CSIRC REPORTS

Monthly Analytic Synopsis

November FY19

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 3
2.1 (b) (5) [redacted] 3
2.2 (b) (5) [redacted] 11
3 Remedy Based Reports 13
3.1 (b) (5) [redacted] 13
3.2 Event Report 14
3.3 Event Category Report 18
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] 34
6.1 (b) (5) [redacted] 34

List of Exhibits

(b) (5) [redacted]

(b) (5) [redacted]

Exhibit 15: Event Report | FY18 Incident Contrast and Distribution 17

(b) (5) [redacted]

Exhibit 21: Firewall Deny Report | Associated Metrics 29

(b) (5) [redacted]

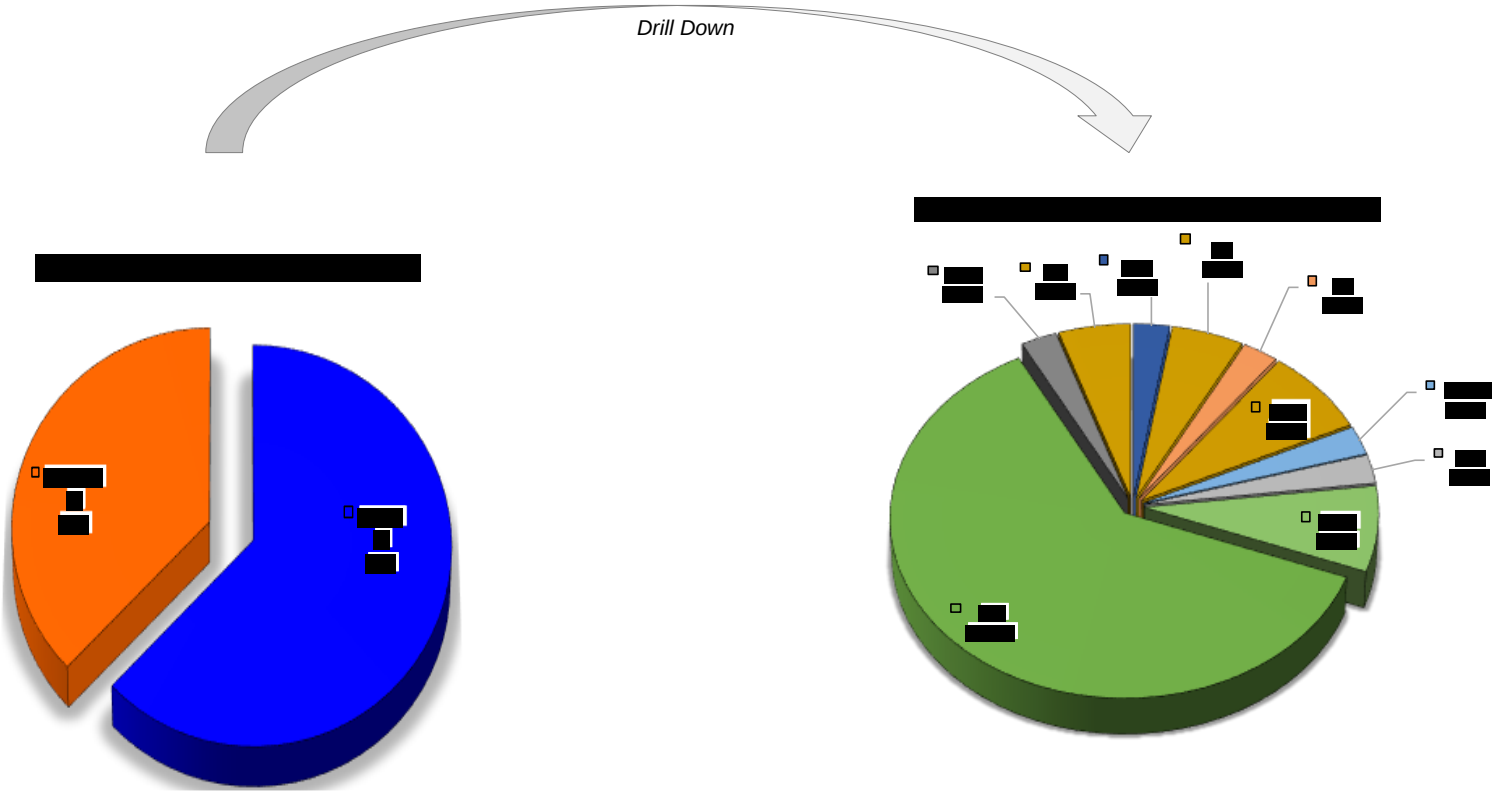
Revision Log

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]

[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]

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]

2.2 (b) (5) [redacted]

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

3 Remedy Based Reports

3.1 (b) (5) [redacted]

The purpose of this report is to show monthly ticket volume and trending. Ticket priority level pertains to the criticality of computer security related incidents (low, medium, high, and critical). Data for this metric is extracted daily from Remedy and refreshed by the 5th business day of each month.

(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.

FY19	Corresponding Statistics for Computer Security Events
Average (monthly):	The agency is incurring an average of **58.5** computer security related events **per month** in FY19.
Average (daily):	The agency is incurring an average of **2.8** computer security related events **per business day** in FY19.
High Month:	**October** is currently the most active month in FY19 with **65** events. Represents **56%** of all events/incidents in FY19.
Low Month:	**November** is currently the low months in FY19 with **52** events. Represents **44%** of all events in FY19.
(b) (5) [redacted]	(b) (5) [redacted]
[redacted]	[redacted]
Trend (slope):	Events/Incidents for FY18 (Oct 2018 through Sep 2019) have a **downward trend** ▼ (i.e. slope of linear regression) of **-0.0769**

FY18	Corresponding Statistics for Computer Security Events
Average (monthly):	The agency is incurring an average of **72.3** computer security related events/incidents **per month** in FY18.
Average (daily):	The agency is incurring an average of **3.5** computer security related events/incidents **per business day** in FY18.
High Month:	**April** is currently the most active month in FY18 with **104** events/incidents. Represents **12%** of all events/incidents in FY18.
Low Month:	**June is** currently the least active months in FY18 with **53** events/incidents. Represents **6%** of all events/incidents in FY18.
(b) (5) [redacted]	(b) (5) [redacted]
[redacted]	[redacted]
Trend (slope):	Events/Incidents for FY18 (Oct 2017 through Sep 2018) have a **upward trend** ▲ (i.e. slope of linear regression) of **0.0204**

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

(b) (5)

[redacted]

3.3 Event Category Report

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.

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)

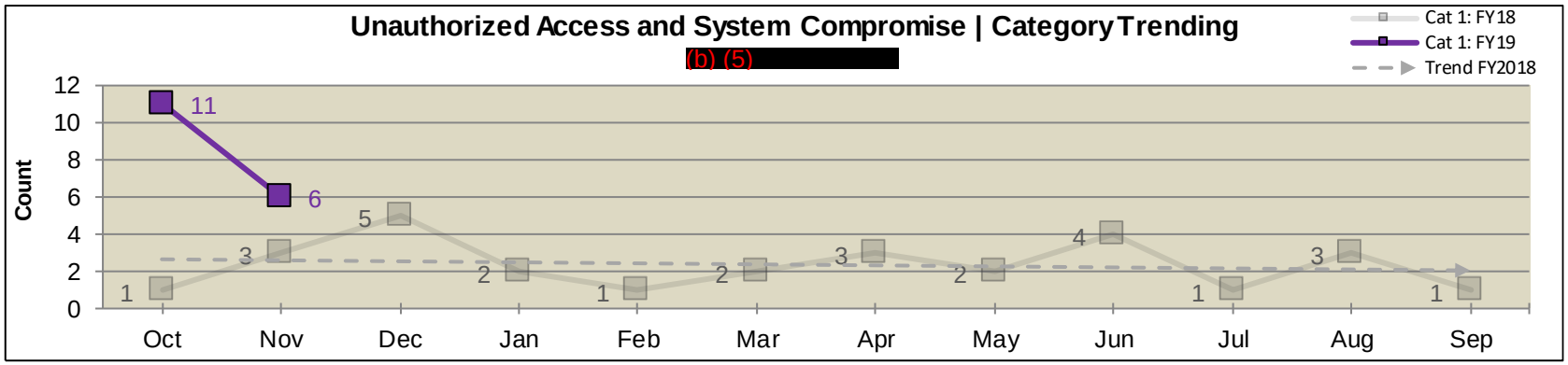
[redacted]

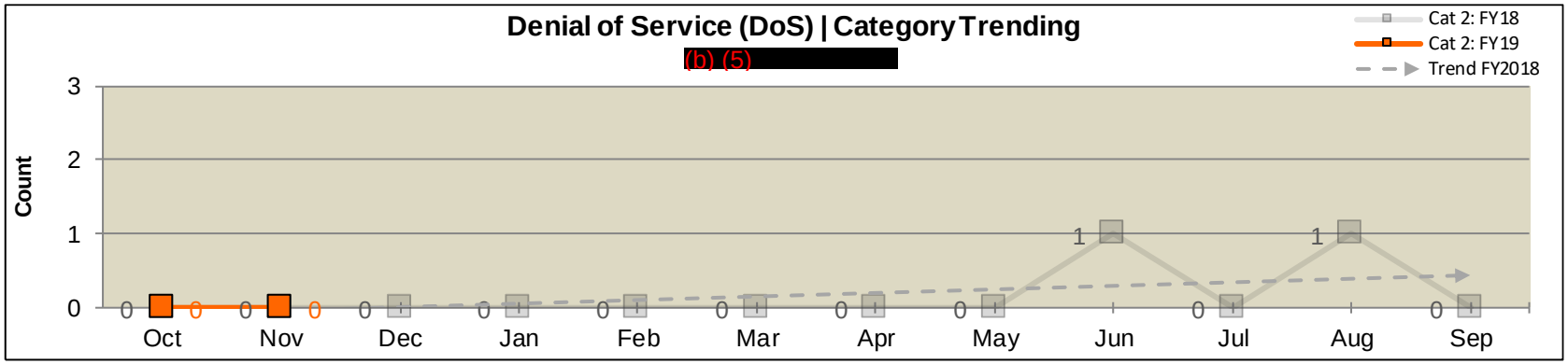
(b) (5)

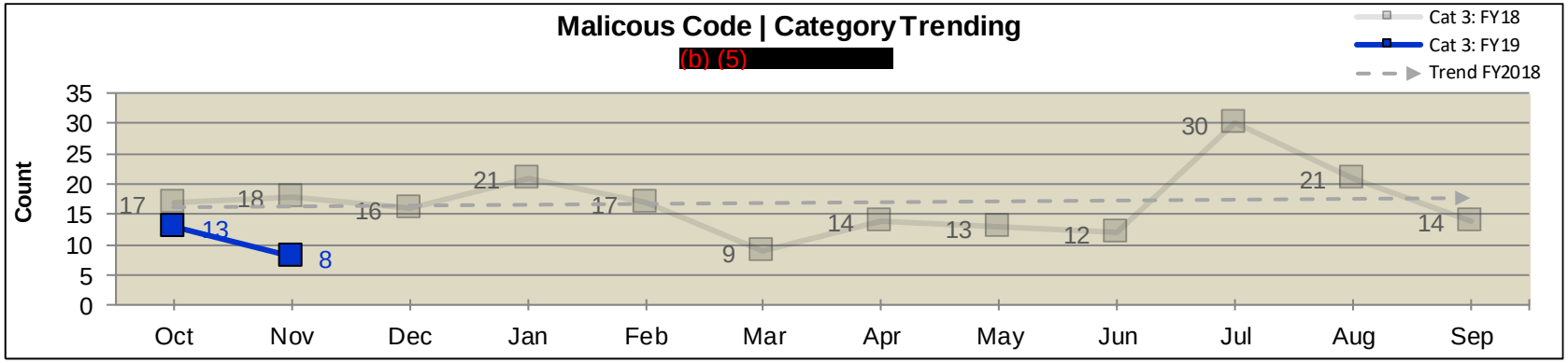
[redacted]

(b) (5)

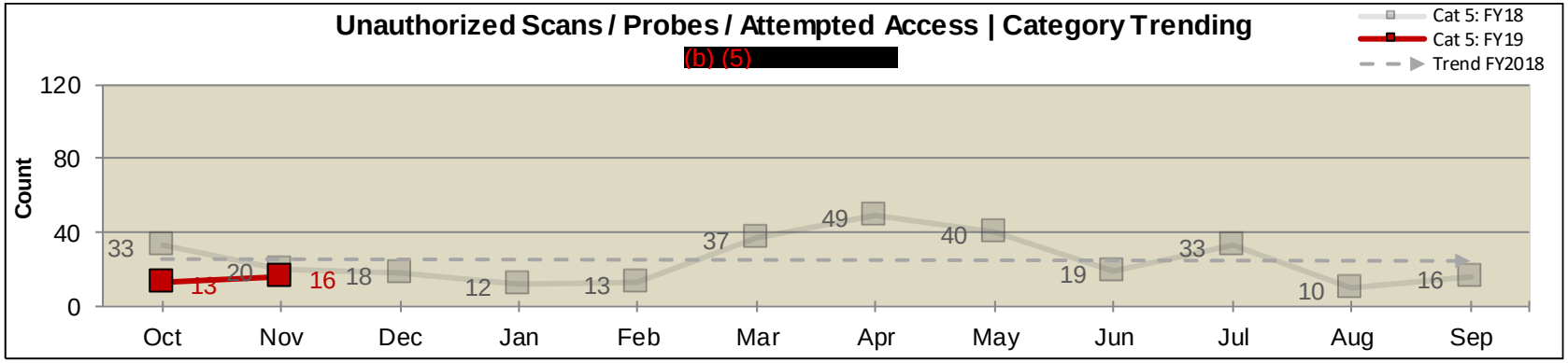
[redacted]


Unauthorized Access and System Compromise | Category Trending
(b) (5) [redacted]
Cat 1: FY18
Cat 1: FY19
Trend FY2018
Count
12
10
8
6
4
2
0
11
6
5
3
2
1
2
3
2
4
1
3
1
1
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep


Denial of Service (DoS) | Category Trending
(b) (5) [redacted]
Cat 2: FY18
Cat 2: FY19
Trend FY2018
Count
3
2
1
0
0
0
0
0
0
0
0
0
0
0
0
1
0
1
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep

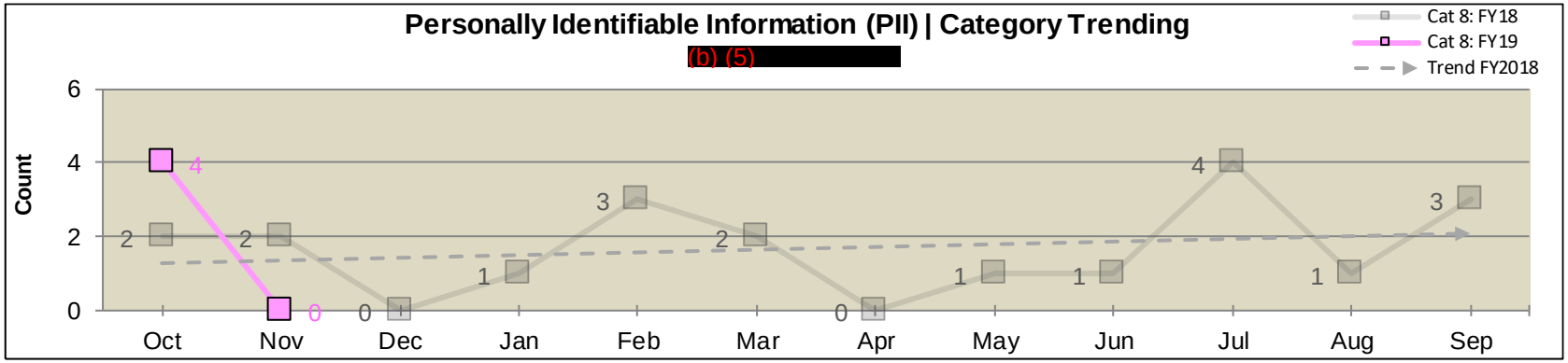

Malicous Code | Category Trending
(b) (5) [redacted]
Cat 3: FY18
Cat 3: FY19
Trend FY2018
Count
35
30
25
20
15
10
5
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
17
18
16
21
17
9
14
13
12
30
21
14
13
8

(b) (5) [redacted]


Unauthorized Scans / Probes / Attempted Access | Category Trending
(b) (5) [redacted]
Cat 5: FY18
Cat 5: FY19
Trend FY2018
Count
120
80
40
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
33
18
12
13
37
49
40
19
33
10
16
13
20
16

(b) (5)

[redacted]


Personally Identifiable Information (PII) | Category Trending
(b) (5)
Cat 8: FY18
Cat 8: FY19
Trend FY2018
Count
6
4
2
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
2
4
2
0
0
1
3
2
0
1
1
4
1
3

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.

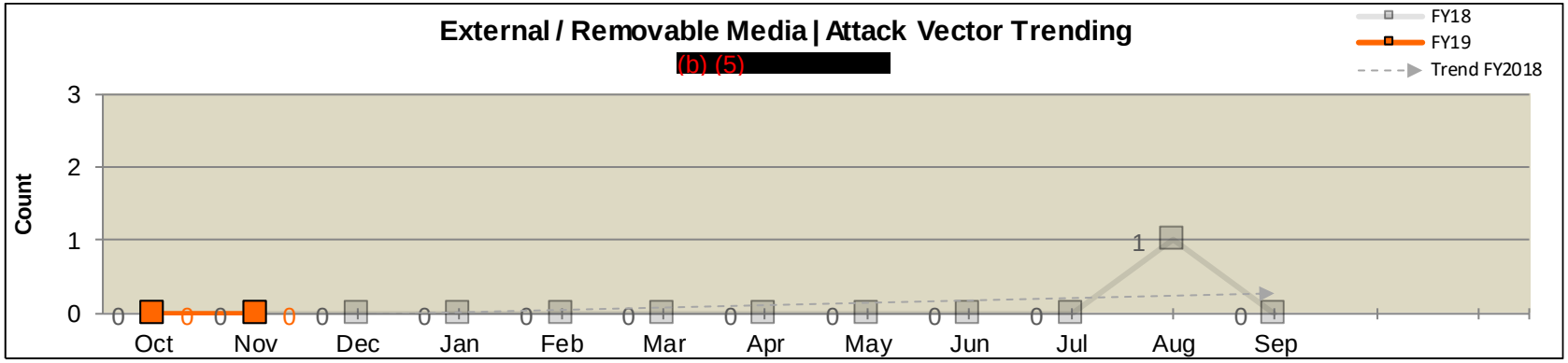
(b) (5)

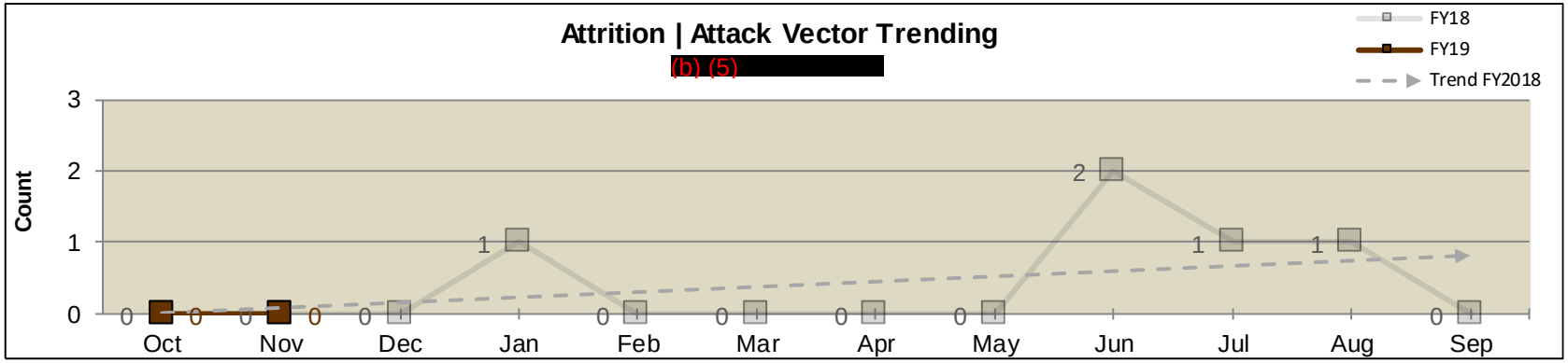
[redacted]

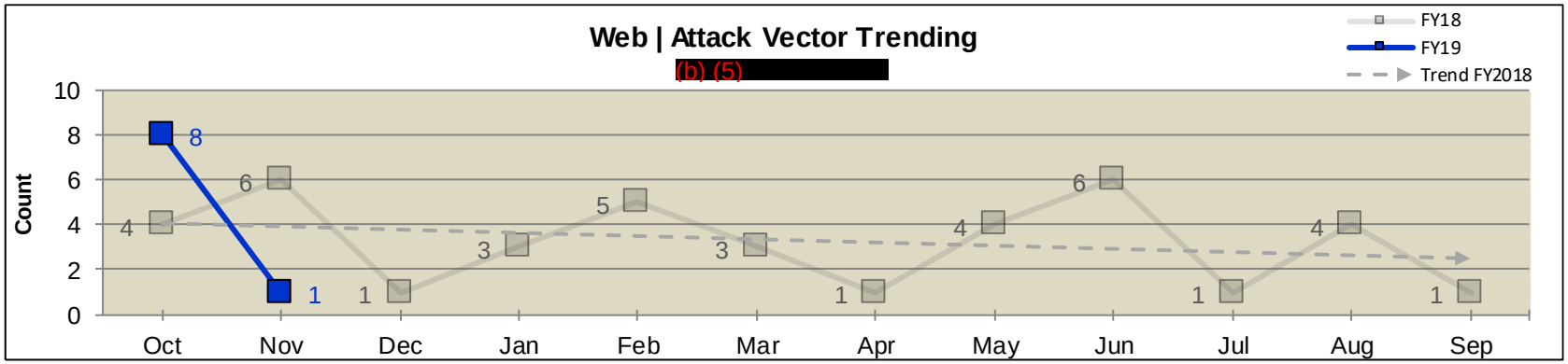
(b) (5)

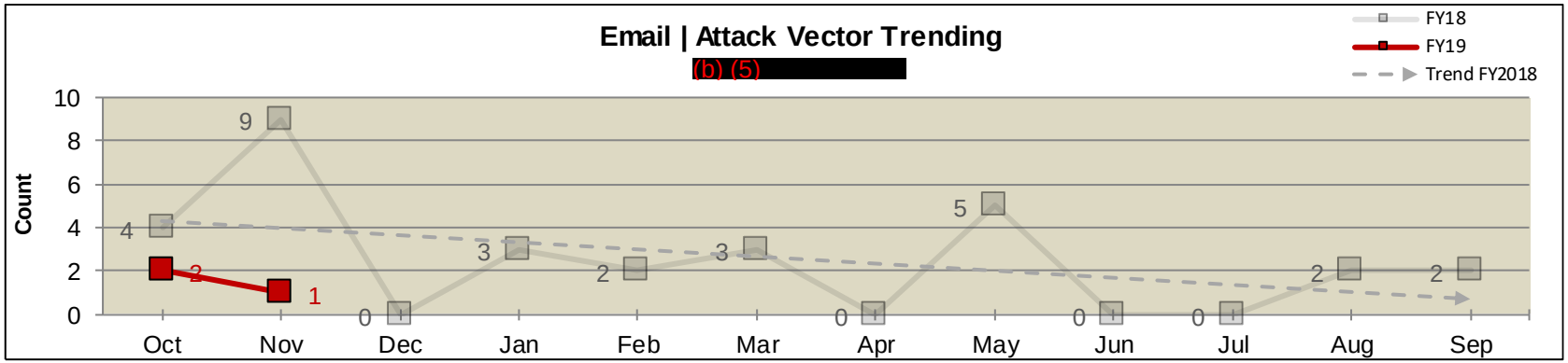
[redacted]

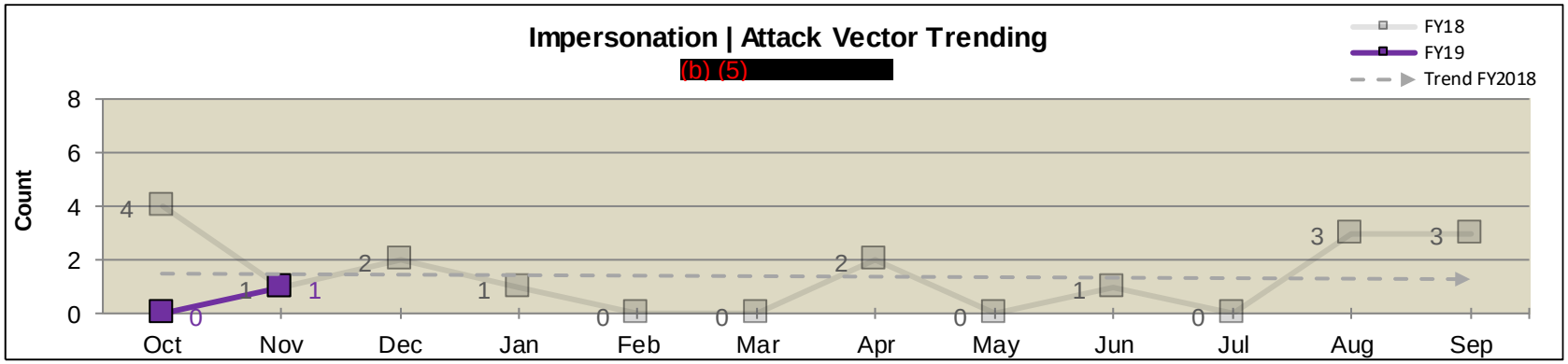
Exhibit 15: Attack Vector Report | Trending







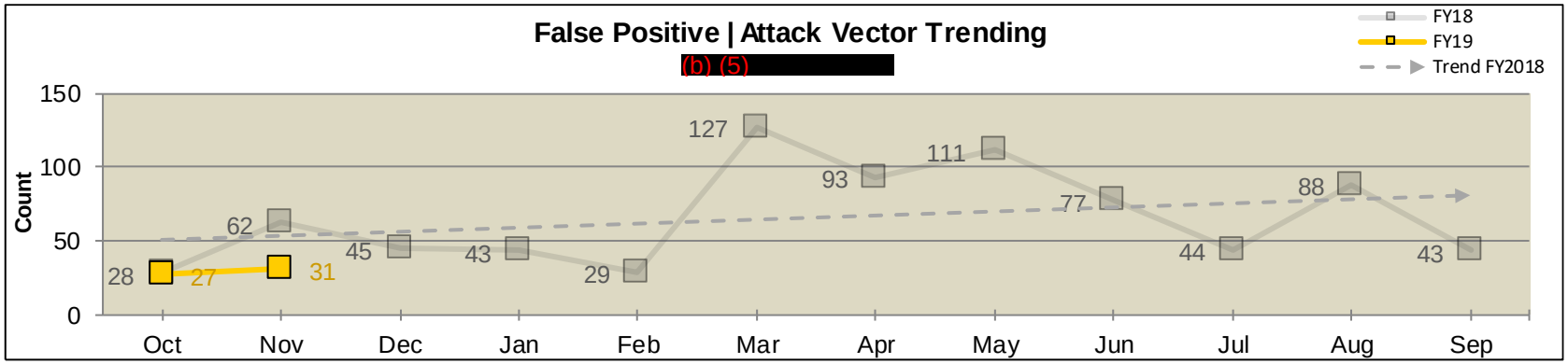

Email | Attack Vector Trending
(b) (5) [redacted]
FY18
FY19
Trend FY2018
Count
10
8
6
4
2
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
4
9
2
1
0
3
2
3
0
5
0
0
2
2

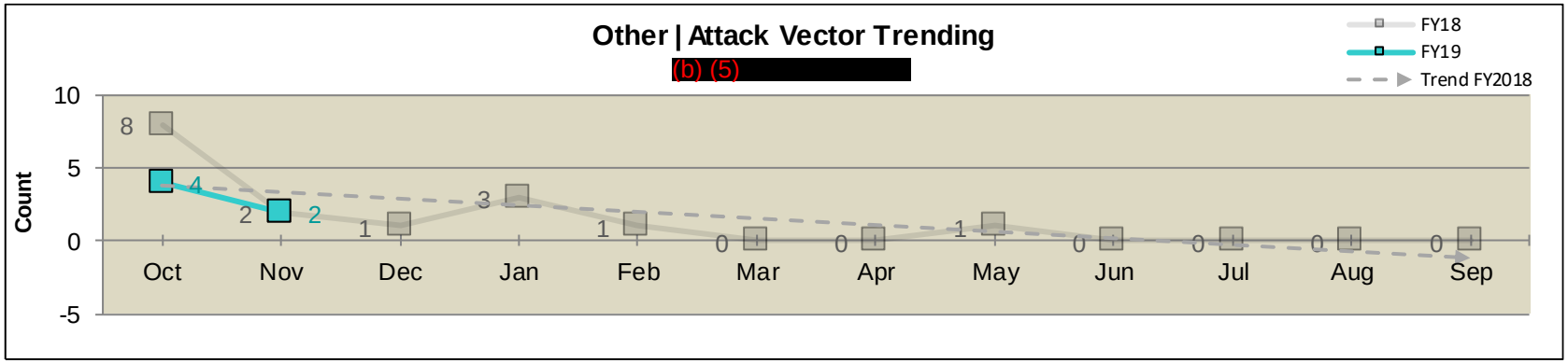

Impersonation | Attack Vector Trending
(b) (5) [redacted]
FY18
FY19
Trend FY2018
Count
8
6
4
2
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
4
0
1
1
2
1
0
0
2
0
1
0
3
3

(b) (5) [redacted]

(b) (5)

[redacted]


False Positive | Attack Vector Trending
(b) (5) [redacted]
FY18
FY19
Trend FY2018
Count
150
100
50
0
28
27
62
31
45
43
29
127
93
111
77
44
88
43
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep


Other | Attack Vector Trending
(b) (5) [redacted]
FY18
FY19
Trend FY2018
Count
10
5
0
-5
8
4
2
2
1
3
1
0
0
1
0
0
0
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep

4 (b) (5) MTIPS Based Reports

4.1 (b) (5)

4.1.1 (b) (5)

(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	CSIRC ► Events ► Incidents ► Successful Attacks
Time Frame: **November 2018 FY19**	Time Frame: **FY19**
Total Attack Attempts: **54277**	Total Attack Attempts: **105057**
Total Successful Attacks: **18**	Total Successful Attacks: **44**
Percentage of Successful Attacks: **0.03%**	Percentage of Successful Attacks: **0.05%**
(b) (5) [redacted]	(b) (5) [redacted]

6 (b) (5) [redacted]

6.1 (b) (5) [redacted]

[redacted]

- [redacted]