



A Walk in the Shadows

February 16, 2016

digital shadows_

Overview

- What is a digital shadow?
- What is cyber situational awareness?
- A walk in the shadows
- Q&A

What is a digital shadow?



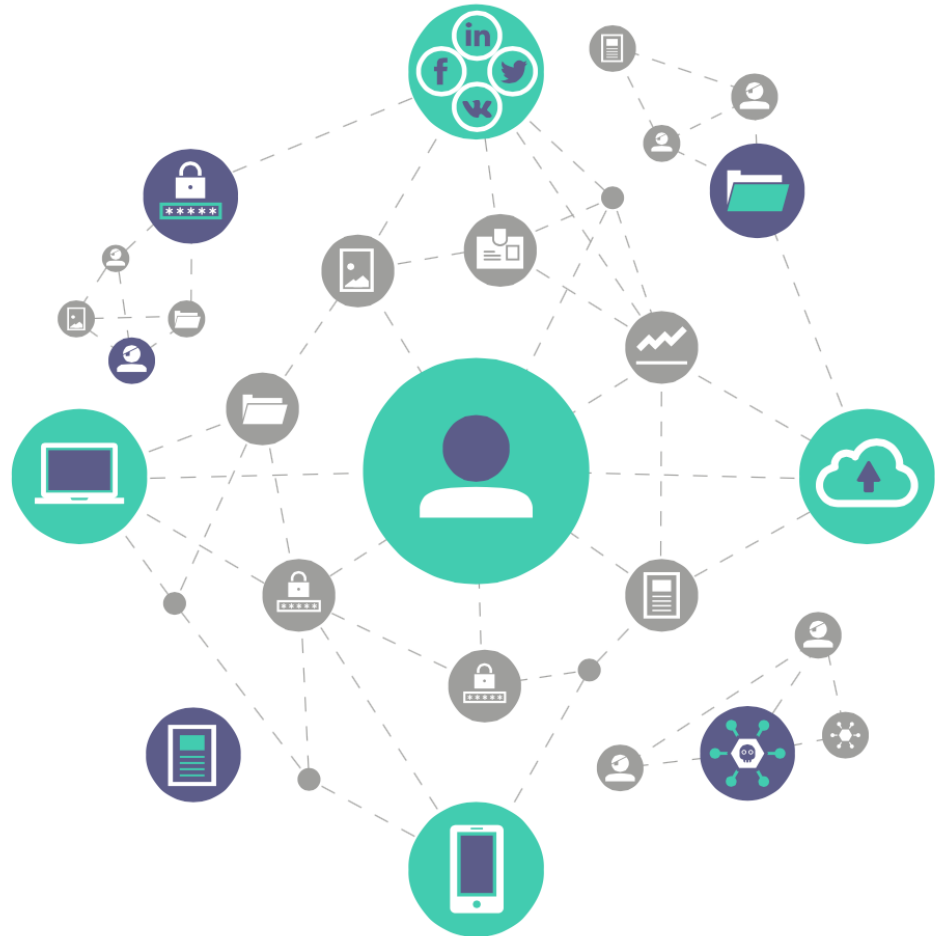
Digital Footprint

As an organization's employees, suppliers and partners transact and socialize online, they leave behind an electronic trail of their activities.



Digital Shadow

Exposed personal, technical or organizational information that is often highly confidential, sensitive or proprietary



The adversary has its own shadow

- Patterns and motives
- Attack vectors of choice
- Dark web activities
- Abuse of brands



Cyber situational awareness



Extensive Coverage



Tailored Intelligence



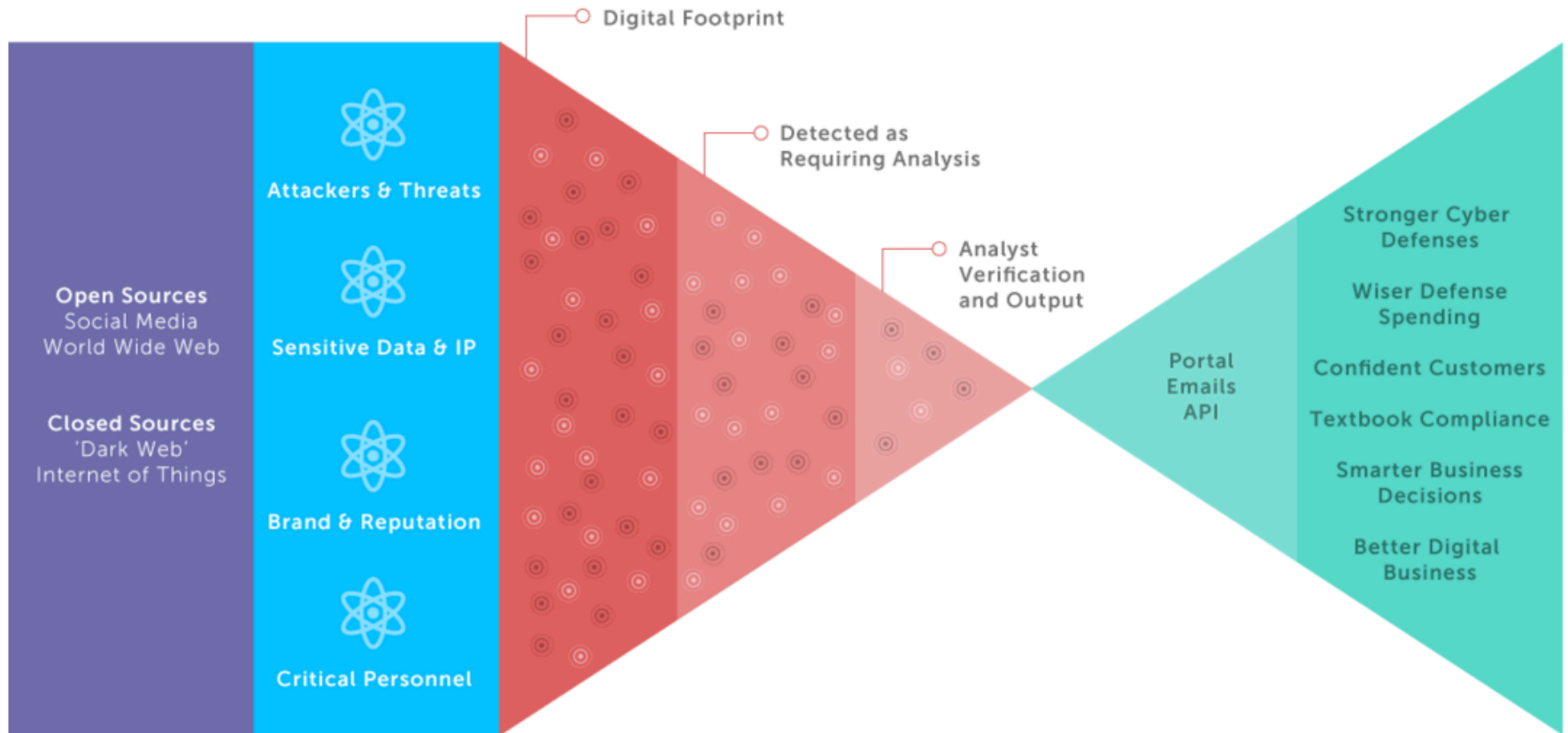
Frictionless Deployment



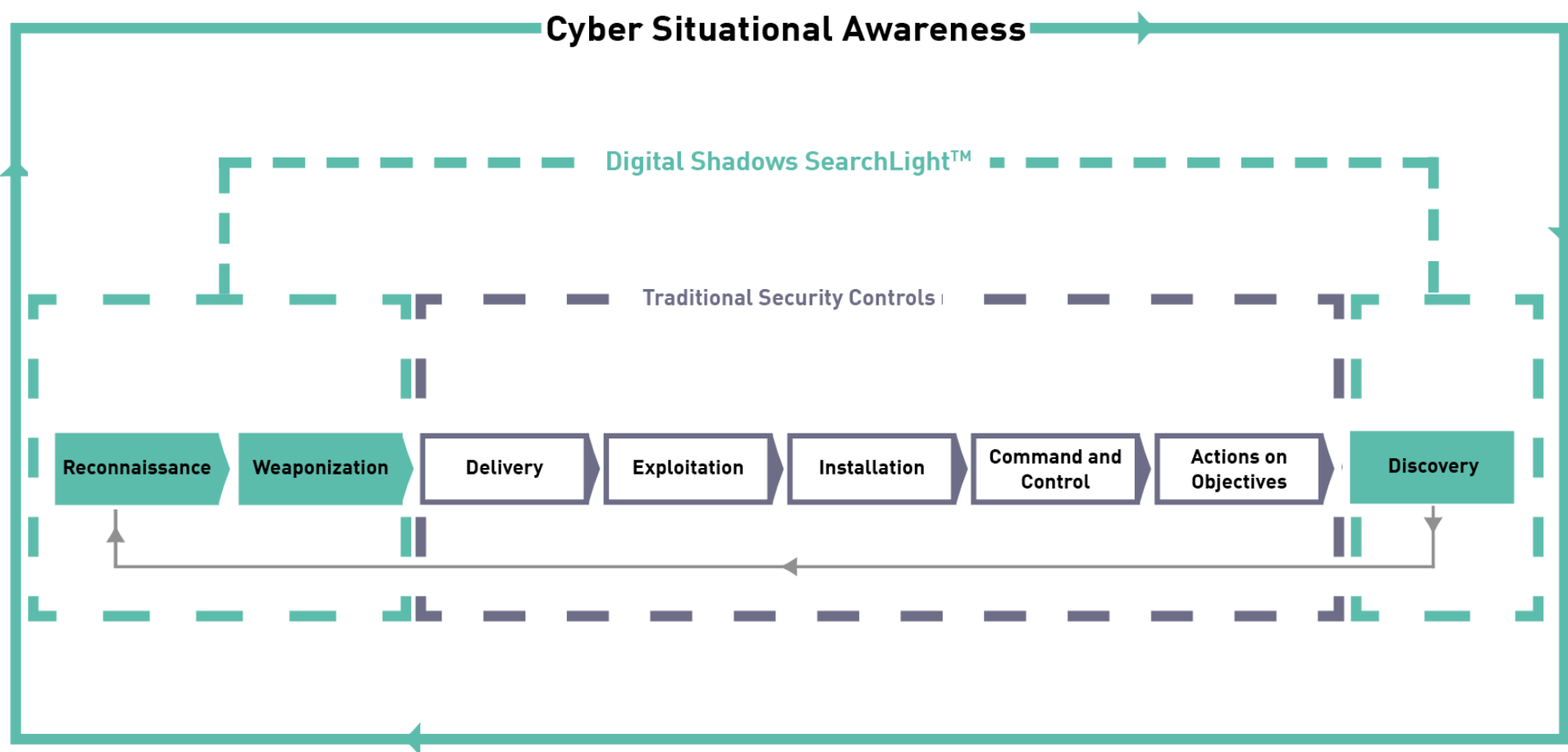
Timely Alerts



Situational Awareness



Cyber situational awareness and the kill chain





A Walk in the Shadows

Social Media – Over sharing

Background



Summary

My primary interests are in mainframe applications and cyber **security**. I try to stay up-to-date in both and learn as many new things as I can.



Experience

Security Engineering & Architecture

United States Steel Corporation

May 2013 – Present (2 years 7 months) | Greater Pittsburgh Area

I work with a multinational team to handle **security** issues for the entire corporation. Systems include Splunk, a Checkpoint Firewall, a McAfee Web Proxy, and HP Service Manager for ticket requests.

▶ 1 project

Code-Sharing – Over sharing

The screenshot shows the GitHub interface for the repository 'aku246 / POC'. The breadcrumb path is 'POC / Development / Code / tibco / TDA / Generic / Config / +'. The latest commit is by 'aku246' on May 22, 2017, with commit ID 2170289. The commit message is 'Updated GV configuration, Timer Interval and mapping, Read File location'. Below the commit, a table lists the files changed in this commit and other recent commits.

File	Commit Message	Time Ago
..		
Dev_NOR-TDAUtilityServices.xml	US19903 Config file for DEV- Qa Utility Service Modified for Nordic...	a year ago
Dev_POL-TDAUtilityServices.xml	updated Redis config details and value of GV CommonConfig/JMSDynamicP...	11 months ago
Dev_TDACreatorGateway.xml	US20205 Creator Gateway Removed double entries for certificate GV's	a year ago
Dev_TDAExcursionAPI.xml	excursion code change and config file update	10 months ago
Dev_TDAWeatherAPI.xml	Updated all dev config for the Generic, Nordic and Poland Region appl...	a year ago
Dev_TDA_MonitoringUtility.xml	Updated GV configuration, Timer Interval and mapping, Read File location	6 months ago
PREPROD_NOR-TDAUtilityServic...	- Preprod and Prod Config Files checked in	11 months ago
PREPROD_TDACreatorGateway.xml	- Preprod and Prod Config Files checked in	11 months ago
PREPROD_TDA_ExcursionAPI.xml	- Preprod and Prod Config Files checked in	11 months ago
PREPROD_TDA_MonitoringUtility...	- Preprod and Prod Config Files checked in	11 months ago
PROD_NOR-TDAUtilityServices.xml	- Preprod and Prod Config Files checked in	11 months ago
PROD_TDACreatorGateway.xml	- Preprod and Prod Config Files checked in	11 months ago
PROD_TDA_ExcursionAPI.xml	- Preprod and Prod Config Files checked in	11 months ago

Code-Sharing – Over sharing

```
<NameValuePairPassword>  
  <name>Connection/JDBC/Password</name>  
  <value>#!xJVQ7krVJERtGuG/E43nc47oNn3WHRY1wjbwJupBLOceae5f98ZV2A==</value>  
</NameValuePairPassword>
```

```
<binding name="CacheManager">  
  <machine>delvmp11tui27.sapient.com</machine>  
  <product>  
    <type>BW</type>
```



Exploiting the Shadows

Hacktivists



Anonymous Long Eaton UK

12 August at 23:48 · Edited ·

Like Page

Anonymous World Legion Council
#OpHitTheBanks is coming!
#BlackHats #WhiteHats #GreyHats #Hackers #Ddos #Activists #Anonymous
#Anons #Bankers
Calling all Black, Grey and White Hat Hackers..
We will be organizing a protest and march at the Major Banks that are
controlling the debt, interest and slavery of our world.



GlobalRevolution

@AnonOpSaudiX2



Follow

#ResistCapitalism #MoveYourMoney
#Occupy
#UAE FIRST GULF BANK<#TangoDown>
fgb.ae

#Anonymous #OpUAE
status.ws/sites/www.fgb. ...

RETWEETS 5 FAVOURITE 1



2:22 a.m. - 17 May 2015



GlobalRevolution

@AnonOpSaudiX2



Follow

#الانونيموس
تعطيل بنوك #السعودية
بنك الراجحي

#TangoDOWN -->
alrajhibank.com.sa

status.ws/sites/www.alra ...

#OpSaudi
#OpArabia

View translation

RETWEETS 3 FAVOURITE 1



12:11 p.m. - 27 Aug 2015

Cyber criminals and the Dark Web

- Loyalty card company data sold
- UK retail bank employee selling customer data

yeah, got bulk hacked [REDACTED] account bro with various point.
you can exchange point with [REDACTED] giftcards

then you just need hacked UK [REDACTED] and linked with giftcard, you
can card all stuff on ebay.

btw,
I've a lot email:pass, which country you need bro?

If you interest I'll create costum listing for you.

price [REDACTED] I take 30% from balance
email : pass depend country, UK 10\$/ 1k , usa 7\$/ 1k

sorry my bad english

thanks,

HACKED ACCOUNT DEALER MARKETPLACE:
<http://k5zq47j6wd3wdvjq.onion/>
DETAIL & PRICE: <http://i25c62nvu4cgeqyz.onion/>

What I can provide:

1. Customer's Name
2. Phone numbers
3. Date of Birth
4. Address
5. Account numbers along with sort codes
6. Account balances
7. Security ID they use for phone banking (you'll be asked to confirm a couple of random letters from this when you're on the phone with customer service)
8. Debit Card number
9. Debit card expiry date
10. If someone has scammed you from the UK or you just want info on someone before you go into business with them in the UK, I can look it up and if they bank with my bank, I will provide it to you. For this, all I need is their bank account and sort code and I'll tell you if I can get it before charging you anything.

All of this is easily enough for an account takeover or maybe even calling up customer service and transferring money from one account to another (you need the security ID which I provide).

Thank you for listening. Any questions?

Chris.brown@digitalshadows.com

07809781056

London

Level 39, One Canada Square, London, E14 5AB

 +44 (0)203 393 7001  enquiries@digitalshadows.com

San Francisco

535 Mission St, Fl. 14, San Francisco, CA 94105

 +1 888 8894143