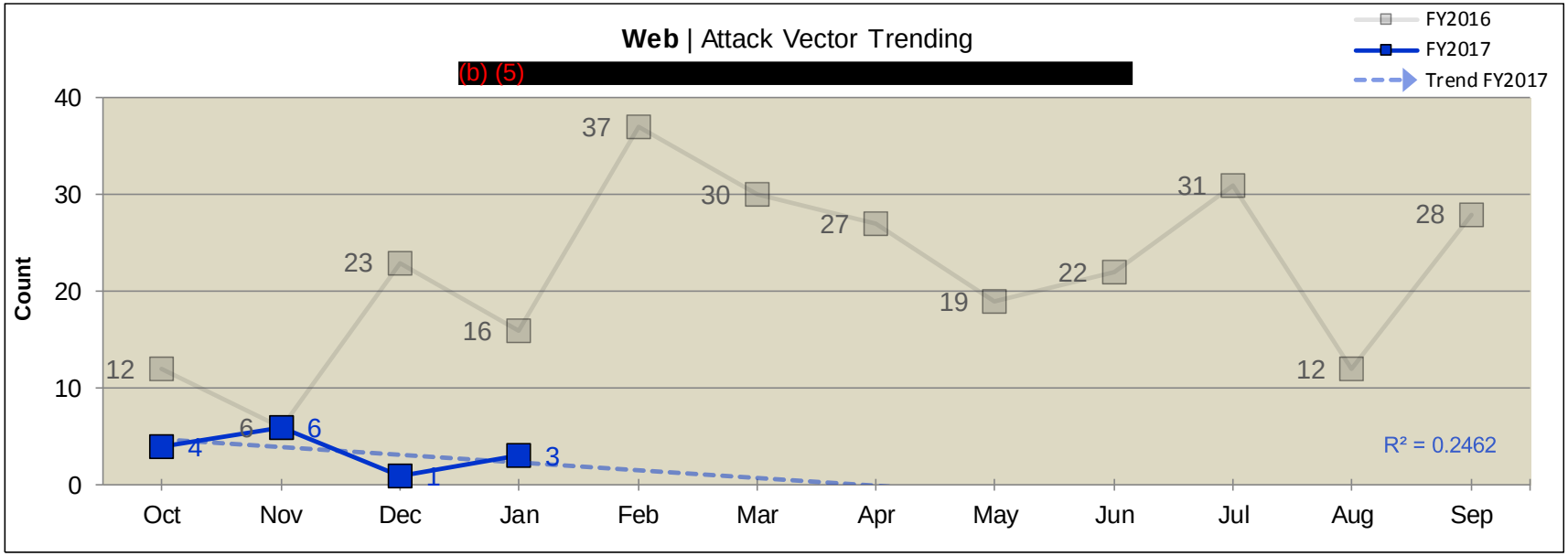
(b) (5)

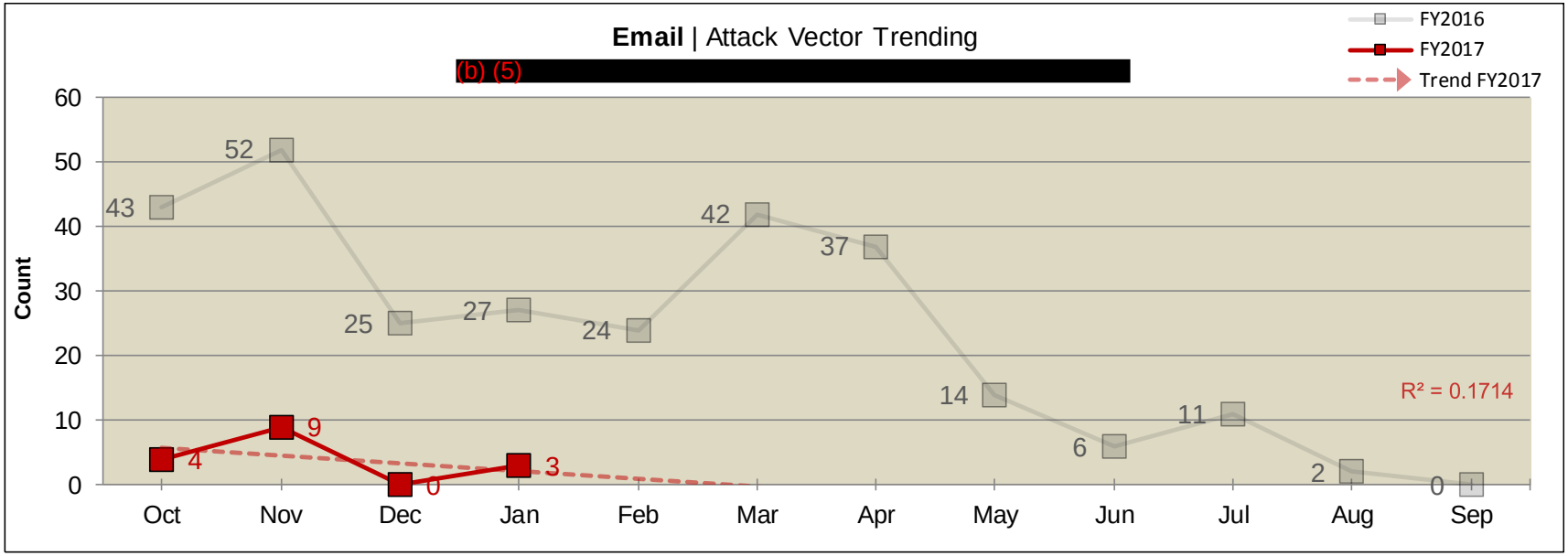
[redacted]

Exhibit 26: Attack Vector | Trending

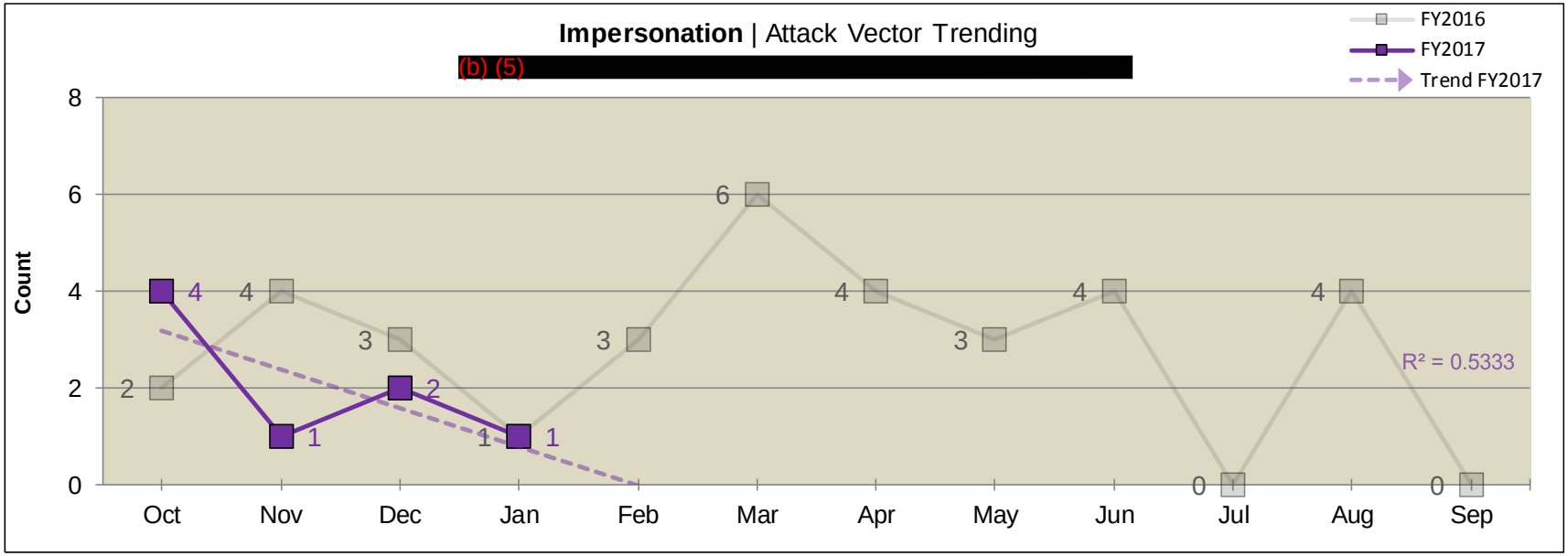








« Return to Table of Contents

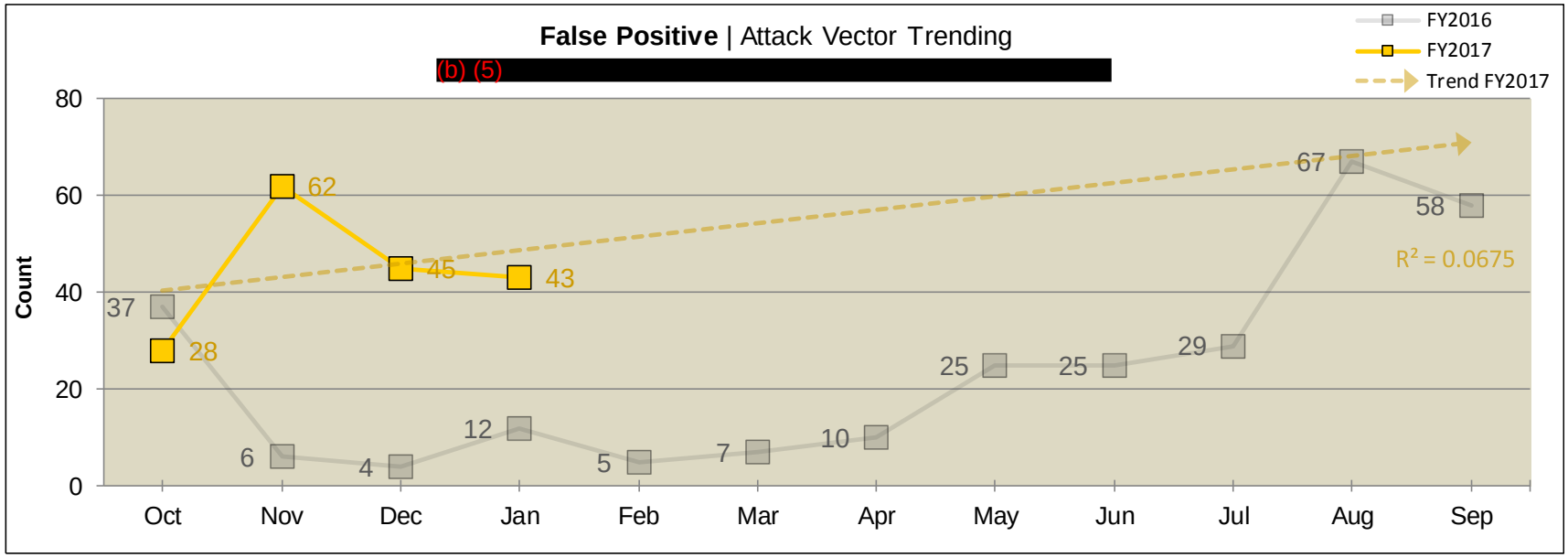

Impersonation | Attack Vector Trending
(b) (5)
FY2016
FY2017
Trend FY2017
Count
8
6
4
2
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
R² = 0.5333

(b) (5)

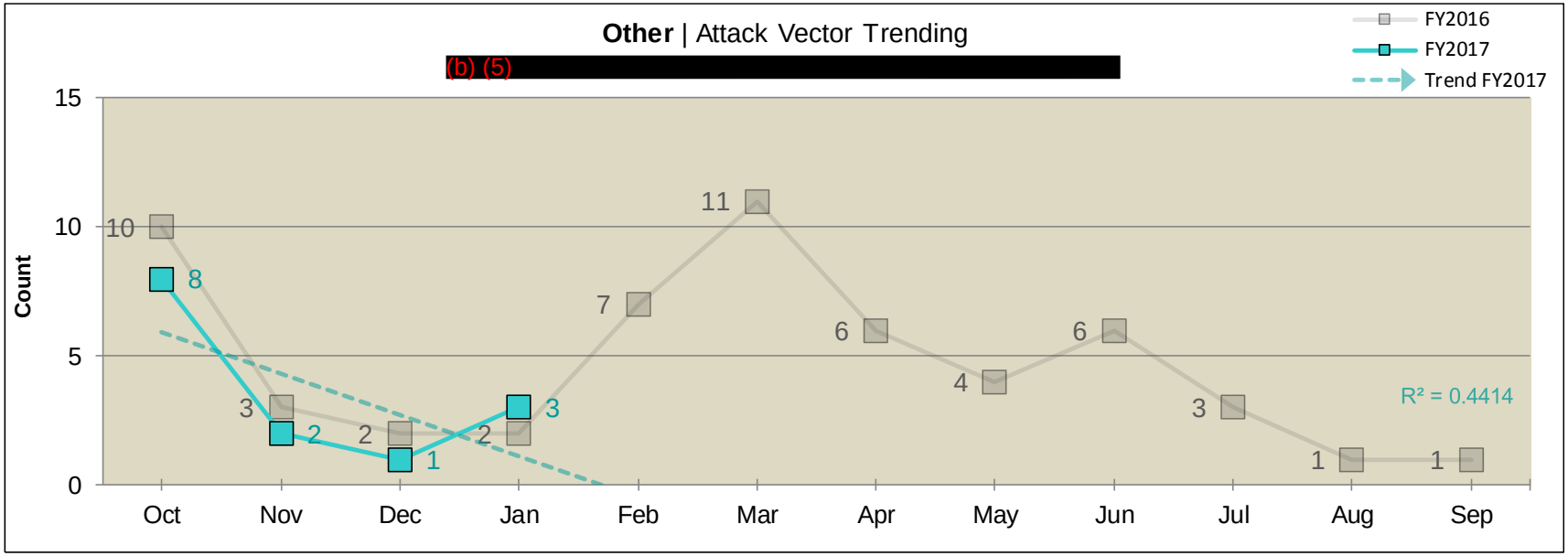
[redacted]

(b) (5)

[redacted]



« Return to Table of Contents


Other | Attack Vector Trending
(b) (5) [redacted]
FY2016
FY2017
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
11
6
4
6
3
1
1
R² = 0.4414

4 (b) (5) [redacted] MTIPS BASED REPORTS

4.1 (b) (5) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[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]

5 EXECUTIVE LEVEL REPORTS

5.1 US-CERT Incident Report

The purpose of this report is a fulfillment of the Presidential Management Council on Cybersecurity reporting requirement. Incidents with US-CERT involvement are tracked on an annual, quarterly, and monthly basis. Data is sourced through Remedy with only duplicates being excluded.

CSIRC ► US-CERT Related Incidents ► Previous Month (01 Jan 2017 - 31 Jan 2017)

Total US-CERT related incidents: **13**

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5) [redacted]

Total False Positives and/or Category 6 (Investigation): **5**

(b) (5) [redacted].

Total phishing incidents with clicking on link: **0**

(b) (5) [redacted]

CSIRC ► US-CERT Related Incidents ► Previous Quarter (01 Oct 2016 - 31 Dec 2016)

Total US-CERT related incidents: **14**

(b) (5) [redacted].

(b) (5) [redacted].

Total False Positives and/or Category 6 (Investigation): **11**

(b) (5) [redacted].

Total phishing events with clicking on link: **0**

(b) (5) [redacted]

CSIRC ► US-CERT Related Incidents ► Previous 365 Days (01 Feb 2016 - 31 Jan 2017)

Total US-CERT related incidents: **97**

(b) (5) [redacted]

(b) (5) [redacted]

Total False Positives and/or Category 6 (Investigation): **15**

(b) (5) [redacted]

Total phishing events with clicking on link: **0**

(b) (5) [redacted]

5.2 Personally Identifiable Information (PII) Incident Report

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.

CSIRC ► Events ► Personally Identifiable Information (PII)
Time Frame: **FY2017 to Date** (01 October 2016 - 31 Jan 2017)
Total CSIRC Events: **256**
Total CSIRC Events Involving Personally Identifiable Information (PII): **5**
(b) (5) [redacted].
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%**

5.3 Successful Incident Attack Report

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 will be reported on monthly and quarterly time periods.

CSIRC ► Events ► Incidents ► Successful Attacks

Time Frame: **Previous Month** (01 Jan 2017 - 31 Jan 2017)

Total Attack Attempts: **9,082**

Total Successful Attacks: **9**

(b) (5) [redacted]

[redacted].

(b) (5) [redacted]

(b) (5) [redacted]

CSIRC ► Events ► Incidents ► Successful Attacks

Time Frame: **Previous Quarter** (01 Oct 2016 - 31 Dec 2016)

Total Attack Attempts: **26,754**

Total Successful Attacks: **37**

Percentage of Successful Attacks: **0.14%**

37 / 26,754 = 0.00138297077 = 0.14%

6 (b) (5) [redacted]

[redacted]

[redacted]

- [redacted]

7 (b) (5) [redacted]

[redacted]

[redacted]

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
FY2014	Fiscal Year 2014
FY2015	Fiscal Year 2015
FY2016	Fiscal Year 2016
FY2017	Fiscal Year 2017
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	Information Security Officer
MTIPS	(AT&T) Managed Trusted Internet Protocol Service
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
SEP	Symantec Endpoint Protection
SP	Special Publications
VPN	Virtual Private Network

CSIRC

Computer Security Incident Response Capability

Keeping IT Secure