

The First Responder: A Tale of Incident Handling and Forensics

Max Keiper

CISSP

GISF, GSEC, GCED, GISP, GCIA, GMON

Who is Max?

- 15 years working within IT and Security
 - Education
 - Private Industry
 - State Government
- Experience:
 - Auditing and Security Controls
 - Logging and Continuous Monitoring
 - Incident Handling and Forensic
- Personal:
 - Love to cook, and love to eat!
 - Florida Keys....Palm Trees and Warm Breezes
 - Always need to be challenged....never satisfied.





Our Discussion...

- What is a Incident?
- What is Incident Response?
- What is an Event?
- 6 Steps of Incident Response
- The 3 P's of Incident Handling



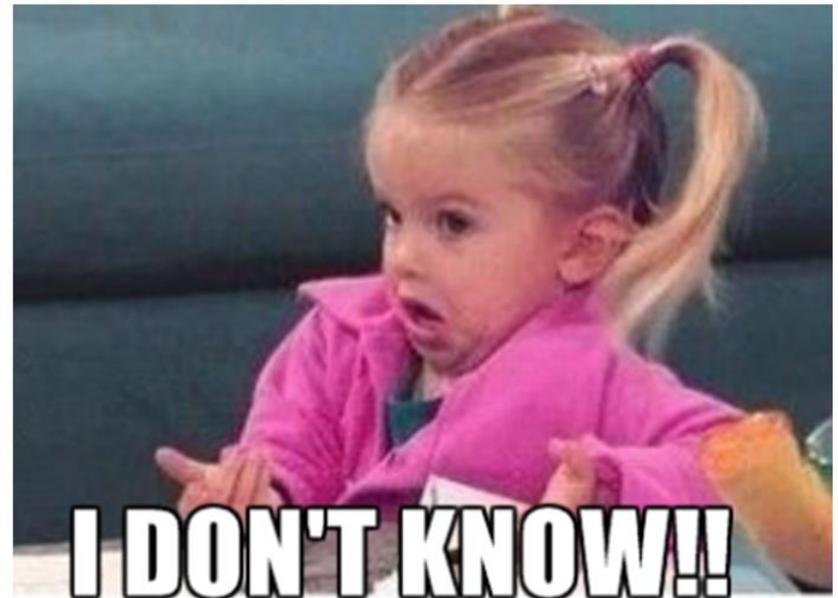
What is an ‘Incident’?

- By Strict Definition:

“Any violation of policy, law, or unacceptable act that involves information assets, such as computers, networks, smart phones, tablets, voice recording systems, cameras, and etc.”(Bejtlich, R, 2005)

Which is an ‘Incident’?

- 1. There are 15,000 unsuccessful login attempts; each 6 seconds apart.
- 2. End user types name and password in login field, then hits enter.
- 3. Login is successful.
- 4. At the home screen, end user types in a search URL .
- 5. Browser opens to a http site .
- 6. End user clicks on a download link on the site.
- 7. End user opens Windows Explorer.
- 8. End user launches a software installer .
- 9. Software installer opens a PHP script that exists on the local system.
- 10. End user logs out.
- 11. Each time a customer clicks on the “buy it” button, a connection to **http://authorizet.com/** opens.



For every action....

- Consequences
 - Sounds bad....really bad
 - Possible Loss of Revenue
 - Short Term
 - Long Term
 - Sony SOE 2011
 - Loss of Reputation
 - Brand
 - Company/Organization or VP/C Level Employees
 - Inter-Organization Professional Team or Individual
 - External Security Team Professional and Peer
 - Might look bad on a resume, but might not.

Incident Examples

- Malicious Code
 - Virus Infection
 - Trojan
 - Worms
 - Malicious Scripting
- Unauthorized Usage of Services
 - Game Play
 - Mail Relay
 - Corporate Assets for Personal Gain
 - Personal Servers on network
- Hoaxes
 - Scams
 - Bomb threats
 - Phishes(Email/Phone)
- Unauthorized Access
 - Access data w/o permission
 - Using another users account
 - Elevating privileges above assigned
 - Abuse account privileges
- Espionage
 - Information Stealing
 - Notebook theft
 - Data copying
 - Tunneling Methods
- Aggressive Probes
 - Port Scans
 - Unusual Network Trends
 - Internal/External Traffic

What is ‘Incident Response’?

- Definition:

“An organized approach to addressing and managing the aftermath of a security breach or attack(also known as an incident). The goal is to handle the situation in **a way that limits damage and reduces recovery** time and costs.”(Rouse, M. 2005)

Steps to Incident Response

- SANS 6 Steps to Incident Handling (SANS,2006)

- 1. Preparation
- 2. Identification
- 3. Containment
- 4. Eradication
- 5. Recovery
- 6. Lessons Learned

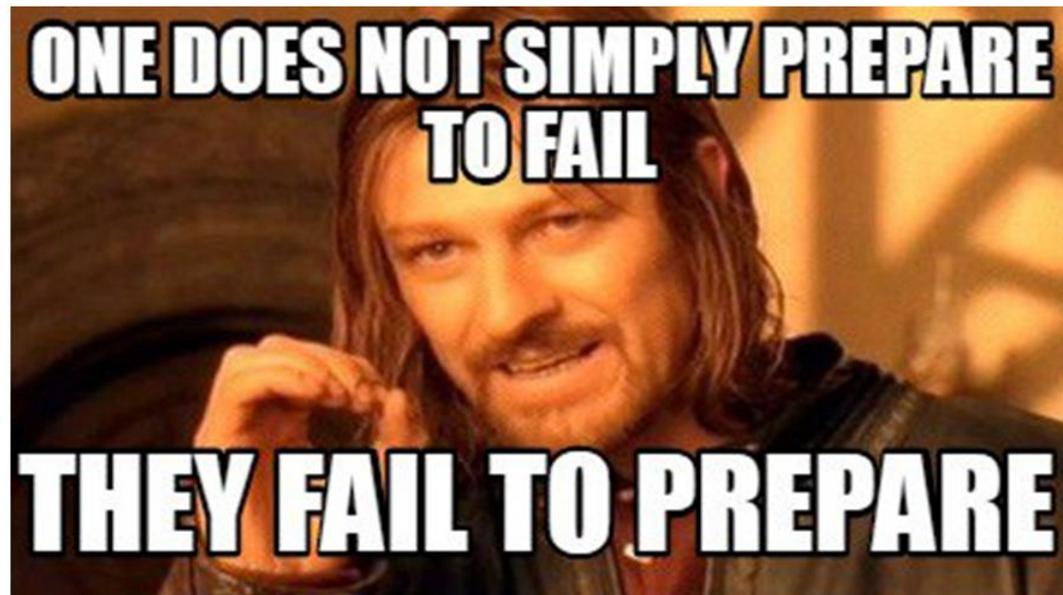
- NIST SP800-61: Computer Security Incident Handling Guide

- 1. Preparation
- 2. Detection and Analysis
- 3. Containment, Eradication and Recovery
- 4. Post-Incident Activity

- NIST Step 3 combines SANS steps 3,4 and 5.

Step 1: Preparation

- Goal is to prepare the team to handle incidents.
 - Hardware failure -> hacked by state sponsored hackers.
 - Ongoing process between Identification and Preparation.
 - Stage to prepare to fight against evil.



Preparation cont....

- Policies
 - Guidance to incidents.
- Response Plan/Strategy
 - Prioritize incidents.
- Communication
 - Contact Strategy/Plan.
- Documentation
 - Evidence(Who, What, When, Where, Why and How)
- Team
 - Legal, HR, PR, IT Staff
- Access Control
 - Team member with ability to add access on the fly
- Tools and Training
 - Software, jump bag, incident drills.

Preparation - Jump Bag

- Incident Handlers Journal
- CIRT Contact List
- USB Drives and Live CD
 - USB preloaded with tools
 - Blank USB for image or payload gathering
 - CD/DVD with a PE image or bootable image
- Laptop with forensic software
- Physical tools(screw drivers, static bags, pens, jumpers, cables of all assortments, SATA drive)
- Drive duplicators with write-block to make bit level images.
- Evidence bags, chain of custody form and tape, zip lock bag.

Stuff the Jump Bag



Step 2: Identification

- This phase is to identify whether an event is an incident or not by collecting and analyzing all the events happening in the system.
- Investigate:
 - Network Perimeter Level
 - Host Perimeter Level
 - System Level
- Gather events from various sources:
 - Log Files
 - IDS
 - Firewalls
- Incident should be reported as soon as possible.

TIME OUT! What is an event?????

- Definition:
 - *“An observable occurrence in an information system that actually happened at some point in time”*
 - An Email
 - A Phone Call
 - A System Crash
 - A Request for Virus scans to be performed on a file or attachment



Event Creating Tools

- Logging:
 - ArcSight
 - Splunk
- IDS/IPS
 - Network IDS
 - Snort
 - OSSIM
 - Bro
 - Host IDS
 - Tripwire
 - OSSEC
- Traffic Monitoring:
 - Ettercap
 - SolarWinds
 - Nagios
- Packet Sniffing:
 - Wireshark
 - Kismet/NetStumbler
- Vulnerability Assessment:
 - Security Center/Nessus
 - Tripwire IP360
 - OpenVAS

Identification cont....

- Recommendation to have 2 incident handlers.
 - 1 handler identify and assess the incident(primary)
 - 1 handler helps gather evidence
- Handlers must document everything.
 - 5W and 1H
- After scope is determined and documenting evidence the CIRT can move forward. (Incident Response Process, 2008)

Step 3: Containment

- The goal is to contain the incident and prevent its spread to other areas.
- Phases:
 - Short-term
 - System back-up(Forensic Tool Kit, EnCase)
 - Long-term containment



Containment cont...2

- Business Unit/Managements blessing!!!
- Isolate the infected system from the network.
 - Pull the network cable.
 - Save network connection information.
 - Move to a different VLAN.
- Make a complete backup of the system.
 - Memory Dump
 - Drive Bit Copy
 - Network Connections
 - Running Services

Containment cont...3

- Protect human life and peoples safety.
- Protect classified and sensitive data.
- Protect other data, including proprietary, scientific, and managerial data.
- Protect hardware and software against attack
- Minimize disruption of computing resources.



Step 4: Eradication

- Removal and Restoration of Affected Systems.
- Continue documenting:
 - Calculates man hours.
 - Overall impact to the organization.
 - Allows for review list to ensure clean up.
- **D - UP!! AND LOCK DOWN!!**
 - Patch the system.
 - Fix the leak, harden the system.
 - Microsoft Baseline Hardening(security templates)
 - Microsoft Security Configuration Wizard
 - CIS Benchmarks(CIS-CAT)
 - Tripwire, SecureCheQ(Free)
 - Secure Build Standard?????!! Build your own checklist.
 - Ensure there is **NO** compromise again!

SecureCheq

Scan System Results Details OVAL XML Summary Report Test Report Print

SecureCheq Rating:  50%



SecureCheq tests for just a sampling of dangerous configuration vulnerabilities. **YOU CAN CONTROL THEM ALL. LEARN HOW.**

Test Name	Result
SUMMARY REPORT	Pass: 50%
TEST REPORT	22 Tests
Windows Remote Desktop Configured to Only ...	FAILED
Windows Remote Desktop Configured to Alway...	FAILED
Safe DLL Search Mode is Enabled	FAILED
Anonymous Access to Windows Shares and Na...	Passed
All Shares are Configured to Prevent Anonymou...	Passed
Windows Default Guest Account is Disabled	Passed
Force Encrypted Windows Network Passwords	Passed
Strong Windows NTLMv2 Authentication Enabl...	FAILED
Strong Encryption for Windows Remote Desko...	FAILED
Enable Strong Encryption for Windows Network ...	FAILED
Enable Strong Encryption for Windows Network ...	FAILED
Windows Password Complexity is Enabled	Passed
Minimum Windows Password Length Configure...	FAILED
Windows Account Lockout Counter Configured...	Passed
Windows Account Lockout Duration Configure...	Passed
System Event Log is Configured to a Sufficient S...	FAILED
Logging of Executed Applications is Enabled	FAILED
Logging of Credential Validation is Enabled	Passed
Logging for Successful and Failed Logon Attem...	Passed
Logging for Successful and Failed Logon Attem...	Passed
Logging of Successful System Change Events is ...	Passed
Security Event Log is Configured to a Sufficient ...	FAILED
Latest Security Patch	
Network Access: Shares That Can Be Accessed A...	
Windows Firewall: Apply Local Firewall Rules (D...	
Windows Guest Account: Disabled	
Wireless Configuration Service: Disabled	

Reference(s):

DISA : 1103

http://iase.disa.mil/stigs/os/windows/lu_windows_2008_dc_v6r120_stig_benchmark_20121026.zip

Microsoft : cc758613

<http://technet.microsoft.com/en-us/library/cc758613.aspx>

NIST SP800-53 R3 : CM-6

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf*(more references below)*

DETAILS

This test determines whether the list of users or groups permitted to 'Log on through Terminal Services' is restricted to the Administrators group. Setting the system to only allow Administrators supports the principle of least privilege by ensuring that only the most trusted users are permitted this access. It is recommended to review the list of allowed users or groups to determine if a failure of this test indicates wider access than is absolutely necessary.

REMEDIATION

To remediate failure of this policy test, assign the Administrators group rights to log on through terminal services.

To apply or modify this setting on Windows 2008, Windows 2008 R2:

1. Select a group policy object to edit within the Microsoft Management Console.
2. Select Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment.
3. Right-click **Allow log on through Remote Desktop Services** and select Properties.
4. In the Properties window, select **Define these policy settings** and in the **Members of this group** panel, select each user and then click Remove.
5. Click the **Add User or Group...** button to open the Add User or Group window, and then click Browse...
6. In the **Enter the object names to select (examples):** box, enter **Administrators**, click **Check Names** to verify the name, and then click OK twice to add the Administrators group.
7. Click OK to close the Properties window.
8. Run the **gpupdate** command to apply the change.



Step 5: Recovery

- Restore services to normal.
- System validation after restoration.
- Testing production processes completely.
- Monitor the system:
 - Undetected Malware.
 - Look for known IOC's.
 - Logging enabled and monitor for unauthorized activity.

Critical Windows Events to Monitor

- Service Creation
- User Creation
- Adding users to privileged groups
- Clearing the event Log
- External Media Detection
- Disabling the Windows Firewall
- Useful Guides:
 - <https://www.iad.gov/iad/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm>
 - <http://www.malwarearchaeology.com/cheat-sheets/>

Event 1: Service Creation

- Monitor for service creation events and enable process tracking logs.
- System Event ID: 7045
- Verify on critical systems.
- **High-entropy service** names are highly suspicious.

A service was installed in the system.

Service Name: PSEXESVC
Service File Name: %SystemRoot%\PSEXESVC.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name:	System	Logged:	3/3/2014 11:32:59 AM
Source:	Service Control Manager	Task Category:	None
Event ID:	7045	Keywords:	Classic
Level:	Information	Computer:	InfoSec-VM2
User:	INFOSEC-VM2\security		
OpCode:	Info		

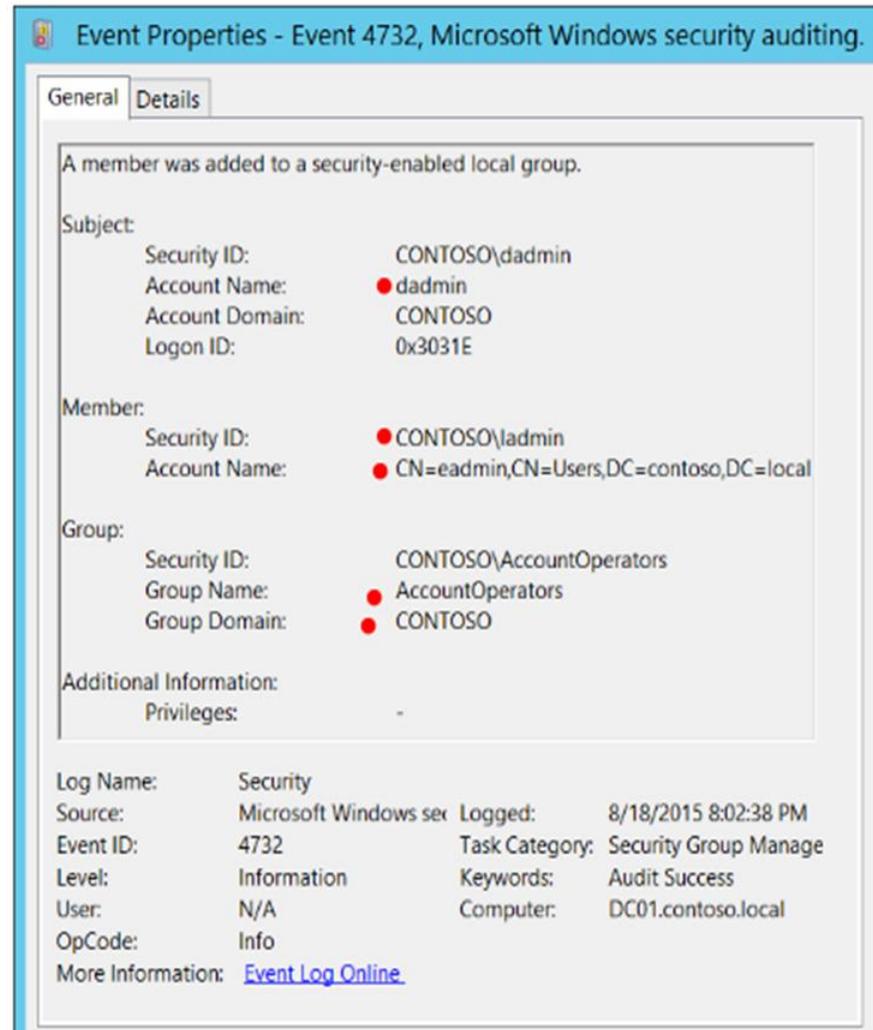
- **Service Name: BhmsdkK304**
- **Service File Name: %SYSTEMROOT%\11ksj.exe**

Event 2: User Creation

- Monitor creation of new accounts
- Creation of local accounts in an Active Directory environment can be a sign of compromise and lateral movement.
- Security Event ID: 4720 – A user account was created
- Security Event ID: 4722 – A user account was enabled
- Security Event ID 4724 – An attempt was made to reset an account's password
- Security Event ID 4738 – A user account was changed.

Event 3: Adding Users to Groups

- Configure systems to issue a log entry and alert when an account is added to or removed from domain administrators' group.
- Log entry and alert when a new local administrator account is added on a system.
- Security Event ID: 4732 – A member was added to a security-enabled local group.

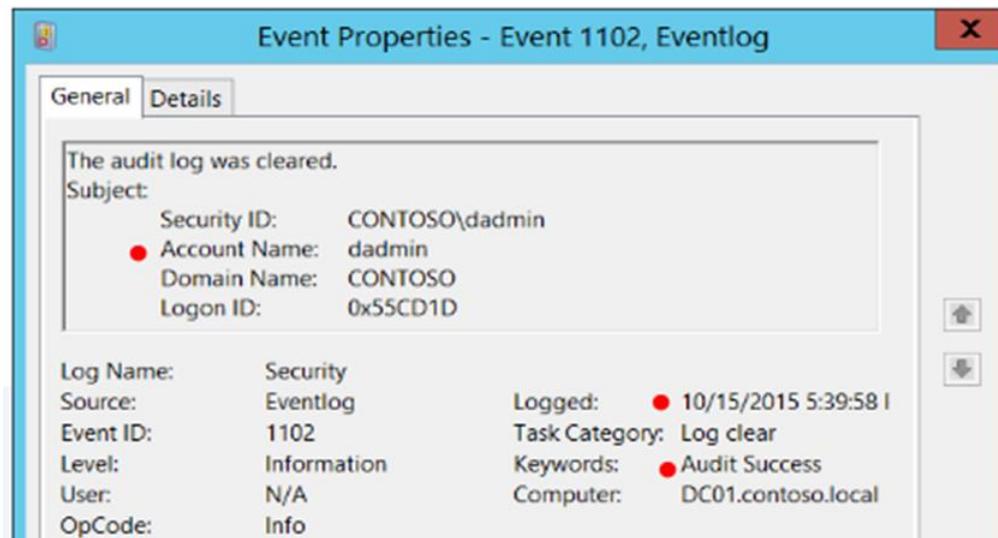


The screenshot displays the 'Event Properties' window for Event 4732, titled 'Event 4732, Microsoft Windows security auditing'. The window is divided into 'General' and 'Details' tabs. The 'Details' tab is active, showing a message: 'A member was added to a security-enabled local group.' Below this, the event details are organized into sections: 'Subject', 'Member', 'Group', and 'Additional Information'. The 'Subject' section lists: Security ID: CONTOSO\dadmin, Account Name: dadmin, Account Domain: CONTOSO, and Logon ID: 0x3031E. The 'Member' section lists: Security ID: CONTOSO\dadmin and Account Name: CN=eadmin,CN=Users,DC=contoso,DC=local. The 'Group' section lists: Security ID: CONTOSO\AccountOperators, Group Name: AccountOperators, and Group Domain: CONTOSO. The 'Additional Information' section shows Privileges: -. At the bottom, a metadata table provides further details.

Log Name:	Security	Logged:	8/18/2015 8:02:38 PM
Source:	Microsoft Windows security auditing	Task Category:	Security Group Management
Event ID:	4732	Keywords:	Audit Success
Level:	Information	Computer:	DC01.contoso.local
User:	N/A		
OpCode:	Info		
More Information:	Event Log Online		

Event 4: Clearing Event Logs

- Erasing logs is a common blackhat technique.
- Covers tracks, destroys evidence of the attack.
- Security Event ID: 1102 – The audit log was cleared.
- System Event ID: 104 – The Application or System log was cleared.



Event 5: External Media Detection

- Limit the use of external devices to those that have a business need.
- Disable auto-run from all removable media.
- Security Event ID : 7045 – Service Creation
- System Event ID(s): 10000, 10001, 10100, 20003, 24576, 24577, 24579 and 20001
- Re-use of an already-seen device = 0 Events



Event 6: Disabling the Firewall

- Disabling generates logs in Windows Application and Service log.
 - Application and Services Logs -> Microsoft -> Windows -> Windows Firewall with Advanced Security -> Firewall
- Use PowerShell to query.
 - PS C:\>Get-Winevent -FilterHashTable @{LogName="Microsoft-Windows-Windows Firewall With Advanced Security/Firewall"; ID=2003}
- Advanced Firewall Event: 2003

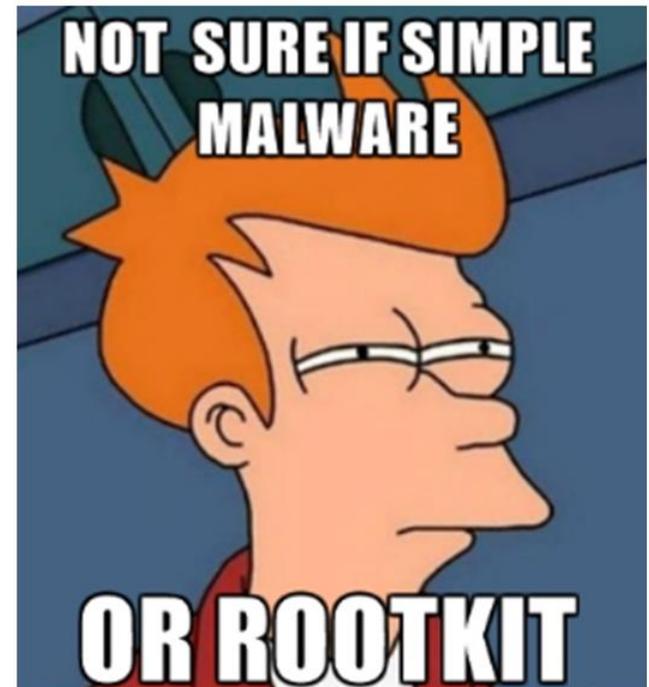


Step 6: Lessons Learned

- Document the entire incident handling process.
 - Power Point
 - Report representing the 5W and 1H
 - Executive Summary
- Overall goal is to learn from the incidents.
- Documentation can be used as training materials.(Bejtlich, 2005)
- Meet within 2 weeks to discuss.

Lessons Learned cont.

- Send any unidentifiable malware to AV vendor.
- Cross training from the Incident Handler.
- Update IOC rules.
 - URL filters
 - Email Filters
 - IDS
- User outreach and education.



The 3 P's of IH

- **Preparation**
 - Train the team.
 - Ensure controls are in place.
 - Always look for ways to improve the Security Program.
- **Patience**
 - Formulate a strategic solution instead of being hasty.
 - When it comes to funding for Security.
- **Persistence**
 - Continue analyzing, automate if possible.
 - Build an IOC dictionary.

Incident Handling Take-Away

- Make sure you take great notes and keep a timeline.
- Ensure the Business Unit/Management is involved and updated.
- Ensure the handling team is running on all cylinders.
- Do not over react or jump to conclusions. Haste makes waste!
- Keep team updated with status as time progresses, checkpoints.
- Prepare the team, keep them educated with latest trends, tools, tactics.
- Learn from your mistakes and always prepare.

Points of Reference

- SANS InfoSec Reading Room
 - www.sans.org/reading-room
 - Incident Handler's Handbook – Patrick Kral
 - Malware 101 – Viruses – John C Bambenek
 - From Events to Incidents o Charles Pham
- NIST SP 800-61 – Incident Handling Guide
- Malware Archaeology
 - www.malwarearchaeology.com/cheat-sheets/
- Center for Internet Security(CIS)
 - www.cisecurity.org
 - System hardening documents.

PRESENTATION FINISHED

ANY QUESTIONS?



CHUCK NORRIS

**APPROVED THIS
PRESENTATION**

