INDICATORS OF COMPROMISE

INDUSTRIAL CONTROL SYSTEM SECURITY WORKSHOP
JUNE 22-23, 2017

JSU JACKSONVILLE STATE UNIVERSITY

NSF

Gadsden State Community College 1898

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

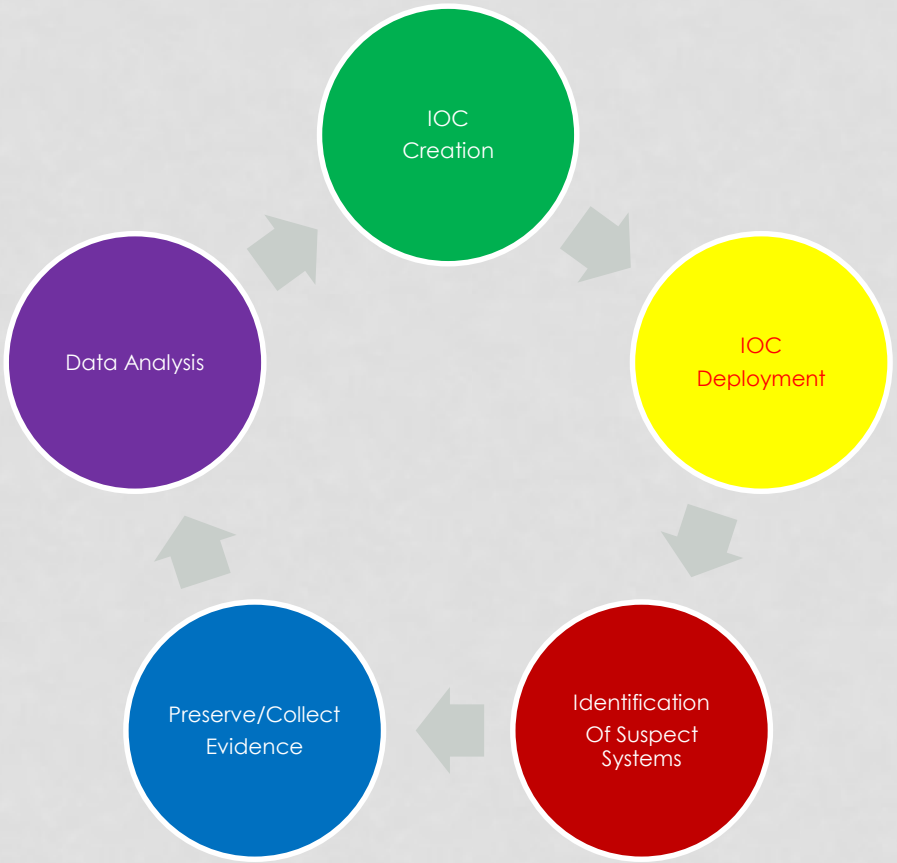
TOP INDICATORS OF COMPROMISE

- 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



Source: www.openioc.org White paper: "Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC." 2013.

PROPERTIES OF THE BEST IOCS

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

Source: www.openioc.org White paper: "Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC." 2013.

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