

# INDICATORS OF COMPROMISE

INDUSTRIAL CONTROL SYSTEM SECURITY WORKSHOP  
JUNE 22-23, 2017



# INDICATORS OF COMPROMISE

- Artifacts or events observed on systems or networks that provide a high degree of confidence that an intrusion has occurred.

# TRADITIONAL FORENSIC ARTIFACTS

- Hash value (MD5 Signature)
- Compile time
- File Size
- Path Locations
- Registry Keys
- Memory

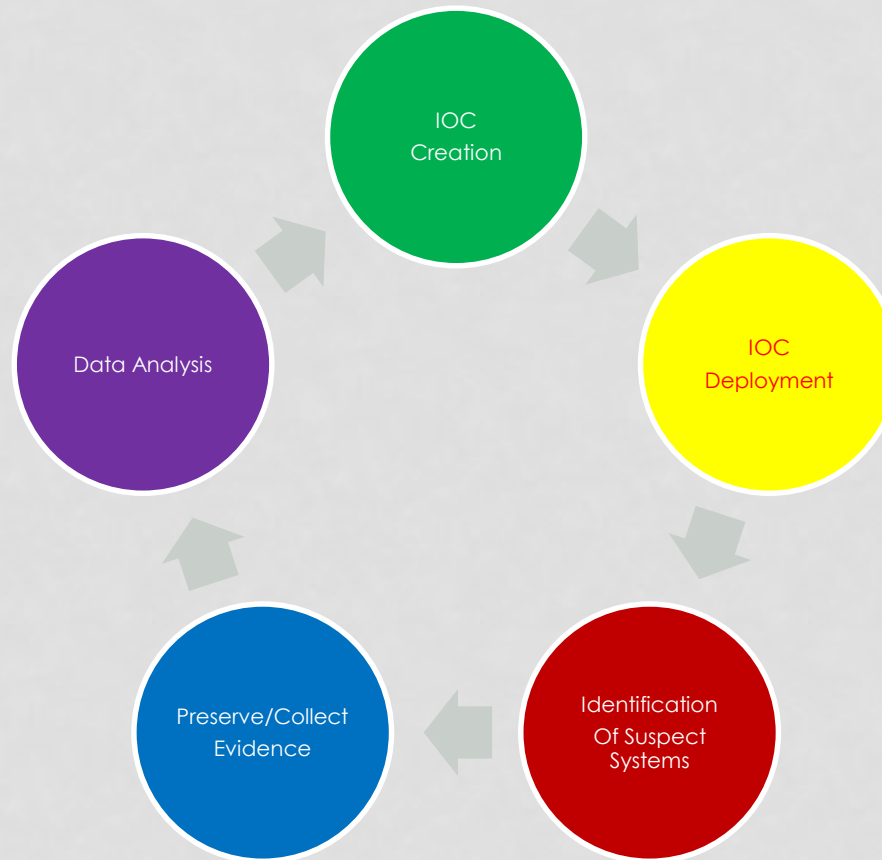
# TOP INDICATORS OF COMPROMISE

- Unusual Outbound Traffic
- Behavior Anomaly on Privileged Account
- Unusual Geographical Connections
- High Volume of Database Transactions
- Spike on Web Traffic Activity
- Activity on Obscure Port
- Suspicious Registry Edits
- Unexpected System Patch
- Signs of DDoS Attacks
- Presence of unfamiliar files

# METHODOLOGY OF CREATING AN IOC

- Do not focus on specific pieces of forensic evidence
- Focus instead on the common thread of actions such as recurring tactics or tools used by adversaries
- Use an iterative and looped continuous improvement processes.

# IOC DEVELOPMENT CYCLE



# PROPERTIES OF THE BEST IOCS

- IOC identifies only attacker activity
- IOC is inexpensive to evaluate
- IOC is expensive for the attacker to evade

# MANDIANT IOC EDITOR

- Free Tool for creating IOCs with a graphical user interface
- Available at the FireEye® (Mandiant) Web site:  
<https://www.fireeye.com/services/freeware/ioc-editor.html>

The screenshot displays the MANDIANT IOC EDITOR application window. The title bar reads "IOCe 2.2.0 - C:\Temp\IOC". The menu bar includes "File", "Search", "Tools", and "Help".

On the left, a table lists existing IOCs:

Name	Created	Updated
"Sam...	2016-06-21 21:5...	2016-0

The main configuration area on the right contains the following fields:

- Name: "Sample"
- Author: G Francia
- GUID: 762822cf-67c7-4d57-a5fc-59f5895ea5b8
- Created: 2016-06-21 21:56:41Z
- Modified: 2016-06-21 22:26:19Z
- Description: Sample threat

Below these fields is a tree view for building the IOC logic:

- OR
  - AND
    - Email Attachment Size is >5700
    - OR
      - Email Sender contains SPAMOrig
      - OR
        - Email Attachment Name contains ShowMe.exe

On the right side of the logic tree, there are two panels:

- Content**: ShowMe.exe, Length: 10
- Context**: Document: Email, Search: Email/Attachm, Context Typ: mir
- Indicator Item**: ID: e3bd1283-ac9
- ID**: Unique ID of the Indicator Item.

At the bottom, a "Save" button is visible. The status bar at the very bottom indicates "Loaded IOCs: 1 | Unsaved IOCs: 1".