RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

# EITC Lessons Learned: Building Our Internal Security Intelligence Capability

SESSION ID: SEC-W08

Tamer El Refaey

Senior Director, Security Monitoring and Operations
Emirates Integrated Telecommunications Co. - UAE

#RSAC

# Quick introduction to EITC

# Why do need security intelligence?

Security threats have evolved drastically

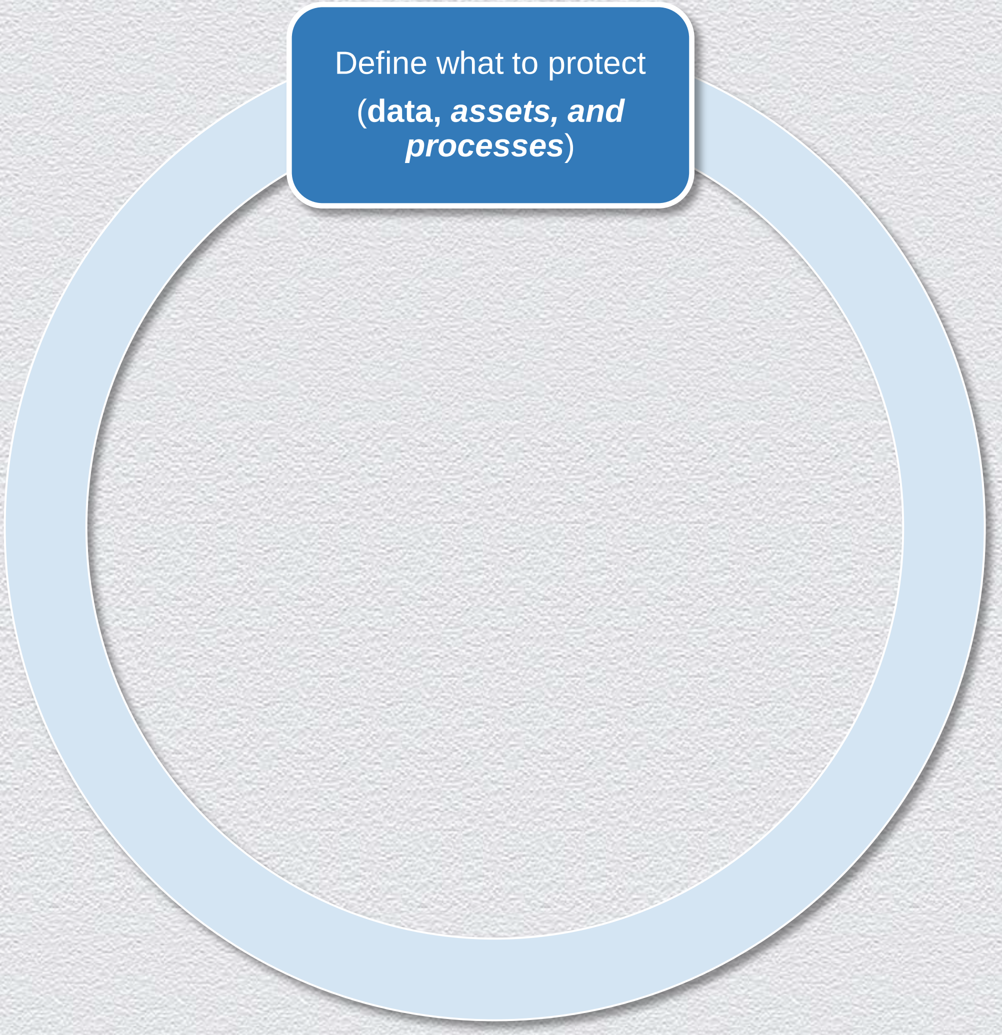
Prevention alone is no longer sufficient

Traditional detection capabilities are limited

Published statistics are disturbing

# EITC Approach

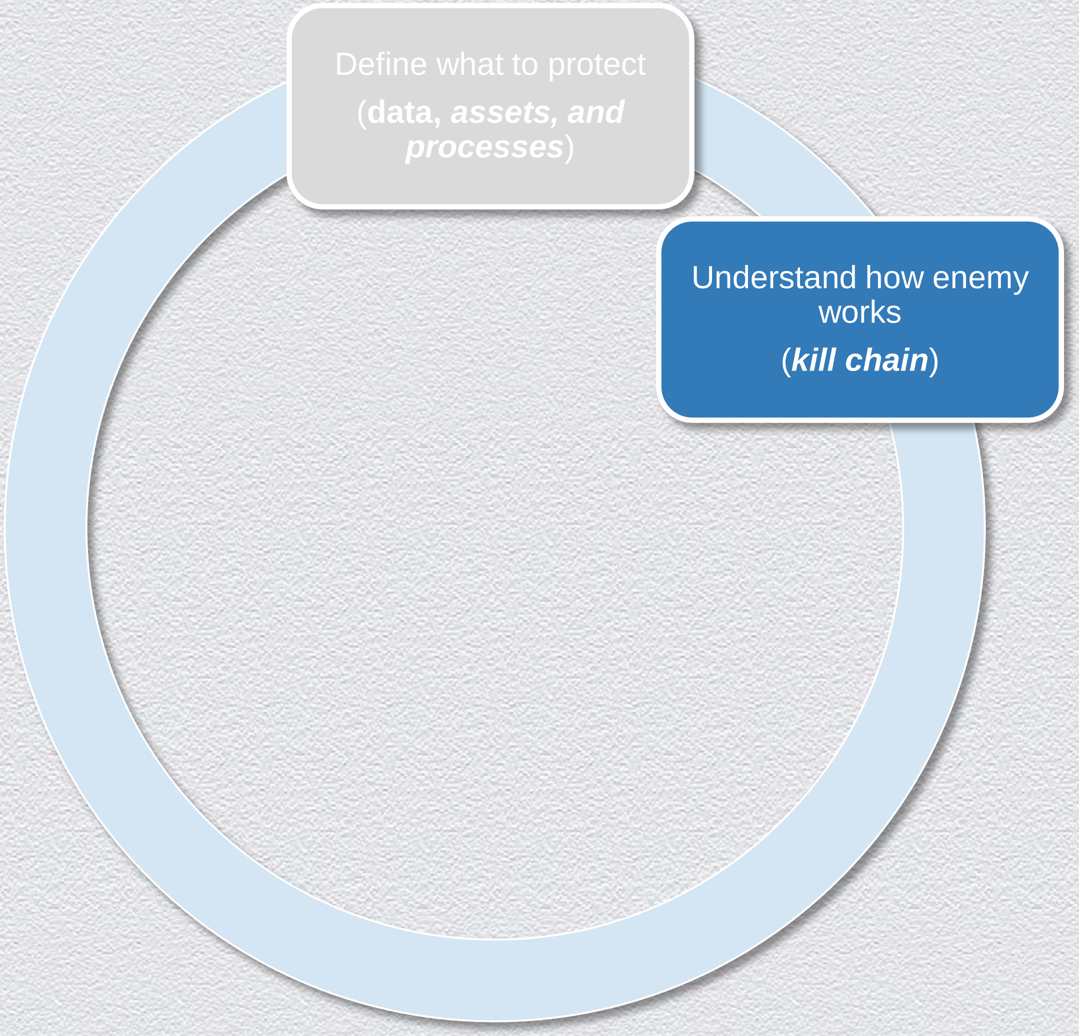
# Approach we used



Define what to protect

(**data**, ***assets*, *and processes***)

# Approach we used



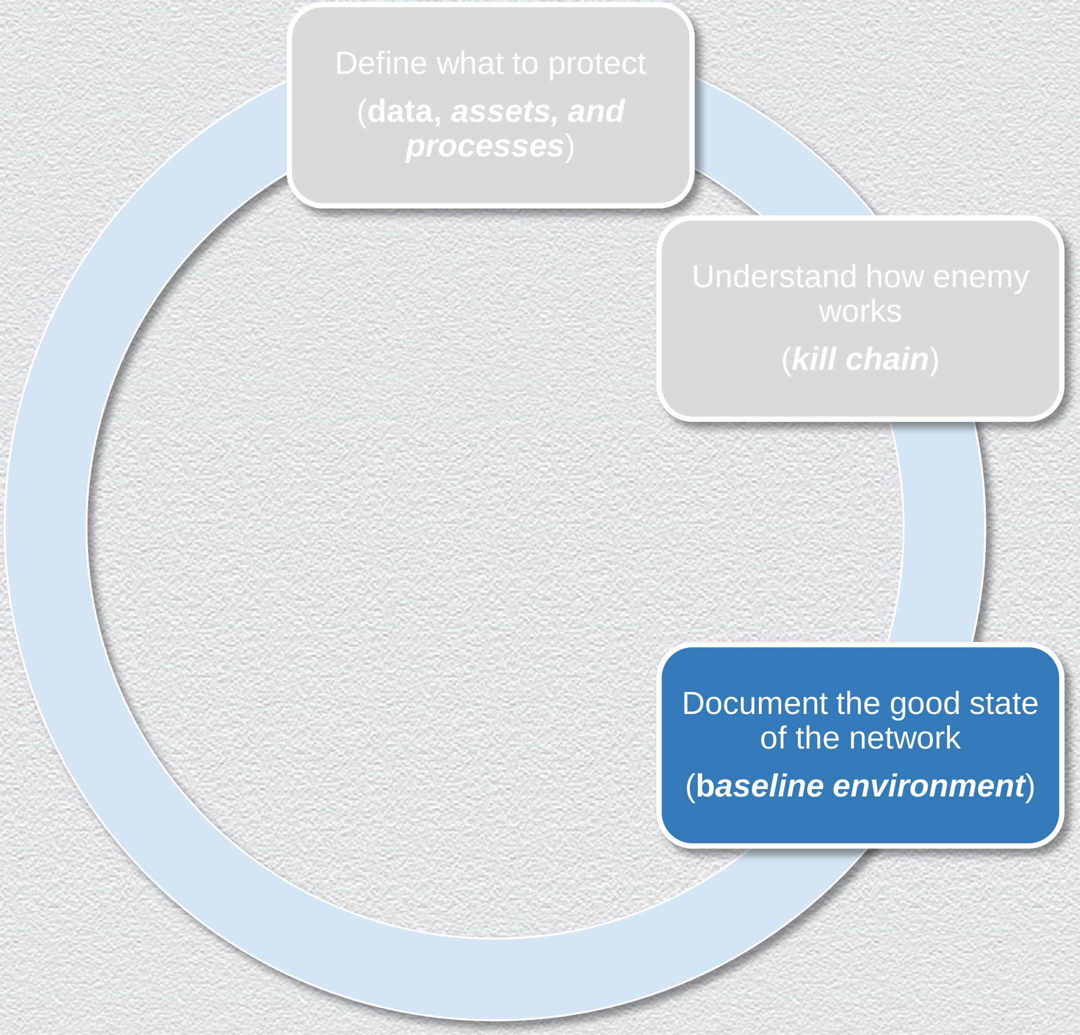
Define what to protect

(***data, assets, and processes***)

Understand how enemy works

(***kill chain***)

# Approach we used



Define what to protect

(***data, assets, and processes***)

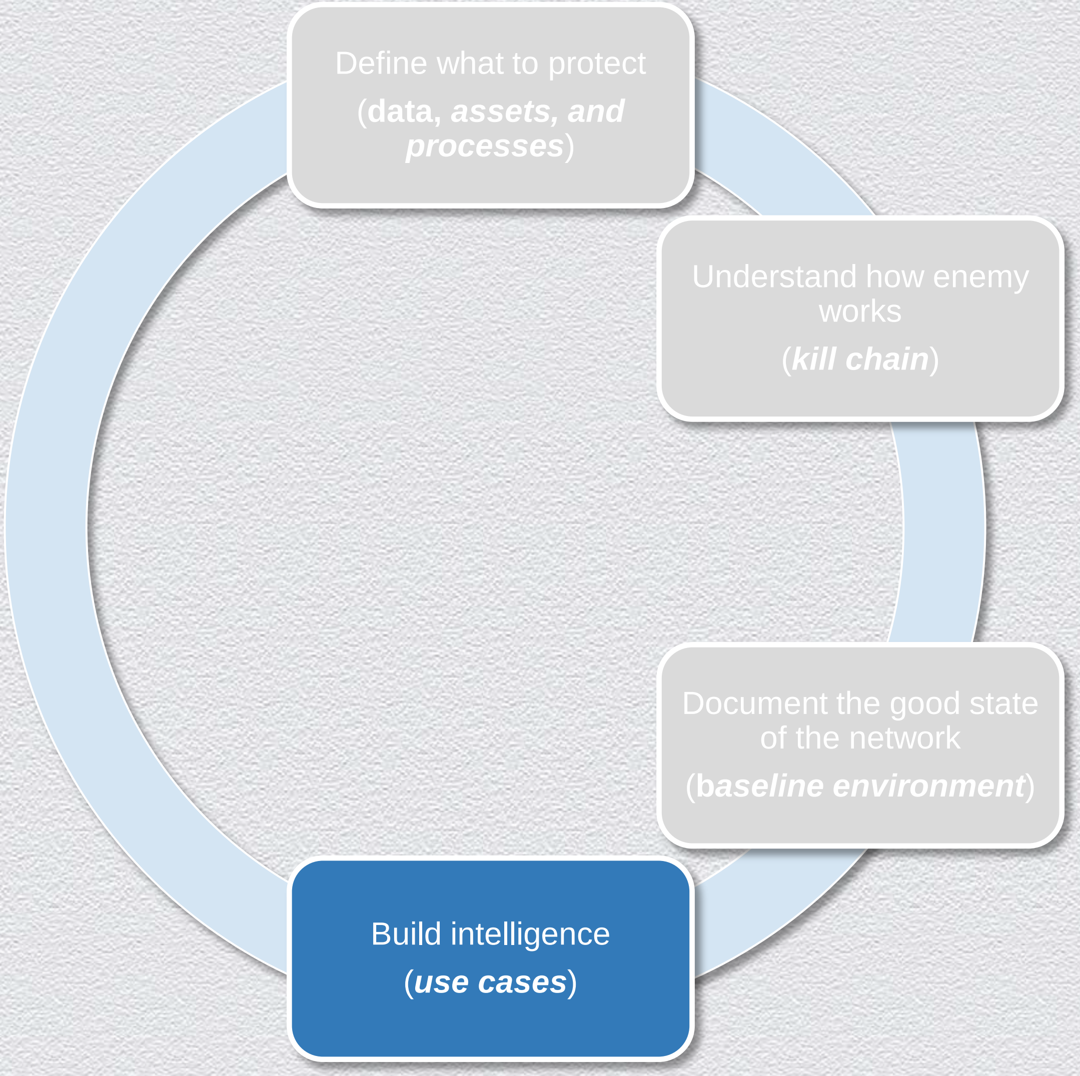
Understand how enemy works

(***kill chain***)

Document the good state of the network

(***baseline environment***)

# Approach we used



Define what to protect

(***data, assets, and processes***)

Understand how enemy works

(***kill chain***)

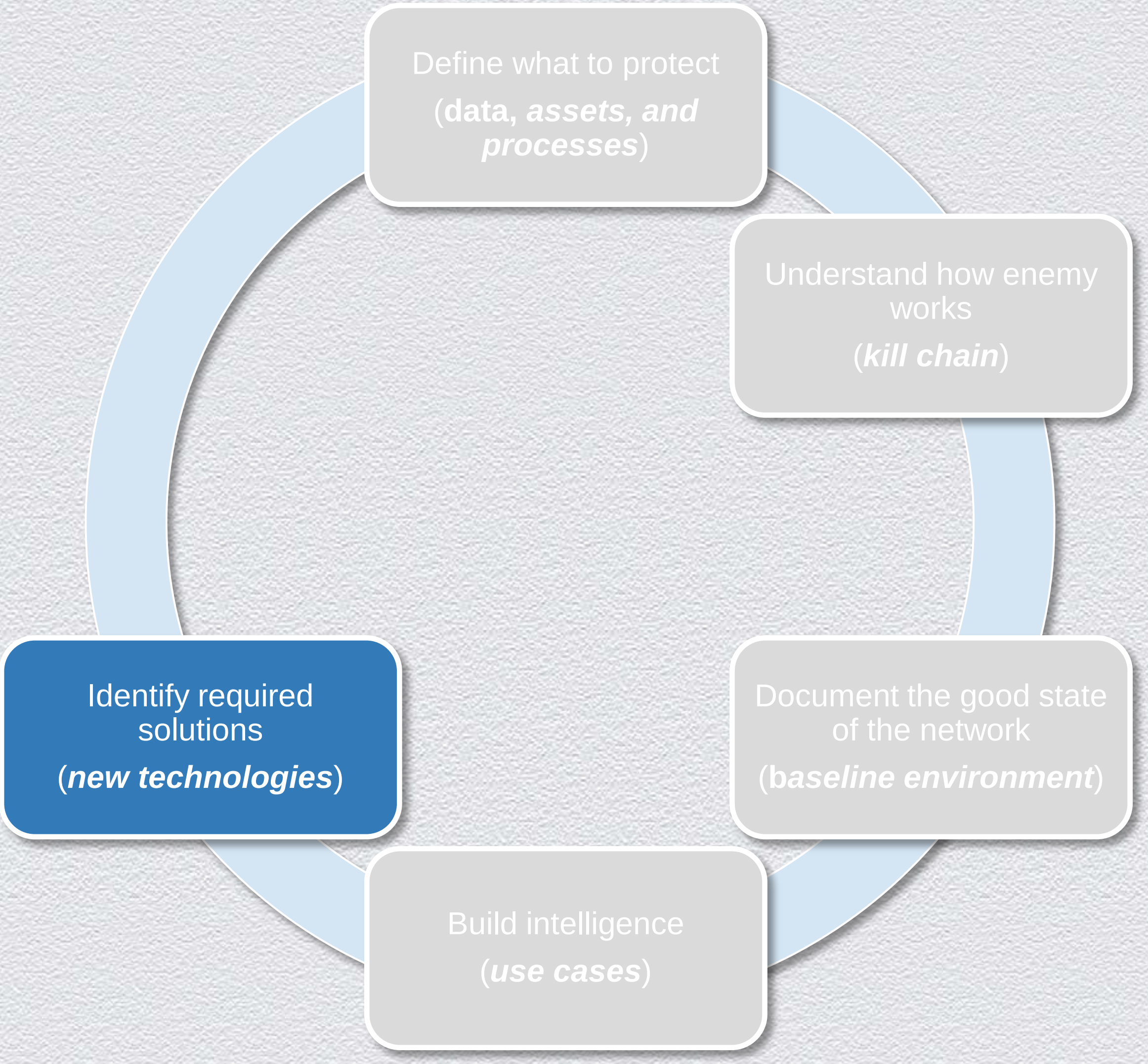
Document the good state of the network

(***baseline environment***)

Build intelligence

(***use cases***)

# Approach we used



Define what to protect

(***data, assets, and processes***)

Understand how enemy works

(***kill chain***)

Document the good state of the network

(***baseline environment***)

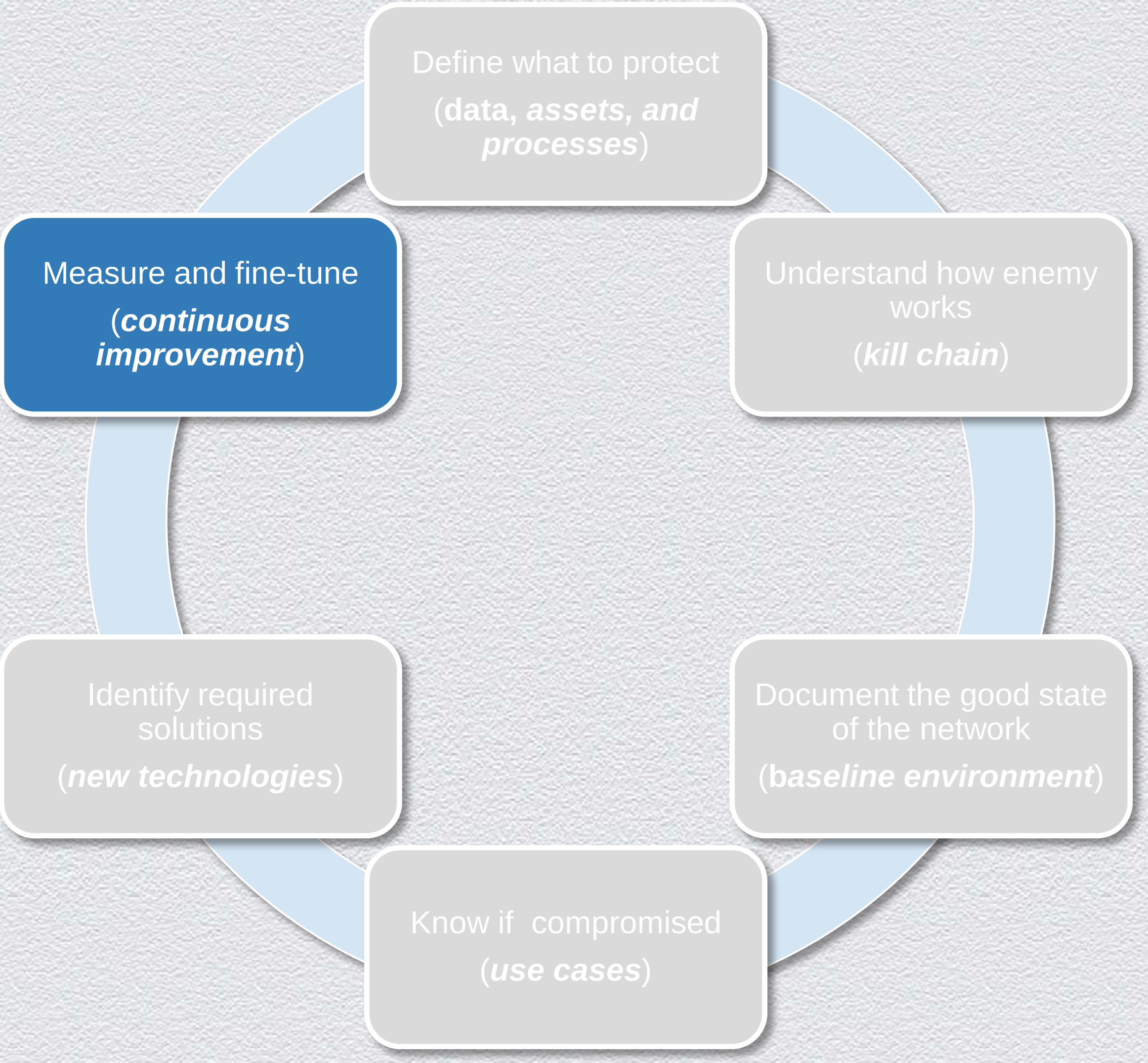
Build intelligence

(***use cases***)

Identify required solutions

(***new technologies***)

# Approach we used



Define what to protect

(***data, assets, and processes***)

Understand how enemy works

(***kill chain***)

Document the good state of the network

(***baseline environment***)

Know if compromised

(***use cases***)

Identify required solutions

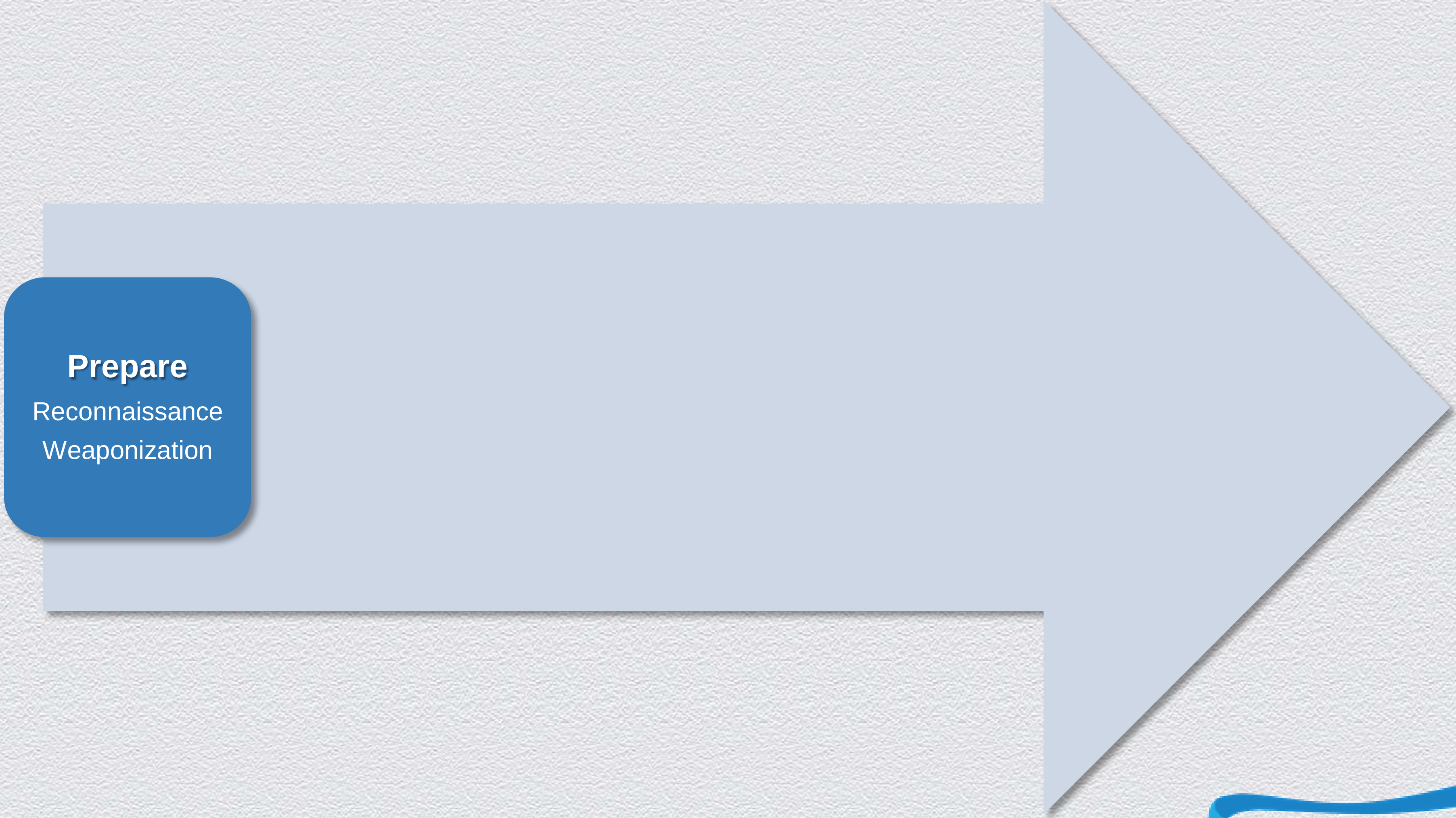
(***new technologies***)

Measure and fine-tune

(***continuous improvement***)

# Deeper dive into EITC security intelligence

# Understand how enemy works



**Prepare**

Reconnaissance

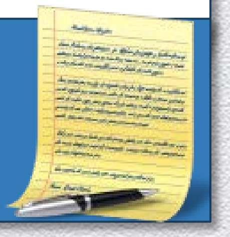
Weaponization

# Prepare: reconnaissance

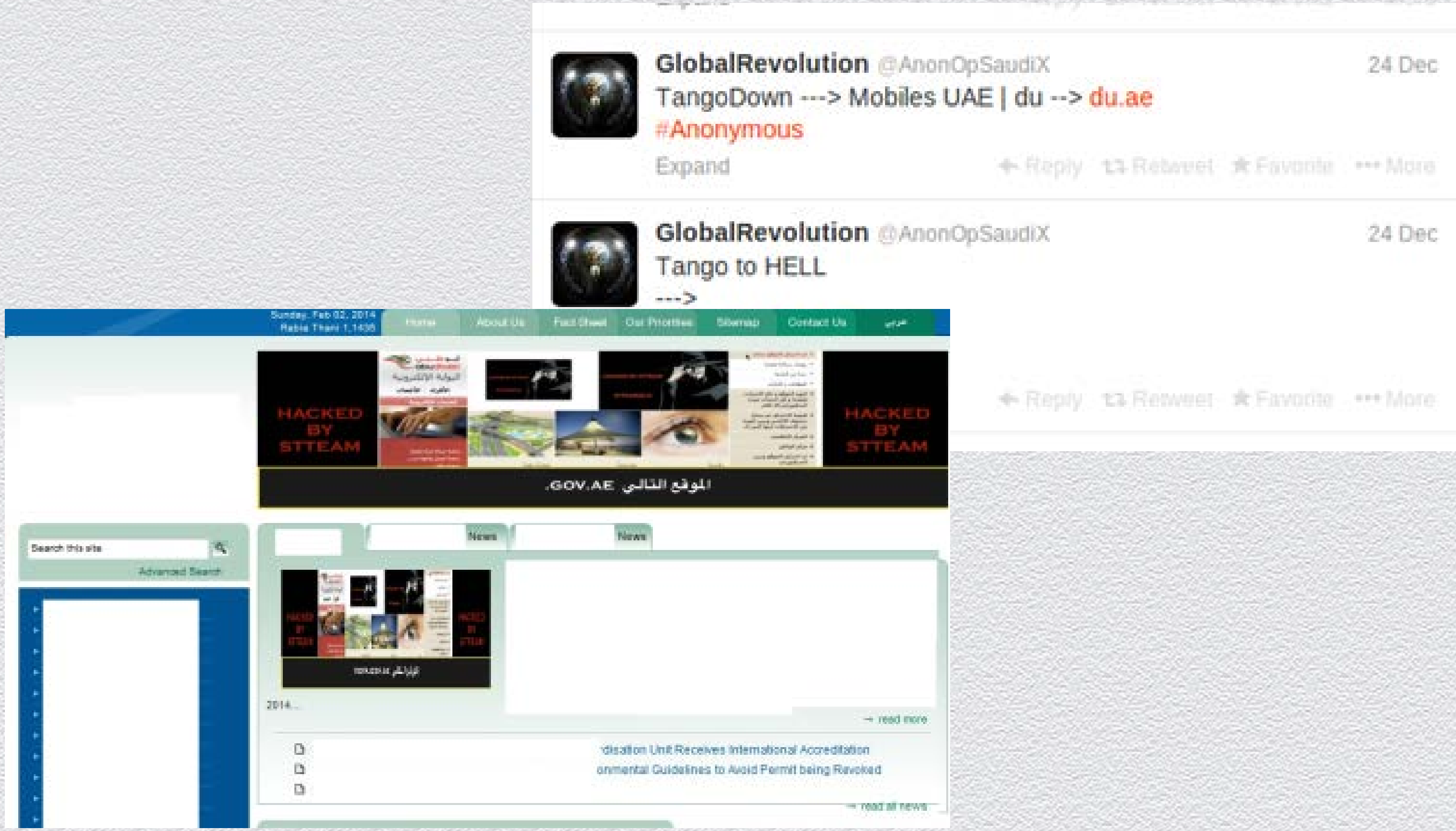
- ❑ Social network analysis
- ❑ Open source intelligence
- ❑ Watch lists

- ❑ Twitter, Pastebin, and Zone-h
- ❑ Google alerts
- ❑ Honeypots
- ❑ Denied traffic on firewall
- ❑ IPs and URLs from intelligence feeds
- ❑ TOR exit nodes
- ❑ Hiding proxies list
- ❑ Criminal ISPs feed

- ❑ Follow twitter accounts such as anonymous, OpPetrol, etc.
- ❑ Twitter search for keyword combinations related to EITC, du, UAE, etc.
- ❑ Pastebin and google alerts for keywords combination
- ❑ Hints posted on defaced websites (zone-h)
- ❑ Communications from suspicious IP addresses



# Prepare: reconnaissance



**GlobalRevolution** @AnonOpSaudiX · 24 Dec

TangoDown ---> Mobiles UAE | du --> du.ae #Anonymous

**GlobalRevolution** @AnonOpSaudiX · 24 Dec

Tango to HELL
--->

Sunday, Feb 02, 2014
Rabia Thani 1,1435

HACKED BY STTEAM

الموقع التالي .GOV.AE

2014...

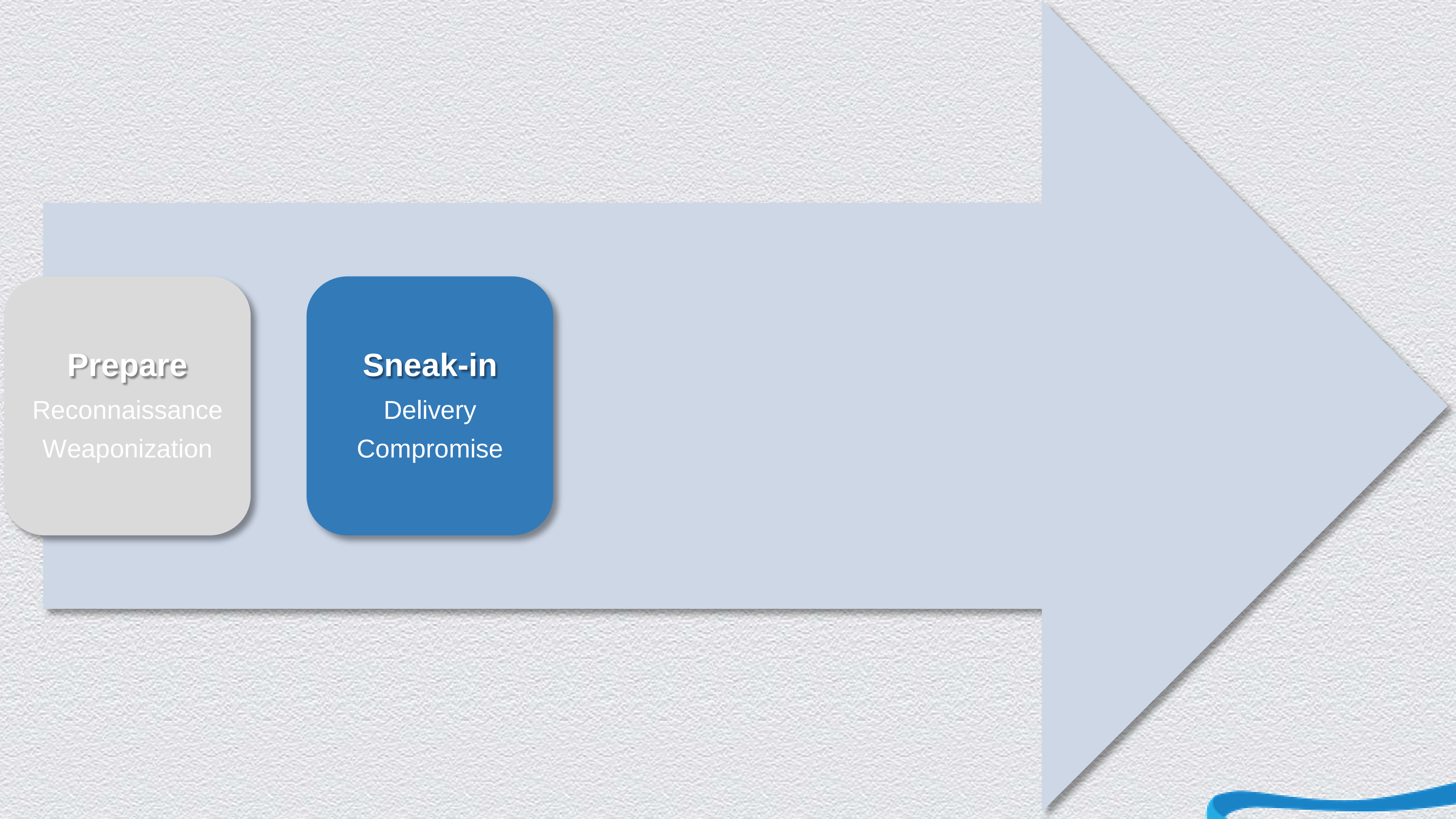
→ read more

- ·disation Unit Receives International Accreditation
- onmental Guidelines to Avoid Permit being Revoked

→ read all news

# Prepare: weaponization

# Understand how enemy works



**Prepare**

Reconnaissance

Weaponization

**Sneak-in**

Delivery

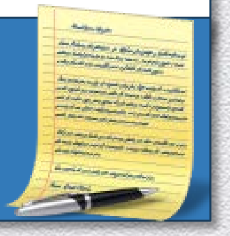
Compromise

# Sneak-in: delivery

- □ Watch lists
- □ E-mail header analysis
- □ Malware analysis

- □ Exchange message tracking
- □ In-house script to read e-mails coming from internet
- □ Network threat detection

- □ Combination of keywords in e-mails
- □ Binaries executed from removable device
- □ Malicious URLs access
- □ Suspicious e-mails sent to privileged and/or VIP users
- □ E-mails from IPs in our watch lists

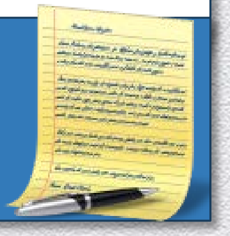


# Sneak-in: compromise

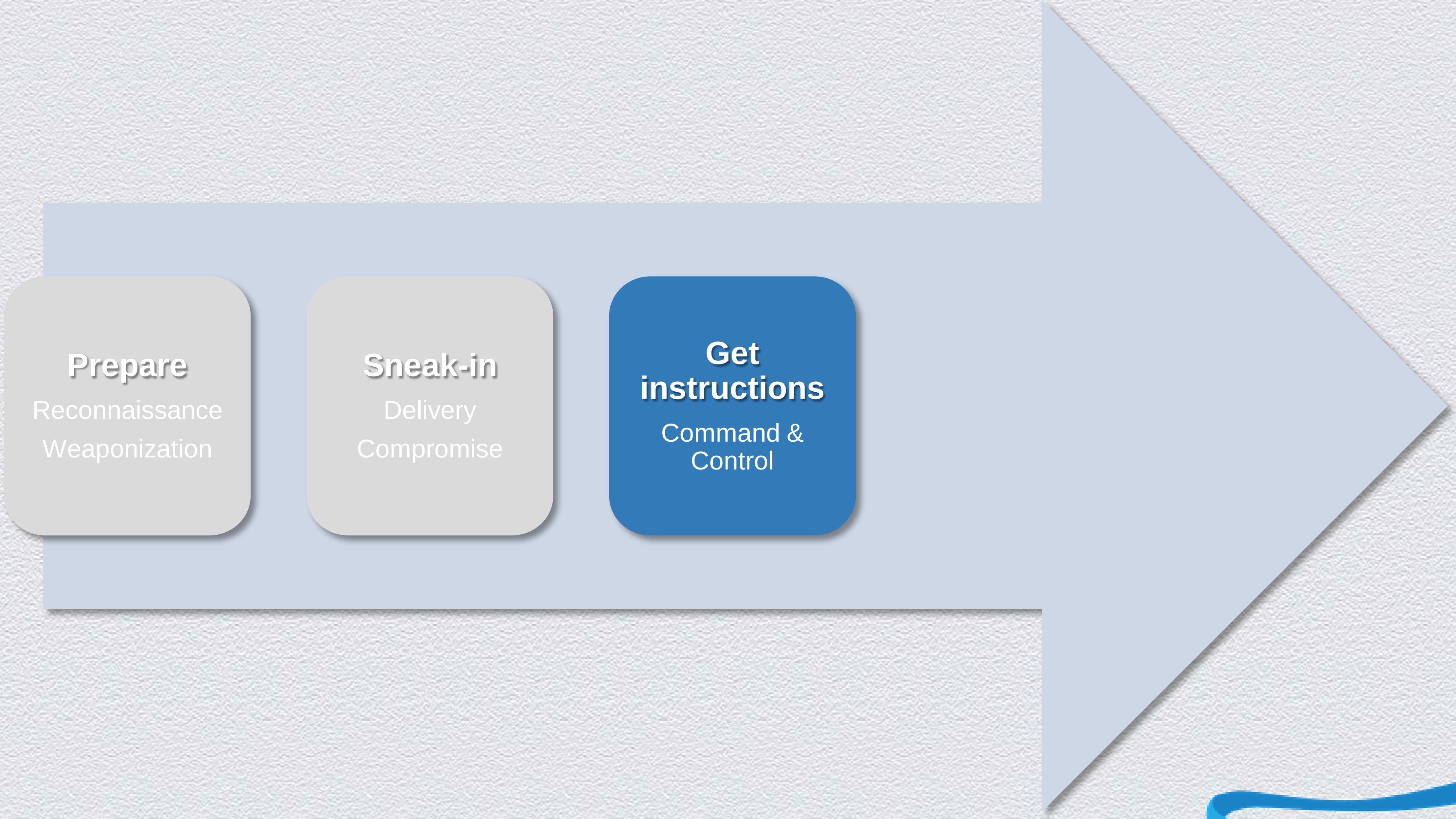
- □ Suspicious hash database
- □ Application whitelisting
- □ Environment base-lining
- □ User/system behavior analysis

- □ Endpoint advanced protection
- □ MWcrawler
- □ Honeypot
- □ Previous incidents
- □ Published IOCs
- □ Host based IDS
- □ Antivirus

- □ Non approved software
- □ Applications running from unusual paths
- □ Binaries in suspicious hash database
- □ Startup registry modifications
- □ Suspicious filenames and extensions
- □ Long file names > 30 characters
- □ Files with double extensions
- □ Files appear and disappear in short period



# Understand how enemy works



**Prepare**

Reconnaissance

Weaponization

**Sneak-in**

Delivery

Compromise

**Get instructions**

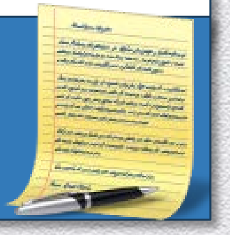
Command & Control

# Get instructions: Command and control

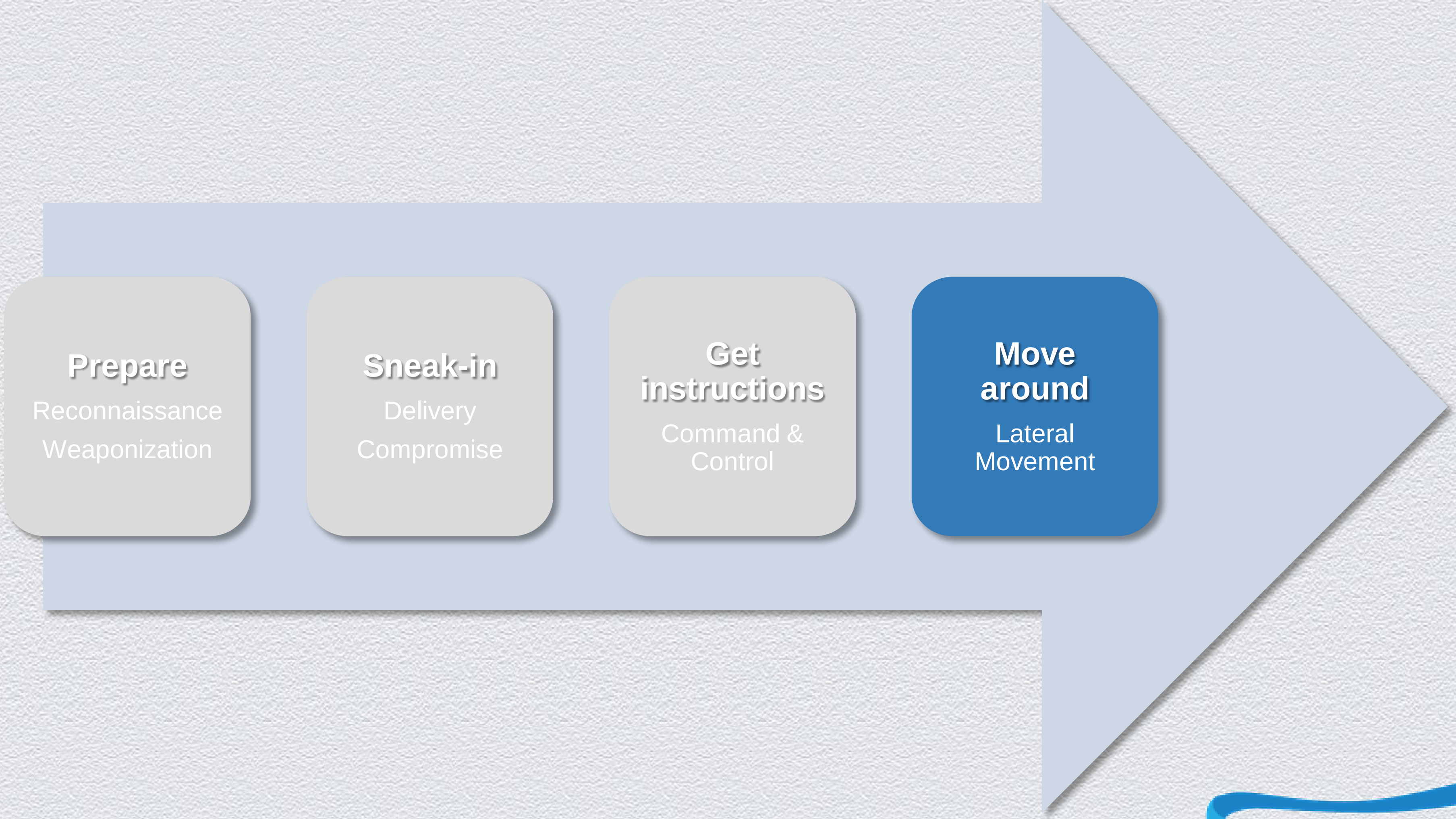
- ❑ Malware analysis
- ❑ Intelligence feeds
- ❑ Base-lining the environment
- ❑ Security analytics

- ❑ Endpoint advanced protection
- ❑ Sandbox
- ❑ Proxy logs
- ❑ DNS logs
- ❑ Firewall logs
- ❑ Free/commercial feeds

- ❑ Binaries attempting to access internet without proxy
- ❑ Call backs detected by Sandbox
- ❑ Communication using IPs not domains
- ❑ Access to known C&C servers
- ❑ DNS queries above average
- ❑ Domains accessed by few users
- ❑ High invalid domains queried by same host



# Understand how enemy works



**Prepare**
Reconnaissance
Weaponization

**Sneak-in**
Delivery
Compromise

**Get instructions**
Command & Control

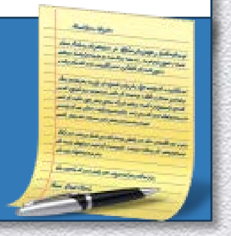
**Move around**
Lateral Movement

# Move around: lateral movement

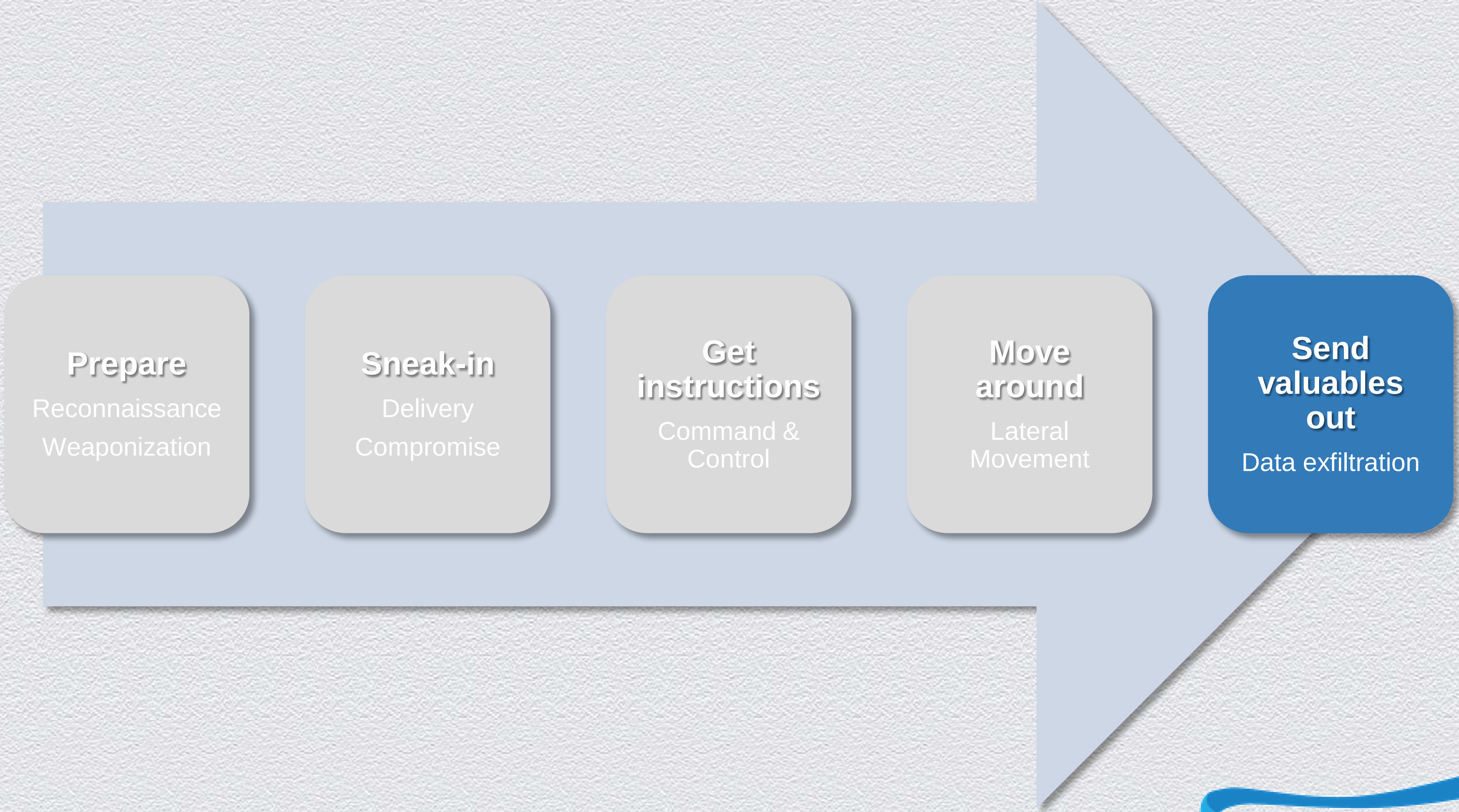
- □ Logical confinement
- □ User/system behavior analysis
- □ Environment base-lining
- □ Security analytics

- □ Endpoint advanced protection
- □ Host based IDS
- □ Antivirus
- □ Data leakage prevention
- □ Database activity monitoring
- □ Access control tools

- □ Admin accounts created on hosts
- □ Non-standard account names
- □ Simultaneous access from different locations
- □ Privileged access outside confined zones
- □ Database access by non-authorized tools
- □ Database errors
- □ Excessive file access
- □ Excessive data queries
- □ Execution of suspicious or uncommon commands



# Understand how enemy works

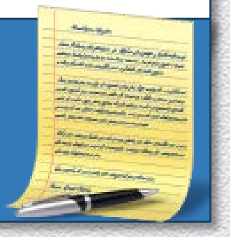


# Send valuables out: exfiltration

- □ Base-lining the environment
- □ Social network analysis
- □ Open source intelligence
- □ Security analytics

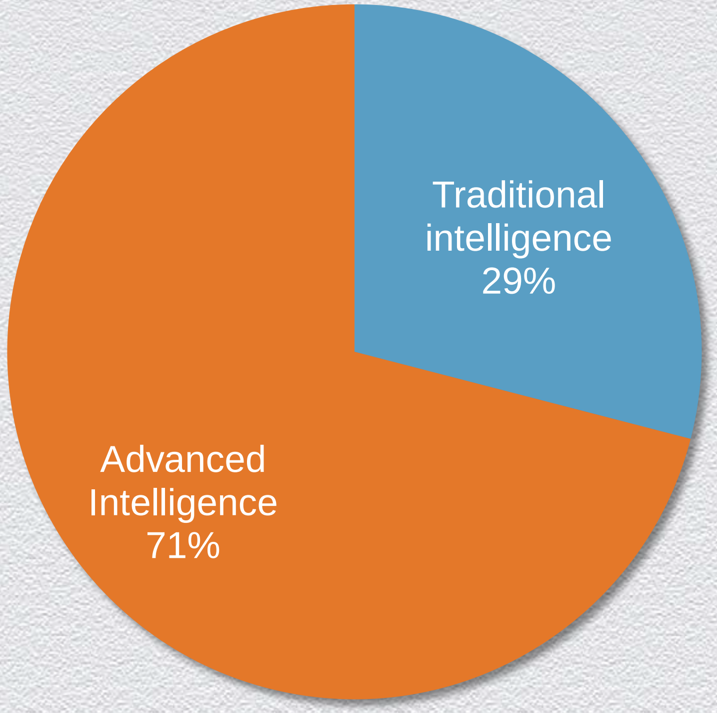
- □ Proxy logs
- □ Firewall logs
- □ DNS logs
- □ Twitter, Pastebin, and Zone-h
- □ Google alerts

- □ High internet uploads over HTTPS, FTP, etc.
- □ Access to suspicious countries
- □ Duration of internet connection > 30 minutes
- □ Communication over IP not domain names
- □ Large outbound e-mails
- □ Long internet session time
- □ Account details leaked on internet



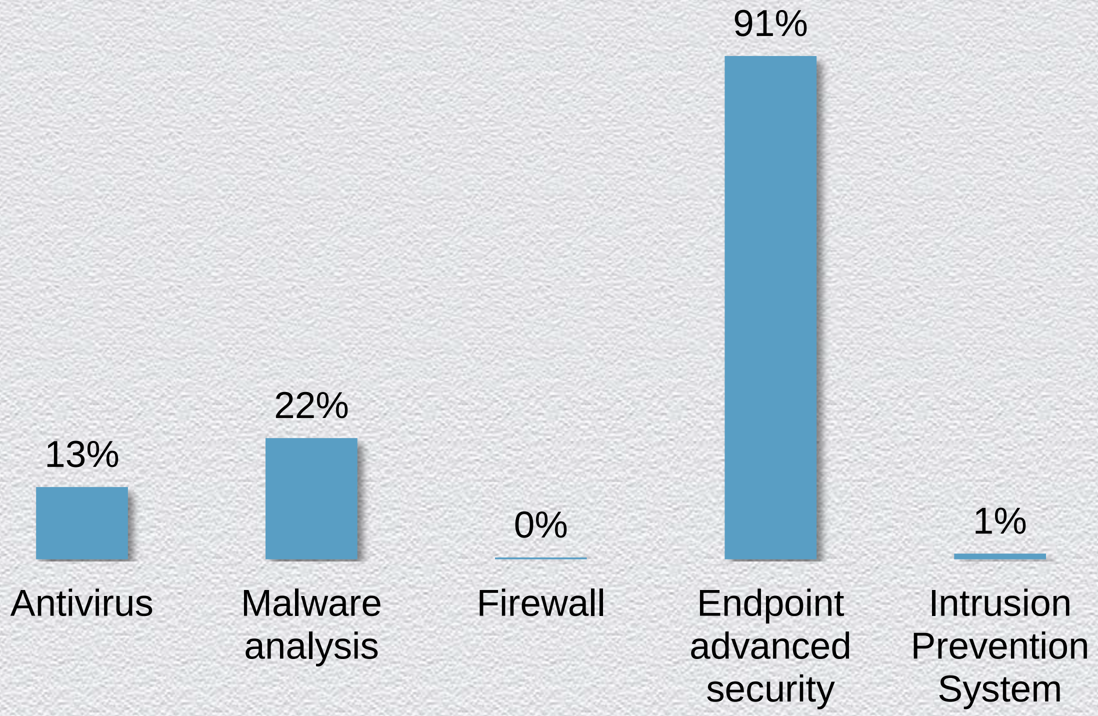
## How our KPIs got enhanced?

# Advanced Vs. traditional intelligence



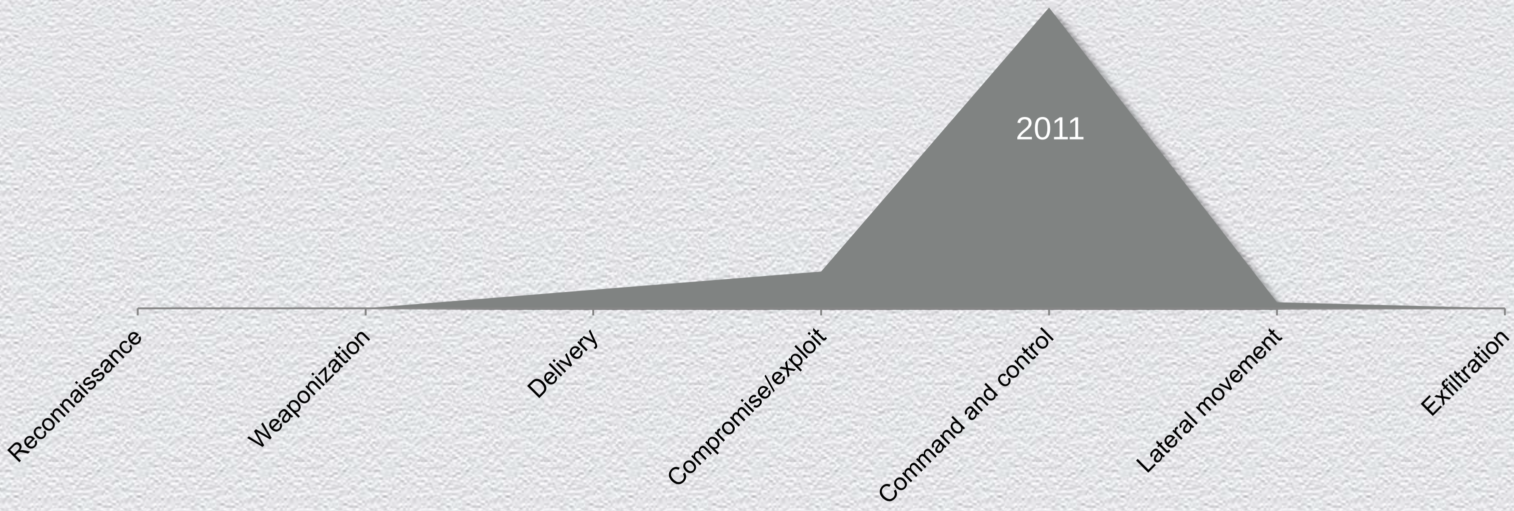
Contribution in incidents detection

# Technology efficiency (incident Vs Alerts)

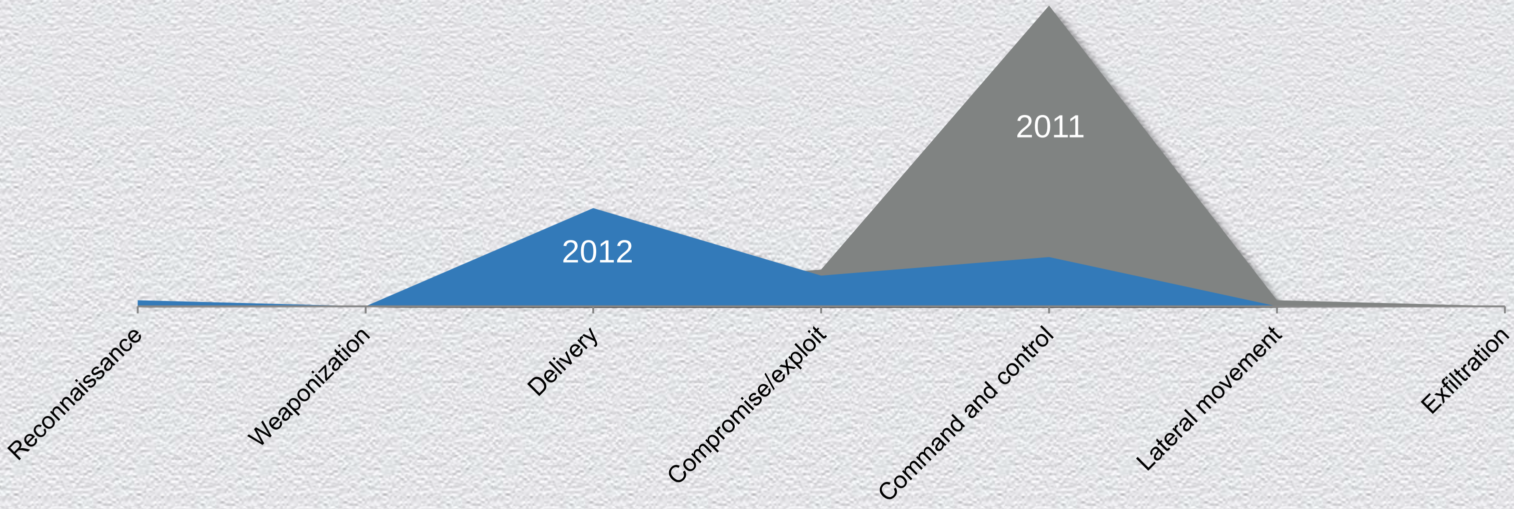


Alert Vs. incidents per technology

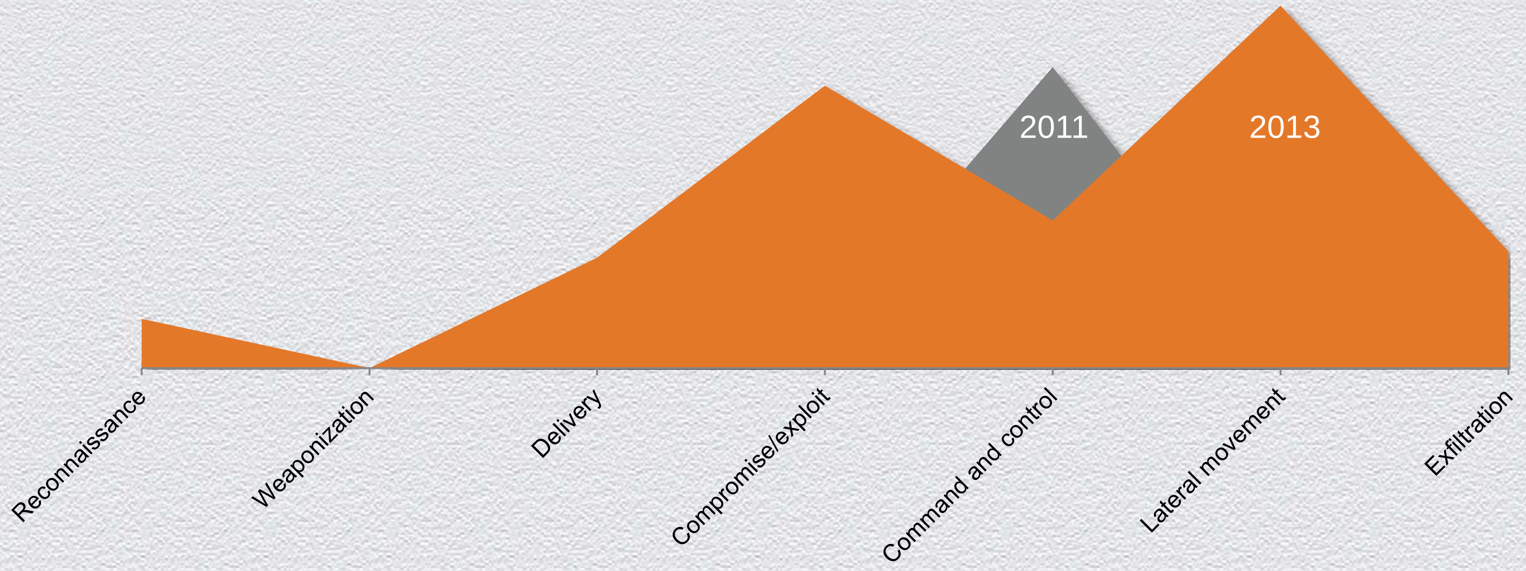
# Incident detection per kill chain phase



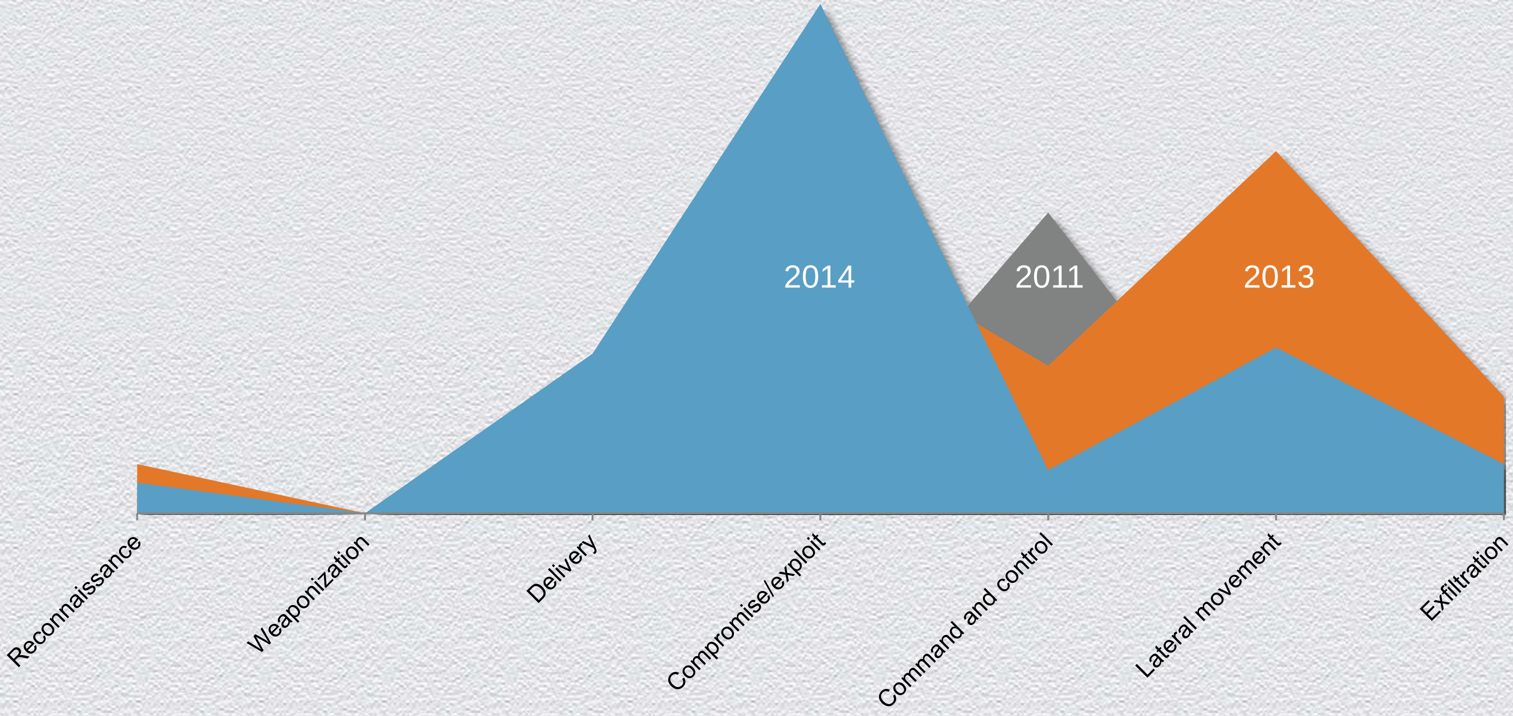
# Incident detection per kill chain phase



# Incident detection per kill chain phase



# Incident detection per kill chain phase



# Average time between compromise attempt and detection

**12.4** days average between compromise attempt and detection compared to **19.6** in 2013.

**82%** of compromise attempts are detected in less than **24** hrs.

# EITC now and then

**1,500** Log sources in 2014 compared to **1,300** in 2011.

**4,500** Analyzed EPS in 2014 compared to **3,000** in 2011.

**540** Intelligence use cases in 2014 compared to **72** in 2011.

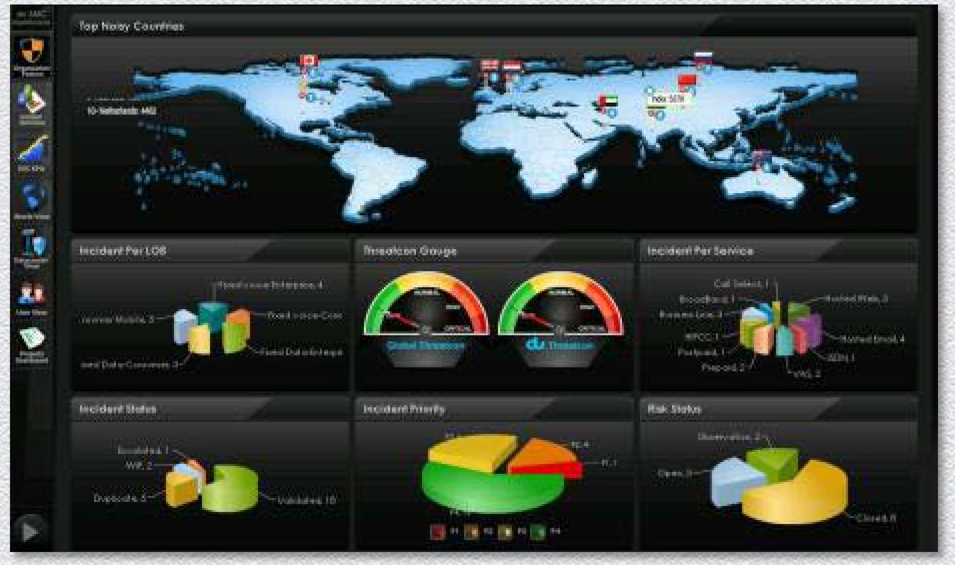
**1,000** Average monthly alerts in 2014 compared to **7,000** in 2011.

**25** Incidents for every 1,000 alerts in 2014 compared to **0.7** in 2011.

# Takeaways

- Our defenses need transformation.
- Detection and incident response became a must.
- Think like the bad guy when building security intelligence.
- Build layers of security intelligence.
- Unconventional threats require unconventional solutions.
- It is a long journey, so enjoy it.

# Video



EITC in-house developed security dashboard

# Your thoughts?