Techdefcon
Digital Forensics & Incident Response (DFIR)
Cyber Defense Center

Cyber Security Incident Response Team (CSIRT)

Shonak Reshamwala

October, 2018

www.techdefcon.com info@techdefcon.com

TechDefcon

The Cybersecurity Accelerator

What we do?	Our approach
Techdefcon is a security accelerator that frees companies from security hassle. Providing bespoke solutions and hands-on operational support, the team helps scaling information security from the ground up.	Security without causing friction, disrupting culture or your budget. We get the ball rolling and bootstrap your security program. **Our value-add lies in the execution.** We have fine-tuned our approach over decades working with companies of all industries and sizes.

Cyber Forensic and Incident Response

We provide IR & Forensics Solutions around the world

- Tailored Intelligence – tailored to your environment and profile
- We offers a full range Incident Response & Forensic
- Investigations focuses on Real Time Forensic Investigations
- Using Technologies that make it possible to search, investigate and actively manage any size of complexity.
- This allows us to respond quickly and effectively to any situation and mitigate risk.
  - 77 people:
  - 20 people developers
  - 6 Intelligence Operations
  - 17 Digital Forensics & Incident Response
  - support for the analysts
  - consolidated defence capabilities to a larger amount of customers at an affordable price
  - 24/7/365: augment or replace existing teams
  - Solution for eliminating many other tools
  - Centralized: No data leaves the customer site

Cyber Forensic and Incident Response

We provide IR & Forensics Solutions around the world

Our incidence response:

- Intelligence
- Detection Response
- Mediation

Intelligence products:

Bulletin (C-Level)
Brief (includes technical indicators, threat profiling)
Assessment (specific to a company -> enters risk management)
Forecast

Collection:

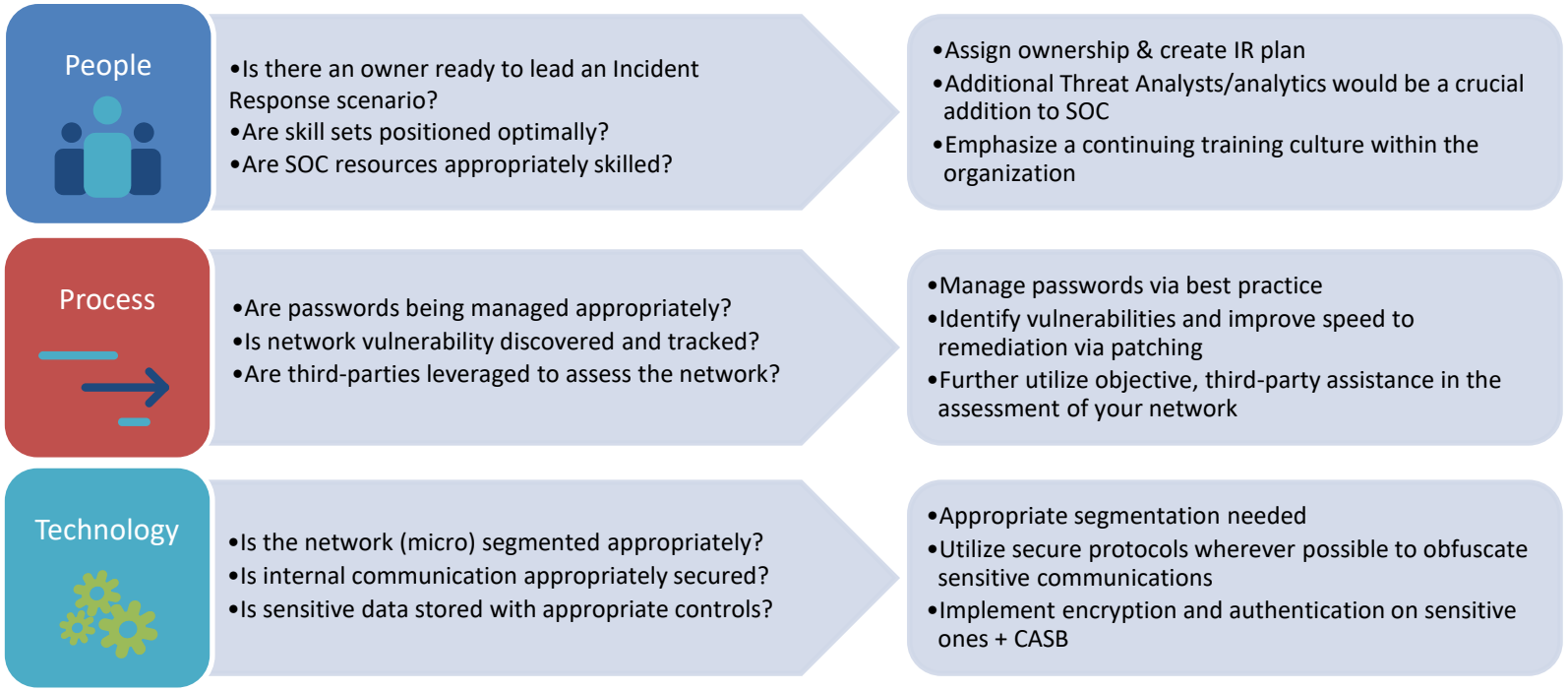
- log file analysis
- malware analysis
- database analysis
- network capture analysis
- data analysis
- visualizations
- identifying file system anomalies.

Log File Analysis example:

- IIS Web Server Logs
- Apache Web Server Logs
- FTP Logs
- Windows Event Logs (EVT and EVTX format)

Approach	Description
	▪ Comprehensive analysis requires static analysis in a suitable forensic tool to view and analyze the file system ▪ Ability to conducting virus scans using MD5 hash signatures
	▪ Operating system virtualization can be used to boot the forensic image ▪ Viewing malicious files within a live virtual environment can put the analysis system at risk of infection so use caution when applying this technique and where possible use an air-gapped network ▪ Ability to see how the malware and the infected system operate. Port scans and live process analysis are now possible ▪ It is possible to setup a controlled network connection to a dummy system and sniff the traffic between the two hosts
	▪ Ability to conduct full malware scan ▪ Viewing malicious files while mounted as local drive can put the analysis system at risk of infection so use caution when applying this technique

Incident Response & Forensics Solutions around People, Process, Technology



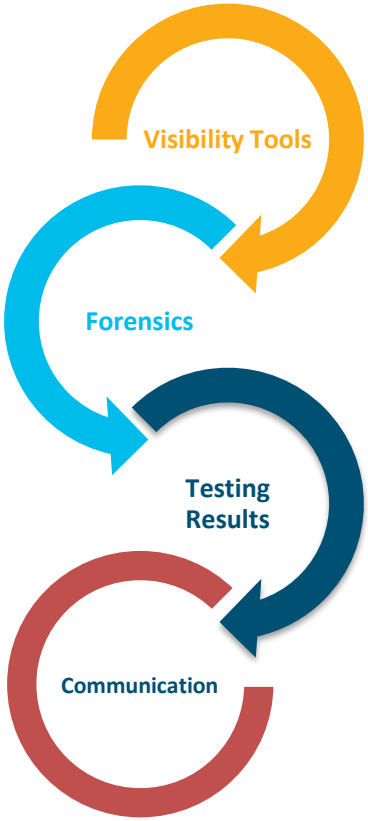
Our approach

Forensics

- Malware reverse engineering, memory forensics, and disk forensics performed on affected hosts

Communication

- Prescribed mechanism, rhythm, and audience for each level of incident severity



Deployed Visibility Tools

- Deployed Cyber Solutions into existing infrastructure to identify other potentially malicious traffic
- Deployed Endpoints solutions to facilitate endpoint, network analysis, and remediation

Testing Results

- App Pen Testing group conducted application hardening post-incident response

How can you prevented or minimized

Incident Response Plan

Communication and Collaboration

Test the IR Plan

We offer to our clients:

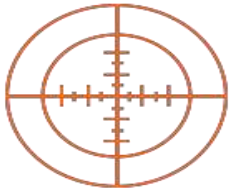
HUNT. DETECT. INVESTIGATE. RESPOND

Minutes

Accuracte

Incident

Delivery



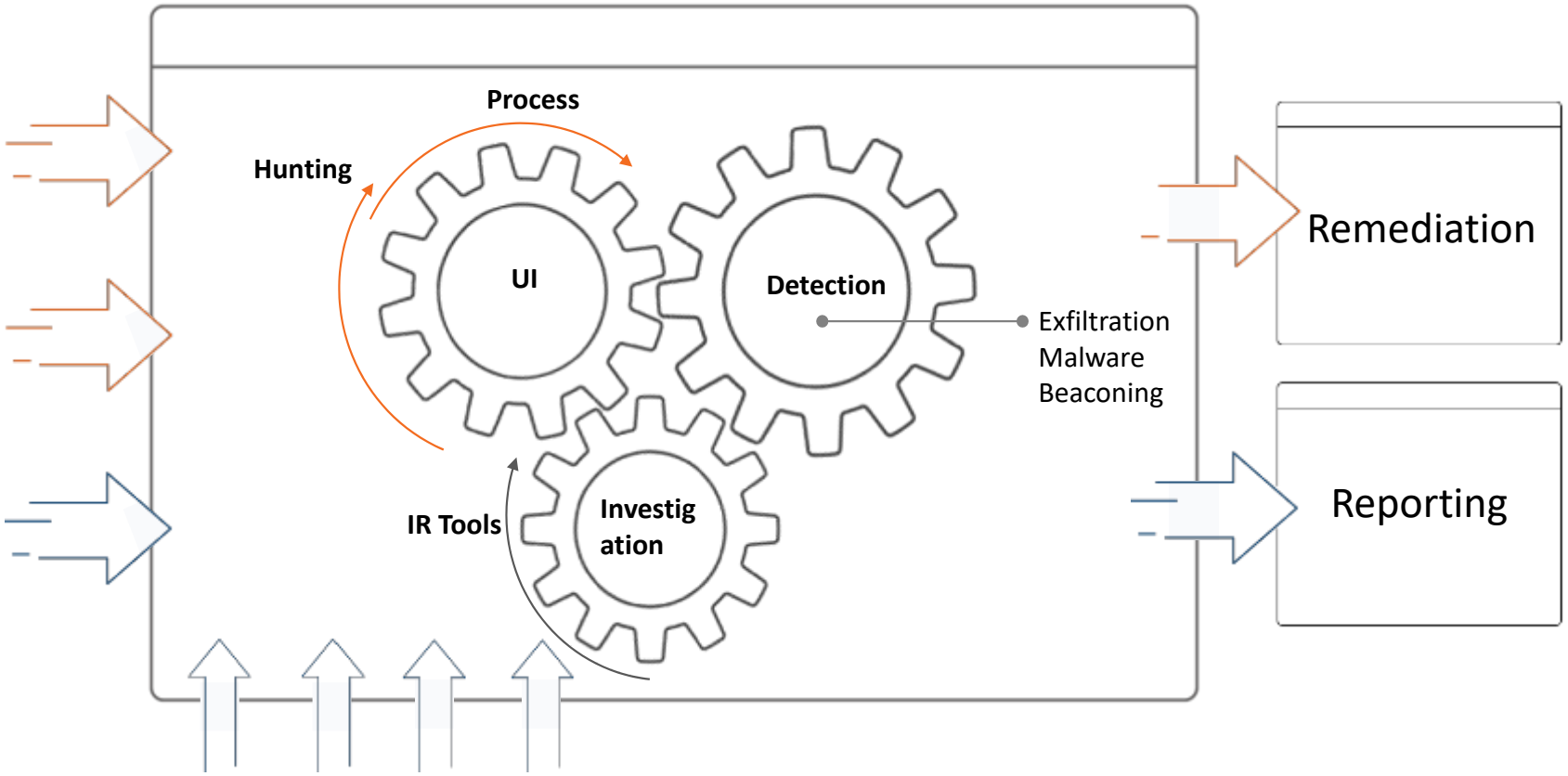
Threat Hunting

- Detecting unknown

Full-Scope Detection

Breach Response

Our Incident Respond Solution



Service Costs

- Any service is available as one-off service, frequent support or managed service.
- A one-off service is a one-time timely or object restricted effort to perform a specified activ
- Contracting, ordering and invoicing are done per one-off service.

Example:

Support a customer forensic analysis with reversing 1 specific malicious file.

Frequent Support

-

On discovery of a Security Incident:

1. a report is created and an investigation carried out to provide details of the attack mechanism
2. in addition to linking remediation advice all contained within the Service customer specific knowledgebase.
3. The security incident is prioritised and categorised according to a standard scheme and the resulting security incident report will be sent to client's CSIRT and CERT teams
4. Escalated in accordance with pre-agreed procedures dependent on its priority and category
5. We will provide skilled resources as well reverse engineering malware analysts.

DFIR Services

1. Digital Forensics
2. Incident Response
3. IT Investigations
4. Malware Analysis
5. Electronic Evidence Collection
6. Electronic Data Recovery & Destruction
7. DFIR-Training & Consulting