



Leveraging Orchestration to Facilitate Knowledge Transfer in Security Operations

About Me



Mike Fowler CISSP

Vice President of Professional Services | DFLabs

Mike Fowler is a former Police Detective and U.S. Air Force veteran with over two decades of experience in incident response and forensic investigations and training.

Mike was a Senior Director in the Professional Development and Training division at Guidance Software training over 5000 students per year. In 2015 the training program was named SC Magazine's "Best IT Security-Related Training Program". Mike currently sits on the Advisory Committee for the Cybersecurity for Executives Certificate Program at the University of South Florida

Mike is a Certified Information Systems Security Professional (CISSP®) and currently makes his home on the East coast of the United States.

What is “Knowledge Transfer” and why do we need it?

The transfer of knowledge related to incident response processes, intelligence and procedures from senior, more experienced incident responders to less experienced responders to act as an organizational force multiplier. Sometimes this is referred to as “Tribal Knowledge”.

Why do we need knowledge transfer as a part of our IR infrastructure

- As threats evolve, so must response capabilities
- Experience is the best teacher, and transferring that expertise can be time consuming
- Training must be built upon a foundation of knowledge application (how it was used effectively) and not merely the provision of knowledge (anecdotal examples frequently lack validity)

Why do we need knowledge transfer as a part of our IR infrastructure (continued)

- Knowledge transfer provides us with 3 key elements needed for a successful incident resolution process;
 - Repeatable
 - Defensible
 - Consistent

Why isn't this a fundamental part of SOC operations?

- Typically, training is not a chief consideration
- It's difficult to gauge the ROI
- There are other alternatives to a formalized process, however these methods tend to be dumping grounds with little positive impact on daily operations

Knowledge Transfer isn't just for Incident Responders

- Legal for GDPR compliance
- HR for personnel issues
- Stake holders for ROI/Funding

5 Key Elements of a Successful Transfer of Knowledge

1. Understand Your Audience
2. Develop Focused Curriculum
3. Designate the Appropriate Delivery Method
4. Designate a Messenger
5. Evaluate the Results

Breaking Down the Elements

Understand Your Audience

- Provide as much context as possible to ensure clarity of task
- Identify who will actually be getting the most benefit from the information, not just who may top the organizational charts
- Craft the message to the audience (IT jargon with legal folks gets blank stares)

Develop Focused Materials

- The information transfer should focus on clearly defined goals for the identified audience ex. ITSEC has 1 set of goals, legal another, Senior stakeholders yet a third.
- Focus the information on those tasks that are relevant to resolving the identified issues
- Should be based on regulations. Absent a defined set of regulations, should be based on best practices.

Determine the Appropriate Delivery Method

- Manual
 - Regularly scheduled training session
 - Internal Listserv
 - Access to webinars and online content
- Automated
 - Formalized Knowledge Base
 - Structured Playbooks

Designate a Messenger

- Should be an organizational/functional SME
- Allow a cross-section of Subject Matter Experts to contribute
- Ensure they are part of periodic reviews

Evaluate the Results

- Training materials are living documents
- Integral part of the after-action report
- Scheduled periodic reviews



Implementing a Framework to Provide Knowledge Transfer Organizationally*

*without breaking the bank

Goals

- Provide cost effective knowledge transfer
- Provide our teams with opportunities that enhance knowledge, develop skills and enrich the organization
- Promote, support and leverage technology resources and tools to improve and enhance incident response workflows
- Provide ongoing leadership and support to the organization's succession efforts

Dual Delivery Method Approach

- Knowledge Base
- Incident Playbooks



Knowledge Base

The library Benjamin Franklin wished he had invented

Benefits of a Formalized Knowledge Base

- Facilitates faster IR processes
- Provides consistent information across incidents
- Connects remote incident handlers to a common ruleset
- Prevents knowledge loss; captures and reuses information
- Focuses on relevant information for your teams
- It's a living document, updates can and should be frequent
- Creates a simplified IR taxonomy that can be included in incident templates

- OBSERVABLES
- IP 42
- Mail 6
- URL 7
- Domain 82
- User details 12
- Artifacts 81
- Address book
- Actors
- Custodians
- Assets
- Knowledge base**
- Correlation

- Customer Proprietary Network Information
 - Cyber Incident Response Guide
 - DNA Evidence
 - FCC Incident Response Guide
 - Financial Services Information Sharing and Analy...
 - Fingerprint analysis
 - Forensic DNA Fundamentals
 - Forensics and Response Standard
 - Healthcare Incident Response
 - Max size for file upload
 - Network-wide security event log monitoring
 - Shellshock
 - US-CERT Forensics
 - Win32-Conficker worm

Details

Title	Customer Proprietary Network Information
Description	Protecting Your Telephone Calling Records Information that Your Telephone Company Collects Your local, long distance and wireless telephone companies, as well as your Voice over Internet Provider VoIP, collect information such as the numbers you call and when you call them, as well as the particular services you use, such as call forwarding or voice mail. These companies collect this customer information, also called Customer Proprietary Network Information CPNI so they can provide the services you have requested and send you bills for them.
Tags	CPNI telco communications mobile network security digital security
Category	-

Attachment details

[DOWNLOAD](#)

File name	CPNI.pdf
File type	pdf
File size	64128 bytes
SHA256	525f611d4f88652190a62663334db4538c4450844f7a7c40422f118d49bbe482
Uploaded	09-18-15 06:52 am

Involved incidents

 Show entries

Incident Id	Kind	Type	Purpose	Status	Created by
04222016-2 [Host : H-04222016-2161]	Forensics	Internal affairs	Generic	Open	IncMan Administrator
04222016-2 [Incident]	Forensics	Internal affairs	Generic	Open	IncMan Administrator
FOR_CASE_94/2015 [Incident]	Incident Response	Application Vulnerability, Internal affairs, Legal, General	Generic	Open	IncMan Administrator
I-7 [Incident]	Incident Response	Civil, General	Mitigation	Open	IncMan Administrator

CREATE NEW INCIDENT

DETAILS

ADDITIONAL INFO

PARENT FOLDER

RELATED INCIDENTS

INVESTIGATORS

PLAYBOOK

RUNBOOK

KNOWLEDGE BASE


NOTIFICATIONS

ARTIFACTS

OBSERVABLES

Custom search

Documents you may be interested in:

	ADD DOCUMENT
<input checked="" type="checkbox"/> US-CERT Forensics 	Title: US-CERT Forensics
<input type="checkbox"/> Forensics and Resp...	Category: Forensic
<input type="checkbox"/> Financial Services...	Description: The need for computer forensics to be practiced in an effective and legal way. The need to understand how computer forensics fits as a strategic element in overall organizational computer security. Network administrators and other computer security staff need to understand issues associated with computer forensics. Those who work in corporate governance, legal departments, or IT should find an overview of computer forensics in an organizational context useful.
<input type="checkbox"/> Shellshock	Tags: US-CERT
<input type="checkbox"/> Forensic DNA Funda...	Number of attached files: 1
<input type="checkbox"/> DNA Evidence	File name: us-cert_forensics.pdf
<input type="checkbox"/> Fingerprint analys...	
<input type="checkbox"/> Healthcare Inciden...	
<input type="checkbox"/> Cyber Incident Res...	

Documents selected:

SAVE

CLOSE



Incident Playbooks

No team ever went to the Super Bowl without one

Benefits of Using Incident Playbooks

- Significantly reduces the chance for human error
- Promotes consistency across incident handlers
- Increases Incident handler confidence
- Reduces training time
- Ensures compliance with requisite industry requirements
- Easily integrates into your existing IR lifecycle
- Promotes retention of established processes and procedures

- AUDIT
 - Social engineering template
- CHANGE REQUEST
 - Execute Firewall Change Request (Manuall...
- CRIMINAL
 - Blackmail attempt Template
 - DDoS Template
 - Forensic and Incident Handling Template
 - Phishing IR Template
 - Website Defacement Template
- DIGITAL FORENSICS
 - Forensic Analysis Template
- DNA ANALYSIS
 - DNA Evidence Analysis Template
- FRAUD
 - Employee Fraud
- INTERNAL AFFAIRS
 - DLP Violation - Email
 - Insider Abuse Template**
 - PII Incident Handling
- INTRUSION
 - Linux intrusion Template
 - Malware Scenario Template
 - Smartphone Malware Template
 - Windows Intrusion Template
- LEGAL INVESTIGATION

Insider Abuse Template

Type	Internal affairs	Last Updated	06-20-18 07:17 am
Related Playbook	Insider abuse		
Description			

Template Actions

+ CATEGORY Collapse all | Expand all

Preparation + TASK + ACTION

Make sure to also have contact points in your public relation team, human resources team and legal department

Action	Make sure to also have contact points in your public relation team, human resources team and legal departme	Description	Make sure to also have contact points in your public relation team, human resources team and legal department
Reference	Make sure to also have contact points in your public relation team, human resources team and legal departme		
Authorization	Owner	Due Date	Mandatory
<input type="text" value="- Please select -"/>	<input type="text" value="- Please select -"/>	<input type="text" value="day"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No


- ▶ Have a centralized logging facility
- ▶ Be sure to have a global authorization and clearance process.
- ▶ Provide strong authentication accordingly to the risk of the business application

Identification + TASK + ACTION

- ▶ Alerts from a SIEM or correlation tools

Summary

- Establishing a formalized knowledge transfer process has a strong ROI
- It fits easily within an organizations incident handling methodology
- Provides low cost, long-term benefits to any organization



Thanks and Have a Great Conference!

Mike.Fowler@DFLabs

<https://www.dflabs.com>