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.

DFLABS
CYBER INCIDENTS UNDER CONTROL

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”.

DFLABS
CYBER INCIDENTS UNDER CONTROL

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)

DFLABS
CYBER INCIDENTS UNDER CONTROL

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

DFLABS
CYBER INCIDENTS UNDER CONTROL

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 positivr impact on daily operations

DFLABS
CYBER INCIDENTS UNDER CONTROL

Knowledge Transfer isn’t just for Incident Responders

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

DFLABS
CYBER INCIDENTS UNDER CONTROL

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

DFLABS
CYBER INCIDENTS UNDER CONTROL

Breaking Down the Elements

DFLABS
CYBER INCIDENTS UNDER CONTROL

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)

DFLABS
CYBER INCIDENTS UNDER CONTROL

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

DFLABS
CYBER INCIDENTS UNDER CONTROL

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

DFLABS
CYBER INCIDENTS UNDER CONTROL

Evaluate the Results

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

DFLABS
CYBER INCIDENTS UNDER CONTROL

Implementing a Framework to Provide Knowledge Transfer Organizationally*

*without breaking the bank

DFLABS
CYBER INCIDENTS UNDER CONTROL

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

DFLABS
CYBER INCIDENTS UNDER CONTROL

Dual Delivery Method Approach

- Knowledge Base
- Incident Playbooks

DFLABS
CYBER INCIDENTS UNDER CONTROL

Knowledge Base

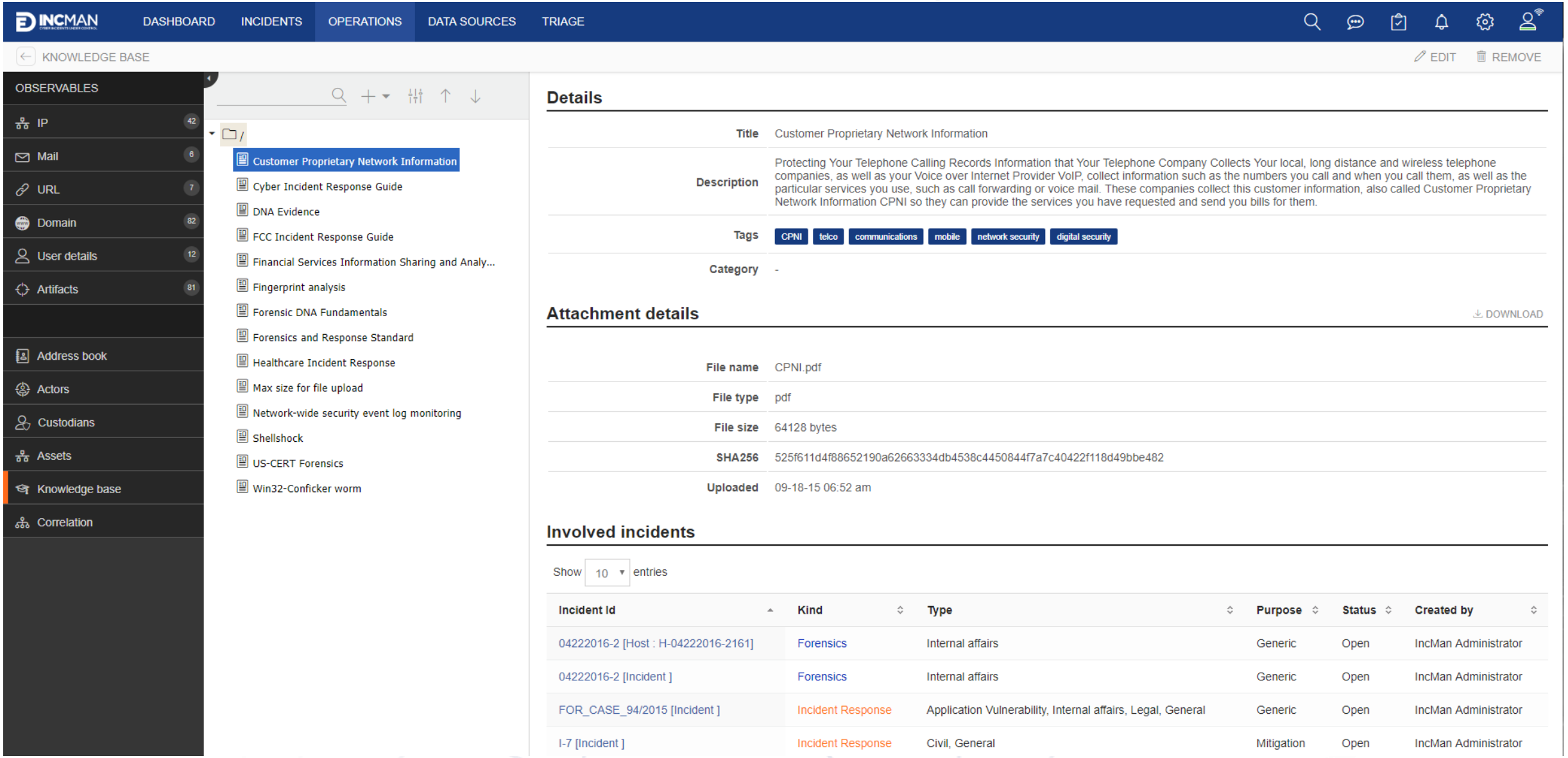
The library Benjamin Franklin wished he had invented

DFLABS
CYBER INCIDENTS UNDER CONTROL

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

DFLABS
CYBER INCIDENTS UNDER CONTROL



DFLABS
CYBER INCIDENTS UNDER CONTROL

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:

- US-CERT Forensics
- Forensics and Resp…
- Financial Services…
- Shellshock
- Forensic DNA Funda…
- DNA Evidence
- Fingerprint analys…
- Healthcare Inciden…
- Cyber Incident Res…

ADD DOCUMENT

Title:	US-CERT Forensics
Category:	Forensic
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.
Tags:	US-CERT
Number of attached files:	1
File name:	us-cert_forensics.pdf

Documents selected:

SAVE CLOSE

DFLABS
CYBER INCIDENTS UNDER CONTROL

Incident Playbooks

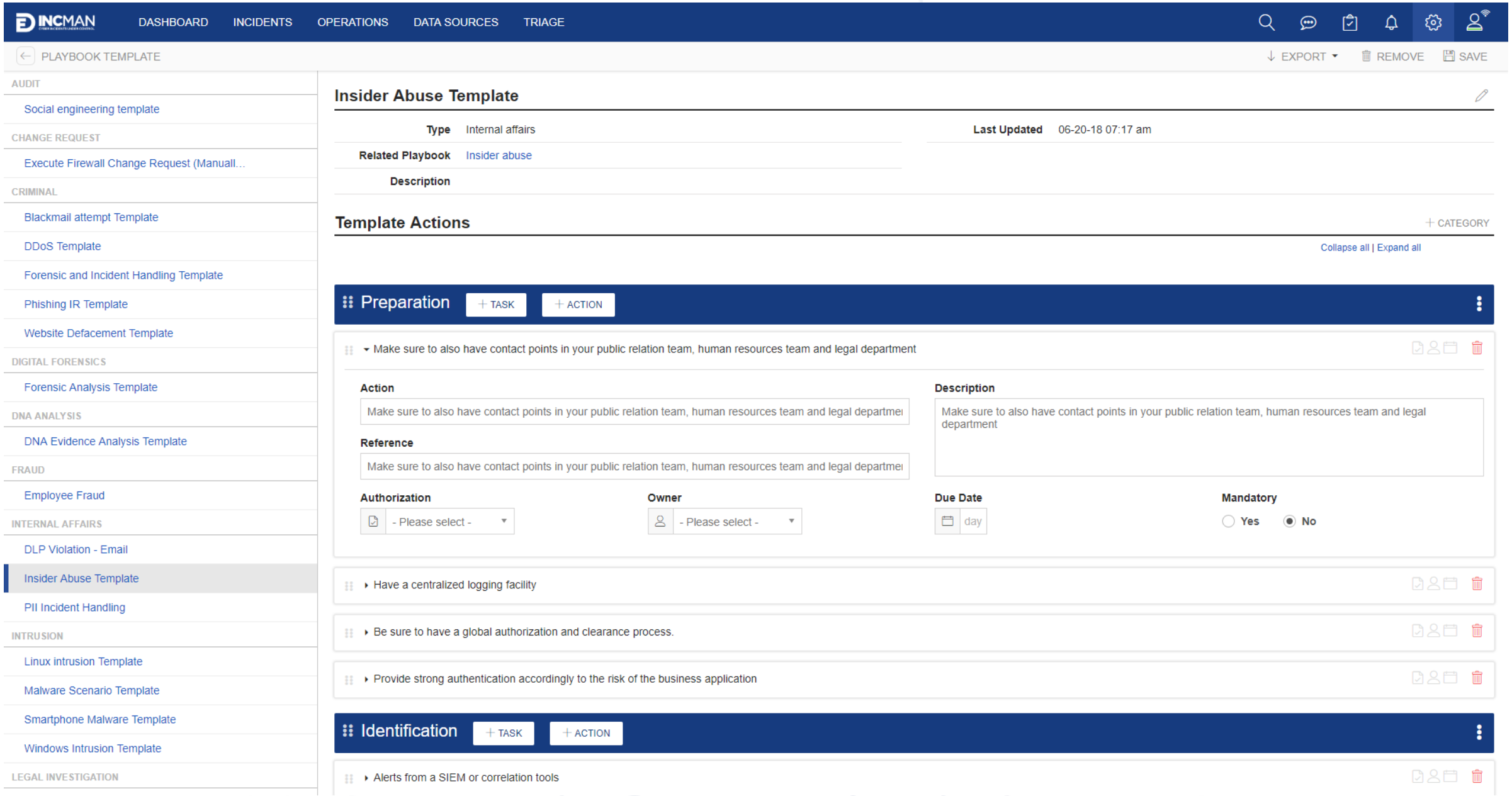
No team ever went to the Super Bowl without one

DFLABS
CYBER INCIDENTS UNDER CONTROL

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

DFLABS
CYBER INCIDENTS UNDER CONTROL



DFLABS
CYBER INCIDENTS UNDER CONTROL

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

DFLABS
CYBER INCIDENTS UNDER CONTROL