

DEVELOPING AND TESTING AN EFFECTIVE INCIDENT RESPONSE PLAN

BY ANDY JORDAN



May 16, 2017

Agenda: What You'll Learn Today!

OUTCOMES

1. What frameworks can you use?
2. What should you include?
3. How do you test it?
4. How do you measure its effectiveness?

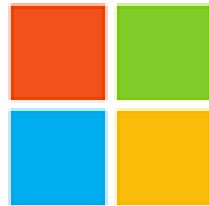


Who Am I

A LITTLE ABOUT ME

Andy Jordan

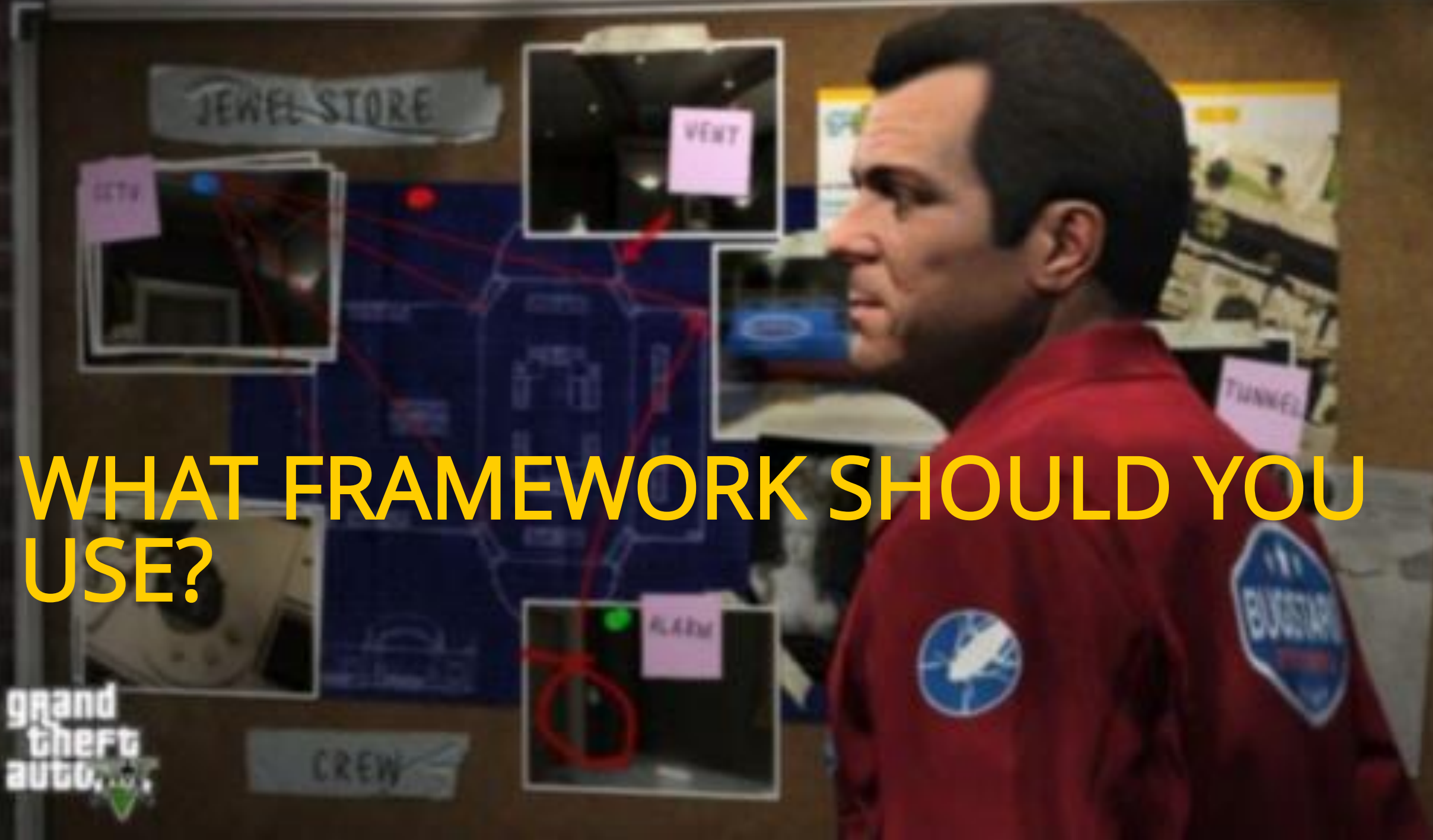
- Senior Security Associate
- Helps manage Bishop Fox's consulting practice
- Began career in IT Infrastructure





WHAT FRAMEWORK SHOULD YOU USE?

grand
theft
auto, III



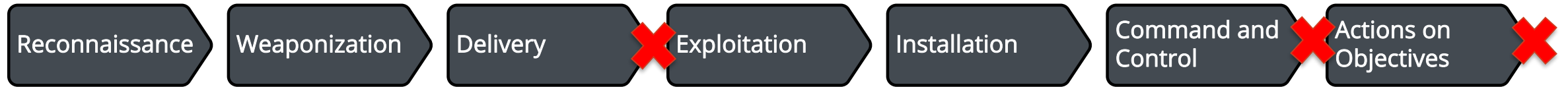
Which Framework Do I Use?

SO MANY TO CHOOSE FROM



Lockheed Martin - Cyber Kill Chain

"KNOW YOUR ENEMY" – SUN TZU



Pros

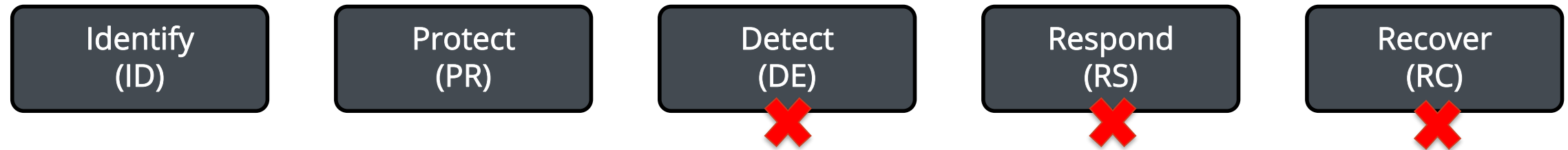
- Attack Centric
- Focused on Prevention
- "Bottom-Up" Approach

Cons

- Requires Threat Management
- Not A Process
- Not Aligned to Overall Strategy
- No Steps for Recovery

NIST – CyberSecurity Framework

THE CISO'S HANDBOOK



Pros

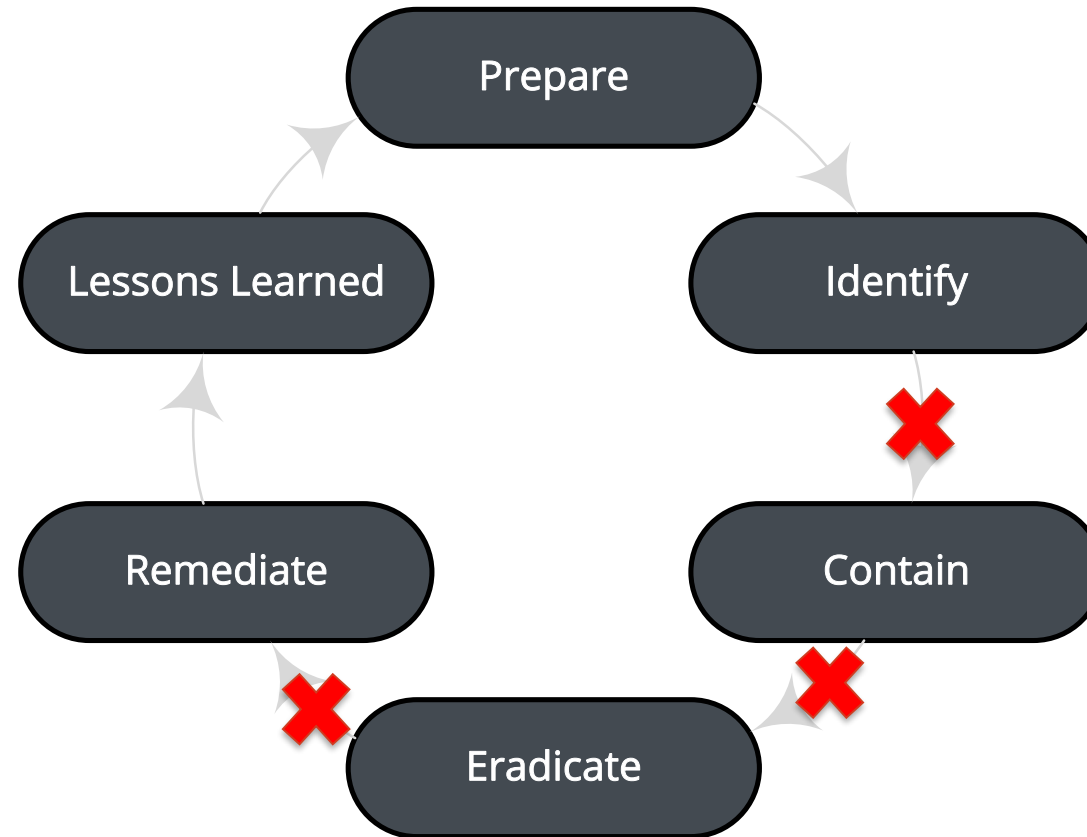
- Easy to Explain
- More Defined
- Improvements Can Be Modular
- “Top-Down” Approach

Cons

- Needs Departmental Adoption
- Could Become A Checklist

SANS - Incident Response Process

INCIDENT RESPONSE IS A LIFECYCLE



Pros

- Lifecycle
- Holistic Response
- Focused on Improvements

Cons

- Reactionary
- Operationally Intensive
- Centralized Approach



**WHAT SHOULD AN INCIDENT
RESPONSE PLAN INCLUDE?**

“Hey Andy, I Found This Weird Image On My Server”

PANIC!



Who Do I Need To Contact?

PAY NO ATTENTION TO THE BLAZING FIRE BEHIND YOU

Sample Incident Handling Procedure

1.0 INTRODUCTION

This document provides some general guidelines and procedure document is meant to provide <COMPANY NAME> support personnel to discover a security incident. The term incident in this document occurs on any part of the NPSN. Some examples of possible incidents are: integrity; denial of system resources; illegal access to a system; loss of system resources, or any kind of damage to a system. Some possible incidents are:

- * You see a strange process running and accumulating
- * You have discovered an intruder logged into your system
- * You have discovered a virus has infected your system
- * You have determined that someone from a remote site is accessing your system

The steps involved in handling a security incident are categorized into: identification of the problem; containment of the problem; eradication of the problem; and the follow-up analysis. The actions taken in some of these steps are discussed in section 2. Section 3 discusses specific procedures for handling hacker/cracker incidents.

1.1 TERMS

Some terms used in this document are:

- ISO - Installation Security Officer
- CSO - Computer Security Officer
- CSA - Computer Security Analyst
- LSA - Lead System Analyst
- CERT - Computer Emergency Response Team
- CIAC - Computer Incident Advisory Capability

1.2 AREAS OF RESPONSIBILITY

In many cases, the actions outlined in this guideline will not be performed by a single person. Many people may be involved during the course of an action. <COMPANY NAME> systems at one time (i.e., a worm attack) may be involved in the investigation of any security incident.

The <COMPANY NAME> ISO (put name here), the <COMPANY NAME> CSO (put name here) will act as the lead for all incidents. In minor incidents, only the CSA will be involved. In major incidents, the ISO, CSO, and CSA will be involved in the coordination effort. The incident coordination team will be assigned specific tasks of the incident handling process and will coordinate the actions of the people involved in the incident response and clean-up are members of the incident coordination team.

Any directives given by a member of the incident coordination team are to be followed.

1.3 IMPORTANT CONSIDERATIONS



day or night. Although most hacker/cracker incidents occur during the day, it is important for managers to be watching their flocks. However, worm and virus attacks can occur at any time and distance considerations in responding to the incident. The list to be notified can not respond within a reasonable time to the first. It will be the responsibility of the people on the scene to respond within the available time frame.

If the media obtains knowledge about a security incident, the incident manager from a site currently responding to the incident. Providing accurate information to the media has side effects. Section 2.3 discusses the policy on release of information.

There are several types of security incidents.

Some incidents eventually involve federal authorities and the possibility of a security incident are not always known at the beginning of, or even during the incident. Log should be kept for all security incidents that are under investigation that can not be altered by others. Manually written logs should be kept. The types of information that should be logged are:

- Date and time the incident was discovered or occurred.
- Name of the person who discovered the incident.
- Location of the incident.
- Name of the person who has been affected.

There are some actions that can only be authorized by the Incident Manager (IME). <COMPANY NAME> also has the responsibility to inform other sites. The list of sites is provided below. Section 3 discusses who should be notified.

The <COMPANY NAME> Operations Manual in the Operations Manual room analysts can be of help when trying to contact the

Contacts

<COMPANY NAME> CSA -



Time To Respond!

USING YOUR INCIDENT RESPONSE PLAN

- Quickly contact the CIRT.
- Follow action plans (and sub-plans).
- Update your Incident Response Plan often.



An Example of the Good

SOCIÉTÉ GÉNÉRALE - WORMS

Preparation

1

- Define actors, for each entity, who will be involved into the crisis cell. These actors should be documented in a contact list kept permanently up to date.
- Make sure that analysis tools are up, functional (Antivirus, IDS, logs analysers), not compromised, and up to date.
- Make sure to have architecture map of your networks.
- Make sure that an up to date inventory of the assets is available.
- Perform a continuous security watch and inform the people in charge of security about the threat trends.

Identification

2

Detect the infection

Information coming from several sources should be gathered and analyzed:

- Antivirus logs,
- Intrusion Detection Systems,
- Suspicious connection attempts on servers,
- High amount of accounts locked,
- Suspicious network traffic,
- Suspicious connection attempts in firewalls,
- High increase of support calls,
- High load or system freeze,
- High volumes of e-mail sent

If one or several of these symptoms have been spotted, the actors defined in the "preparation" step will get in touch and if necessary, create a crisis cell.

Identify the infection

Analyze the symptoms to identify the worm, its propagation vectors and countermeasures.

Leads can be found from :

- CERT's bulletins;
- External support contacts (antivirus companies, etc.) ;
- Security websites (Secunia, SecurityFocus etc.)

Notify Chief Information Security Officer.
Contact your CERT if required.

Assess the perimeter of the infection

Define the boundaries of the infection (i.e.: global infection, bounded to a subsidiary, etc.).
If possible, identify the business impact of the infection.

Containment

3

The following actions should be performed and monitored by the crisis management cell:

1. Disconnect the infected area from the Internet.
2. Isolate the infected area. Disconnect it from any network.
3. If business-critical traffic cannot be disconnected, allow it after ensuring that it cannot be an infection vector or find validated circumventions techniques.
4. Neutralize the propagation vectors. A propagation vector can be anything from network traffic to software flaw. Relevant countermeasures have to be applied (patch, traffic blocking, disable devices, etc.)
For example, the following techniques can be used:
 - Patch deployment tools (WSUS),
 - Windows GPO,
 - Firewall rules,
 - Operational procedures.
5. Repeat steps 2 to 4 on each sub-area of the infected area until the worm stops spreading. If possible, monitor the infection using analysis tools (antivirus console, server logs, support calls).

The spreading of the worm must be monitored.



Mobile devices

Make sure that no laptop, PDA or mobile storage can be used as a propagation vector by the worm. If possible, block all their connections.

Ask end-users to follow directives precisely.

An Example of the Good

SOCIÉTÉ GÉNÉRALE - WORMS

<h2 style="background-color: red; color: white; padding: 2px;">Remediation 4</h2> <p>Identify Identify tools and remediation methods. The following resources should be considered:</p> <ul style="list-style-type: none">- Vendor fixes (Microsoft, Oracle, etc.)- Antivirus signature database- External support contacts- Security websites <p>Define a disinfection process. The process has to be validated by an external structure, like your CERT for example.</p> <p>Test Test the disinfection process and make sure that it properly works without damaging any service.</p> <p>Deploy Deploy the disinfection tools. Several options can be used:</p> <ul style="list-style-type: none">- Windows WSUS- GPO- Antivirus signature deployment- Manual disinfection <p><u>Warning:</u> some worms can block some of the remediation deployment methods. If so, a workaround has to be found.</p> <p>Remediation progress should be monitored by the crisis cell.</p>	<h2 style="background-color: #d9ead3; padding: 2px;">Recovery 5</h2> <p>Verify all previous steps have been done correctly and get a management approval before following next steps.</p> <ol style="list-style-type: none">1. Reopen the network traffic that was used as a propagation method by the worm.2. Reconnect sub-areas together3. Reconnect the mobile laptops to the area4. Reconnect the area to your local network5. Reconnect the area to the Internet <p>All of these steps shall be made in a step-by-step manner and a technical monitoring shall be enforced by the crisis team.</p>	<div style="display: flex; justify-content: space-between;"> SOCIETE GENERALE CERT SOCIETE GENERALE</div> <h3 style="text-align: center;">Incident Response Methodology</h3>
<p style="text-align: center;">IRM #1</p> <h3 style="text-align: center;">Worm Infection Response</h3> <p style="text-align: center;">Guidelines to handle information system Worm infections</p> <hr/> <p style="text-align: center;">IRM Author: CERT SG/ Vincent Ferran-Lacome IRM version: 1.2</p> <p style="text-align: center;">E-Mail: cert.sg@socgen.com Web: http://cert.societegenerale.com Twitter: @CertSG</p>		
<h3 style="text-align: center; background-color: #f0f0f0; padding: 2px;">Abstract</h3> <p>This Incident Response Methodology is a cheat sheet dedicated to incident handlers investigating a precise security issue. Who should use IRM sheets?</p> <ul style="list-style-type: none">• Administrators• Security Operation Center• CISOs and deputies• CERTs (Computer Emergency Response Team) <p>Remember: If you face an incident, follow IRM, take notes and do not panic. Contact your CERT immediately if needed.</p>		
<h3 style="text-align: center; background-color: #f0f0f0; padding: 2px;">Incident handling steps</h3> <p>6 steps are defined to handle security Incidents</p> <ul style="list-style-type: none"> Preparation: get ready to handle the incident Identification: detect the incident Containment: limit the impact of the incident Remediation: remove the threat Recovery: recover to a normal stage Aftermath: draw up and improve the process <p>IRM provides detailed information for each step.</p>		
<p>This document is for public use</p>		





**HOW DO YOU TEST YOUR
INCIDENT RESPONSE PLAN?**

Reviewing Previous Incidents

EXAMPLE FROM WANNACRYPT RANSOMWARE

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00

Send \$600 worth of bitcoin to this address:

Bitcoin ACCEPTED HERE

How to buy bitcoins?

Contact Us

Check Payment

Decrypt

Copy

Know how you will respond ahead of time

\$600 is the minimum you will spend

Digging Through Threat Data

EXAMPLE OF BLACK-MARKET CREDENTIAL SALES

The screenshot shows a listing on AlphaBay Market for "brokerage or bank account logins - balance from \$0 to \$2 600 000". The listing includes a description, a price list, and a table of features. A red callout box points to the description text, and another red callout box points to the price list.

AlphaBay Market | Logged in as [redacted] [Logout]
BTC: [redacted] / XMR: [redacted] / ETH: [redacted]
USD 1008.99 | CAD 1347.48 | EUR 938.25 | AUD 1306.41 | GBP 814.79

Fraud > Accounts & Bank Drops > [redacted]

[redacted] brokerage or bank account logins - balance from \$0 to \$2 600 000

no address or state provided, only logins and balance no tutorial on how to use them
STOP LEAVING NEGATIVE FEEDBACK IF YOU CANT LOGIN BECAUSE OF SECURITY CHECKS, THIS IS YOUR PROBLEM !! NEGATIVE FEEDBACK GREATLY AFFECTS OUR VENDOR PROFILE \$3000+ account balance for \$18 \$8000+ account balance for \$28 \$35000+ account balance for \$70 \$60000+ account balance for \$92 \$100000+ account balance b...

Sold by mike.g | 20 sold since Oct 21, 2016 | Vendor Level 5 | Trust Level 5

	Features	Features
Product class	Digital goods	Origin country
Quantity left	Unlimited	Ships to
Ends in	Never	Payment
		Escrow

Product Description

no address or state provided, only logins and balance
no tutorial on how to use them

STOP LEAVING NEGATIVE FEEDBACK IF YOU CANT LOGIN BECAUSE OF SECURITY CHECKS, THIS IS YOUR PROBLEM !!
NEGATIVE FEEDBACK GREATLY AFFECTS OUR VENDOR PROFILE

- \$3000+ account balance for \$18
- \$8000+ account balance for \$28
- \$35000+ account balance for \$70
- \$60000+ account balance for \$92
- \$100000+ account balance for \$99

Awareness of Organizational Controls

An account with \$3,000 in funds sells for \$18



Make Your Incident Tabletops More Realistic

LET'S PLAY A GAME!


Incident Response Game



News Leaks

Malicious Actor has bragged to 6pm news station about his attack. 2x people must now produce a written statement.

Incident Response Game



Confusion!

Operational / Non-related issue occurs.

Incident Response Game



No Logs!?

System is not configured to log system/application events.


Incident Response Game



Technology Fail

Every remote participant must redial into the bridge.


Incident Response Game



Backup Integrity

Restored file comes back with garbage data.
Full reimage/recreation of data must be performed.
(Add 8 hours to reimage process.)

Incident Response Game

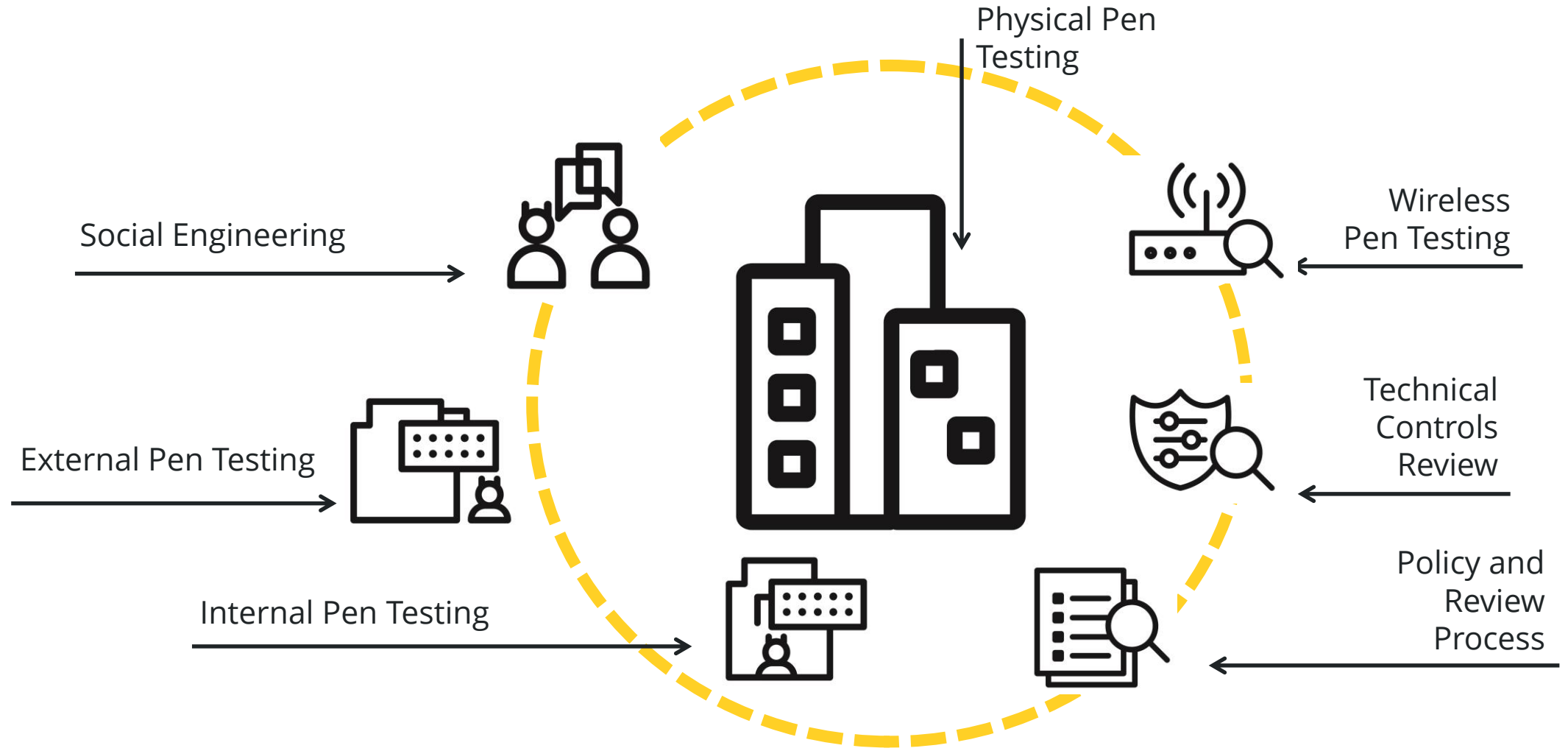


Second Incident

2x people must leave the tabletop to support another issue.

Red Team Testing

STOPPING AN ACTIVE ATTACK IN A CONTROLLED ENVIRONMENT





HOW DO YOU MEASURE YOUR
INCIDENT RESPONSE PLAN?

Example Dashboard – “How Much Fuel Do I Have?”

WOULD YOU DRIVE THIS CAR?



Example Dashboard

IT'S PRETTY HUH?

Vulnerability Management Dashboard

ACCOUNTABILITY INCREASED THROUGH OWNERSHIP VISIBILITY

TRACK OUTSTANDING OR REMEDIATED ISSUES

MOVING CURSOR OVER CHART REVEALS MORE DETAILED INFORMATION

SELECT A HOST TO OPEN A DIRECT LINK TO THE ASSET

Department: System Engineering
 Director: Employee One; Technical Point of Contact: Employee Two
 Last Updated - 41 minutes ago

Asset Groups: Dynamic, Servers,

Filters

Quick Asset Dropdown: 0-30, 30-60, 61-90, 91-180, 181+

Asset Groups Dropdown: 1, 2, 3, 4, 5

Severity Selection

Quick Statistics

Compliance	40%
Severity 5	10,2381
Severity 4	2,038
Severity 3	1,028
Total Live Hosts	100
Authenticating Hosts	80 (80%)
Workstations	50
Servers	50
Most Vulnerable Host	SERVICES.ACME.COM
Most Common Issue	18363 - Outdated Java 7

Vulnerability Data

IP	DNS	OS	Score
10.62.11.249	SFO0A131.ACME.COM	Windows Server 2003	14,715
10.64.208.151	SERVICES.ACME.COM	Windows NT	9,217,939
10.68.102.128	SFO0IS25.ACME.COM	Windows Server 2008	5,719
10.62.82.19	SFO0A339.ACME.COM	Unknown	193
10.61.20.83	SFO0S86-OLD.ACME.COM	Windows Server 2012	41
172.16.100.2	SFO0S94-OLD.ACME.COM	Cisco IOS 12.X	193
106.182.79.3	SFO0S95-OLD.ACME.COM	Windows Server 2000	1,093,854
10.28.197.1	ARZ0F82.ACME.COM	Linux 2.6	103
67.29.211.97	LAS0F177.ACME.COM	Windows 7 Enterprise	937
73.4.1.21	...	Enterprise	159

Remediation Age

Age	Severity 3	Severity 4	Severity 5
0-30	408	192	102
31-60	386	99	391
61-90	976	291	390
91-180	2,948	3,034	2,019
181+	1,927	2,937	19,327

Exceptions

HOST	EXPIRATION
SFO0A4.ACME.COM	November 11 th 2015
AZ0AB.ACME.COM	December 3 rd 2015

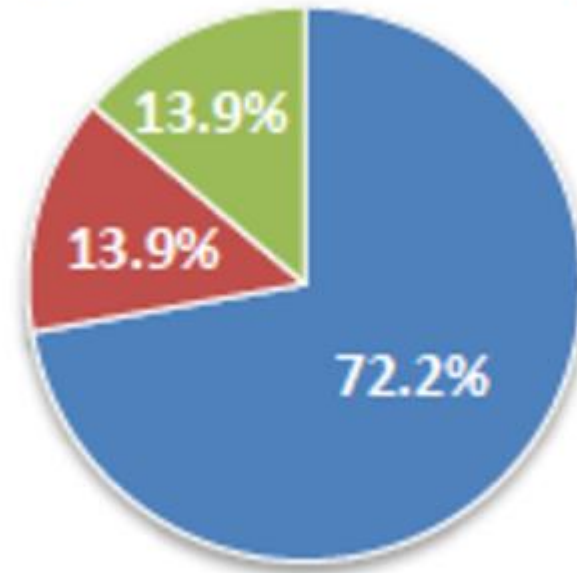
Vulnerability Age



Report Example 1 – Security Visibility

CURRENT STATE

Business Critical Systems Visibility

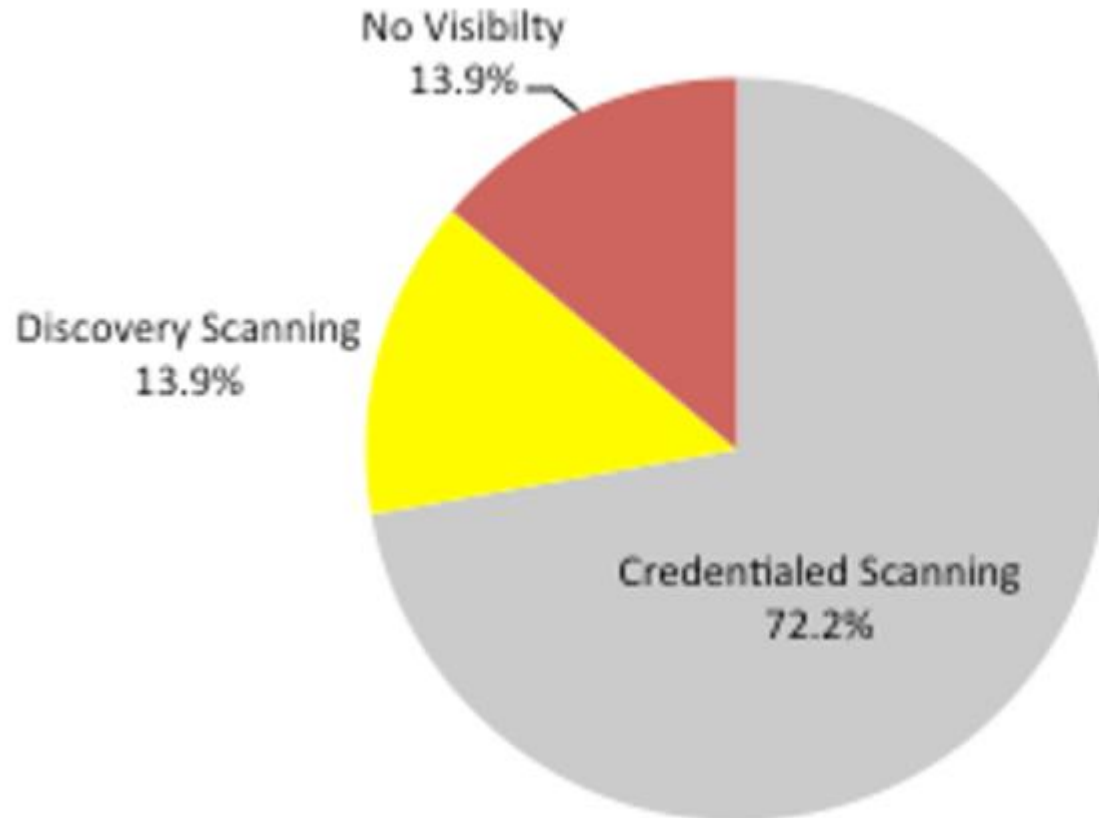


- Credential Scanning
- Discovery Scanning
- No Visibility

Report Example 1 – Security Visibility

RECOMMENDED STATE

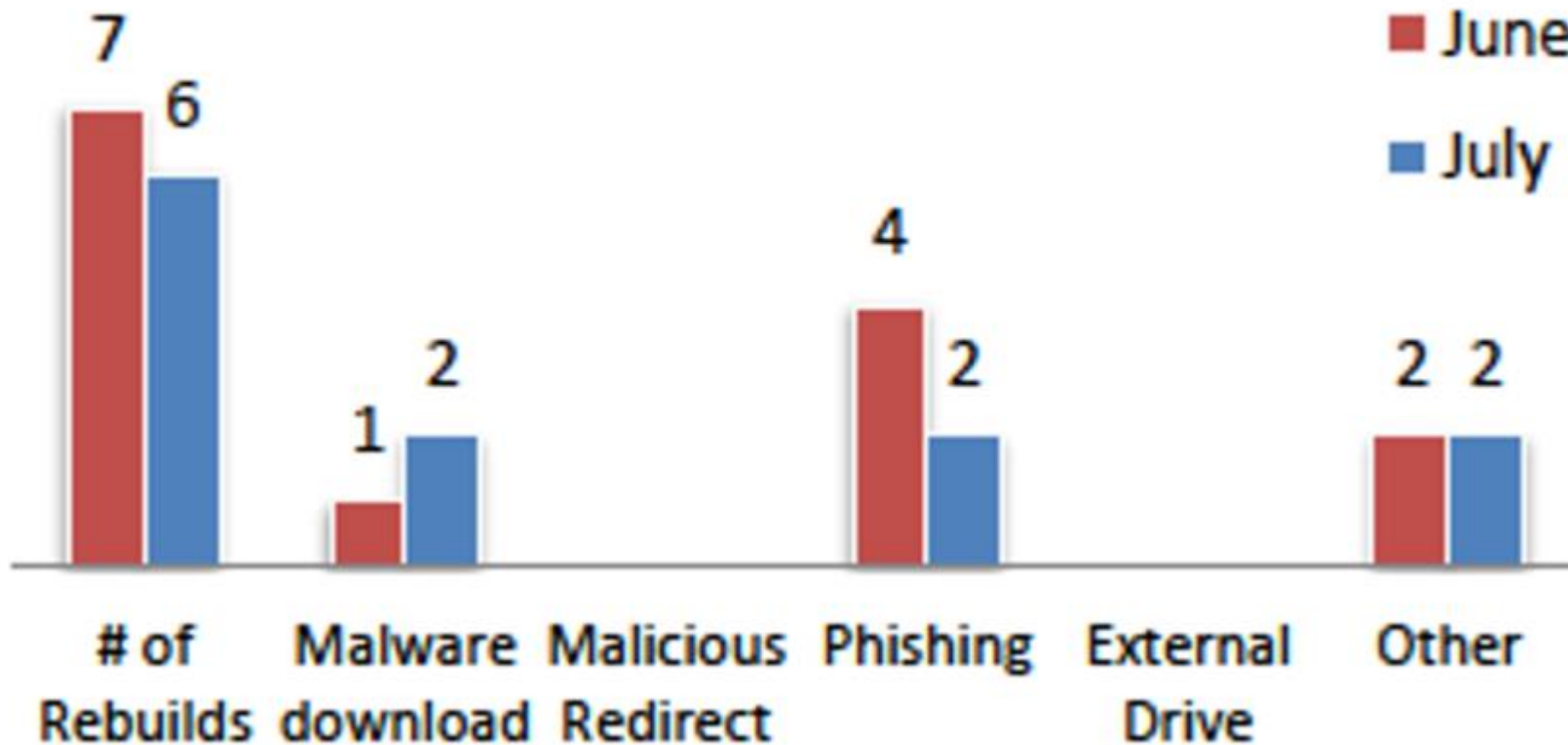
Business Critical Systems Visibility Percentage Visibility



Report Example 2 – Security Incidents by Type

CURRENT STATE

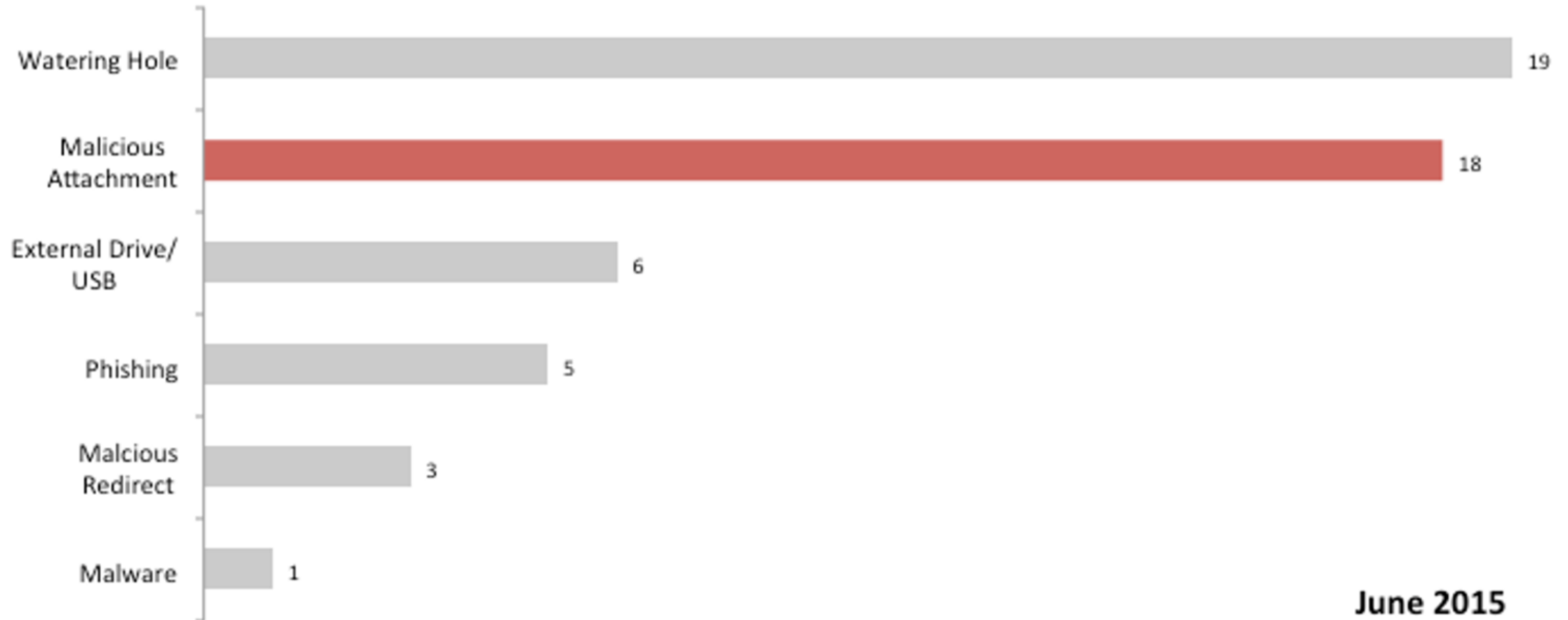
Infection Vector



Report Example 2 – Security Incidents by Type

RECOMMENDED STATE

Previous Month Compromise Vector Breakdown



June 2015



Popular SOC Metrics

SOMETHING TO GET STARTED WITH

1. Total Time to Respond

- *Aggregate for All SOC Analysts (8-Weeks Rolling)*

2. Visibility Matrix

- *Percentage of Total Devices Compared to Actual Devices Monitored*

3. Resolved Security Incidents

- *Count by Month (13-Months Rolling)*
- *Count by Category (8-Weeks Rolling)*

4. Capacity Model

- *Alert Volume Average by Hour each day (8-Weeks Rolling)*



Other Questions to Ask Along The Way

IT'S ABOUT THE JOURNEY

- Were you able to close down other attack vectors?
- What improvements can you make to the plan?
- What types of security awareness can be communicated to the organization?





**HOW DO WE BRING THIS ALL
TOGETHER?**

The Key Takeaways

DOES YOUR INCIDENT RESPONSE PLAN SINK OR SWIM?

1. You want to **use a framework** that works for your organization
2. You want your Incident Response Plan to be **usable**
3. You want sub-plans that are customized for **how you realistically handle situations**
4. You should **have metrics that answer questions**, not create more problems



Thank You



Attributions (Images in Slides)

[Beach View](#)

[Grand Theft Auto](#)

[Mountaintop](#)

[Skull](#)

[Construction](#)

[Fighter](#)

[Photographers](#)

[Street Signs](#)

[Magnifying Glass](#)

[Error Notice](#)

[Shredded Receipts](#)

[Tunnel](#)

[Dog Graphic](#)

[Car Dash](#)

[Horcruxes](#)

[Mario](#)