ENABLING DISTRIBUTED INCIDENT MANAGEMENT

TOM MILLAR
Chief of Communications, US-CERT

Enabling What?

- "Distributed Incident Management"
- Coordinated, concurrent action directed to rapidly identify an incident, analyze its implications, assess the impact, and respond effectively across multiple heterogeneous sectors, communities and organizations
- And automating wherever possible

Some CSIRTs practice limited coordination in incident management today, because they have to (i.e. US-CERT).

We need to formalize the "doctrine" of distributed/coordinated incident management in order to benefit from network effects.

Obstacles and Approaches

- The "PICERF" process model
- An alternative "loop" model
- The "CAT 01-06" incident taxonomy
- An alternative Method & Impact taxonomy

The most commonly used process model for cyber incident response today is over 20 years old. We call it "PICERF."

PICERF:

- Prepare
- Identify
- Contain
- Eradicate
- Recover
- Follow-up

The PICERF model was born out of a DOE lab's experiences handling targeted intrusions in the late 1980s - then borrowed by SANS and later NIST

PICERF describes a linear framework for handling an incident within your own shop.

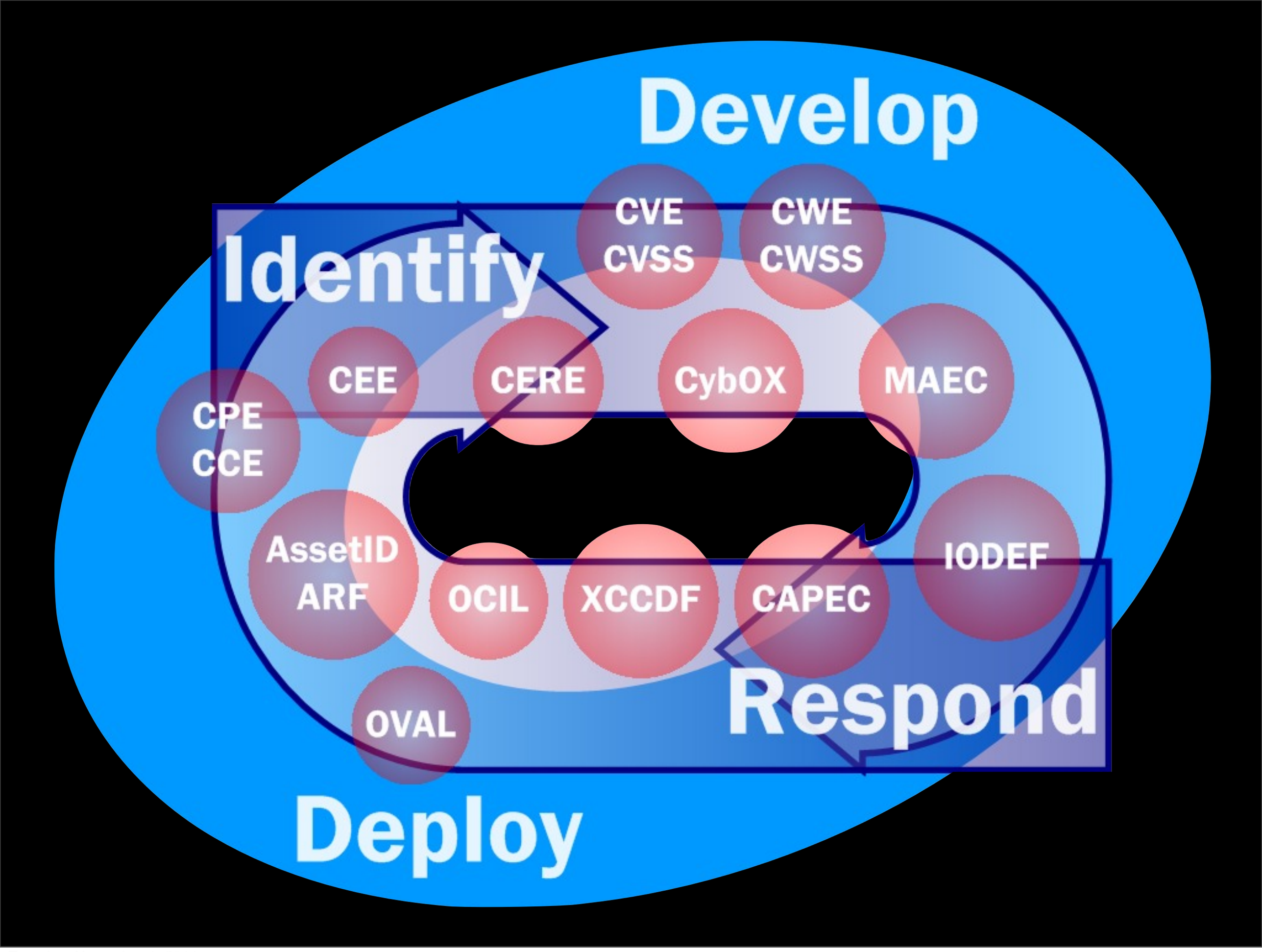
Liaison and information sharing functions are peripheral!

Our alternative is based on OODA:

- Observe
- Orient
- Decide
- Act

Using the OODA loop as a starting point, we developed a process model that integrates liaison and collaboration throughout

The model is also data-driven - each phase implies the collection, enrichment and collaboration around certain data elements


Develop
Identify
CVE
CVSS
CWE
CWSS
CEE
CERE
CybOX
MAEC
CPE
CCE
AssetID
ARF
OCIL
XCCDF
CAPEC
IODEF
OVAL
Respond
Deploy

Tying the phases of our "Identify" and "Response" cycles to data elements allowed us to identify a gap:

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	A person gains logical or physical access without permission to a federal agency network, system, application, data, or other technical resource.	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Inappropriate Usage	A person violates acceptable use of any network or computer use policies.	Weekly
CAT 5	Scans/Probes/ Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

#1 Problem with the 2006-era Categories: Conflating *Effects* (root access, denial of service) with *Causes* (malware, improper use)

Cause = Method

Effect = Impact

More Specifically:

- Method
- Functional Impact
- Information Impact
- Time and Money Impacts
- Recoverability

Methods:

- Resource Exhaustion
- External Media
- Web
- E-Mail
- Improper Usage
- Lost/Stolen Equipment
- Other

Functional Impact Types:

- High = "Closed for Business"
- Medium = Restricted
- Low = Loss of efficiency
- None

Information Impact Types:

- Privacy = PII, PHI
- Proprietary = PROPIN, PCII
- Classified = S, TS, SCI
- Controlled Unclassified
- None

Recoverability:

- Impossible = "Barn door, horse, etc."
- Severe = TTR is unpredictable
- Major = Recovery demands new resources
- Minor = Recovery is possible with current resources

By separating method from impact, and allowing for multiple dimensions of impact, we can begin to develop better tailored data models for incidents

Hypothesis:
Better data =
Better coordination =
Better response across
near, medium and long
term - eventually
including safer code!