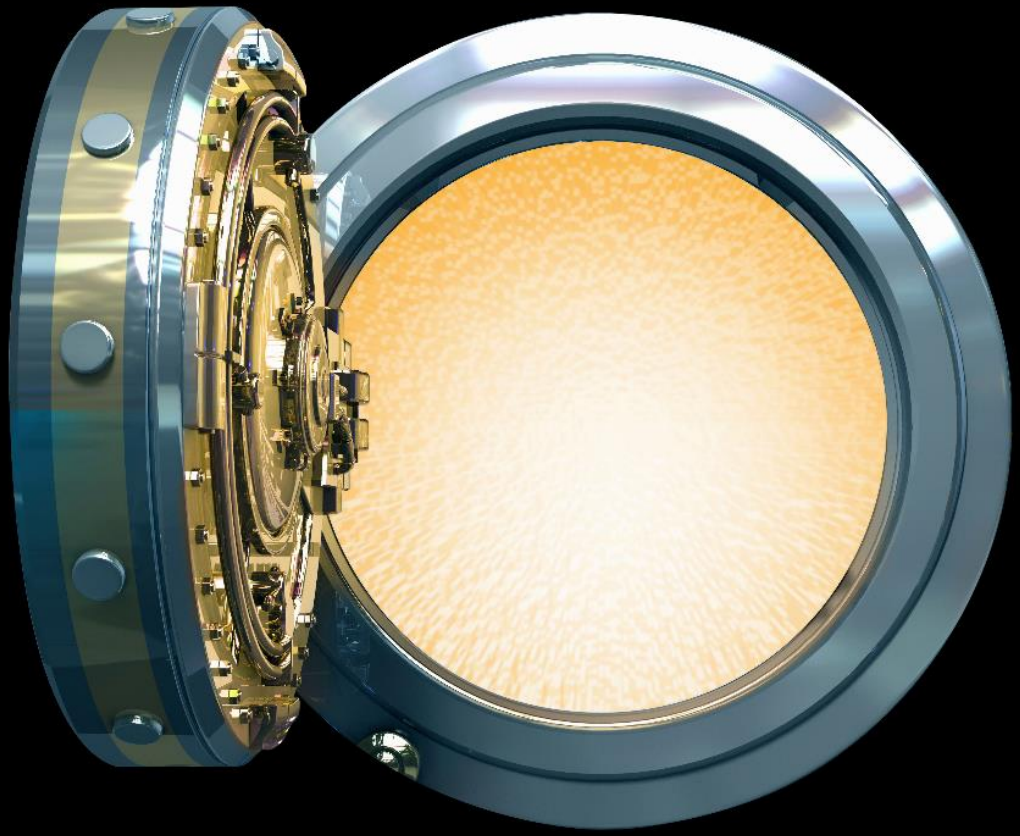
Deloitte.



Fraud Awareness Seminar

From Princes to MuddyWater

Presenters

Lucas Chiloane

- Senior Manager – Risk Advisory
- Cyber Forensics

Emmanuel Adigun

- Senior Manager – Risk Advisory
- Vulnerability Management (Ethical hacking)

What is Cyber Crime

Cyber crime

Cyber crime – A crime or other offence committed through the use of the Internet aided by electronic communications/systems and/or devices. It is any criminal activity involving computers and networks.

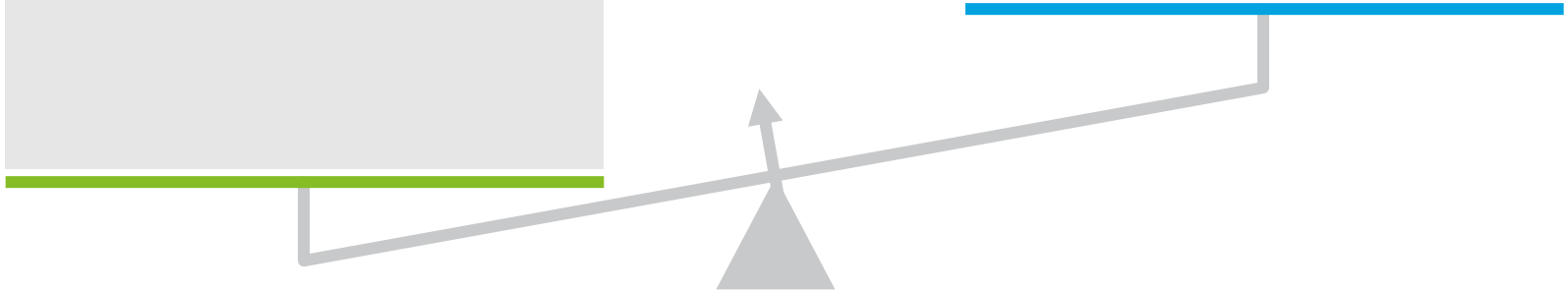
Traditional Criminal Vs. Cybercriminal

Traditional Criminal

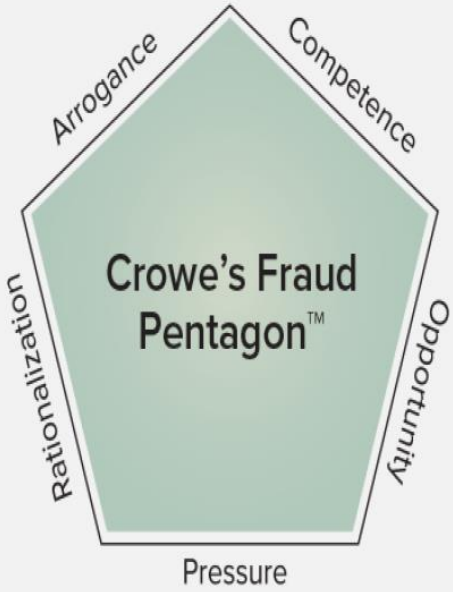
- Somewhat predictable
- Bound to specific location
- Paper trail
- Set motive
- ID

Cybercriminal

- Could be anywhere
- No profile
- Bits and Bytes
- Unpredictable
- Volatile
- IP
- Open source



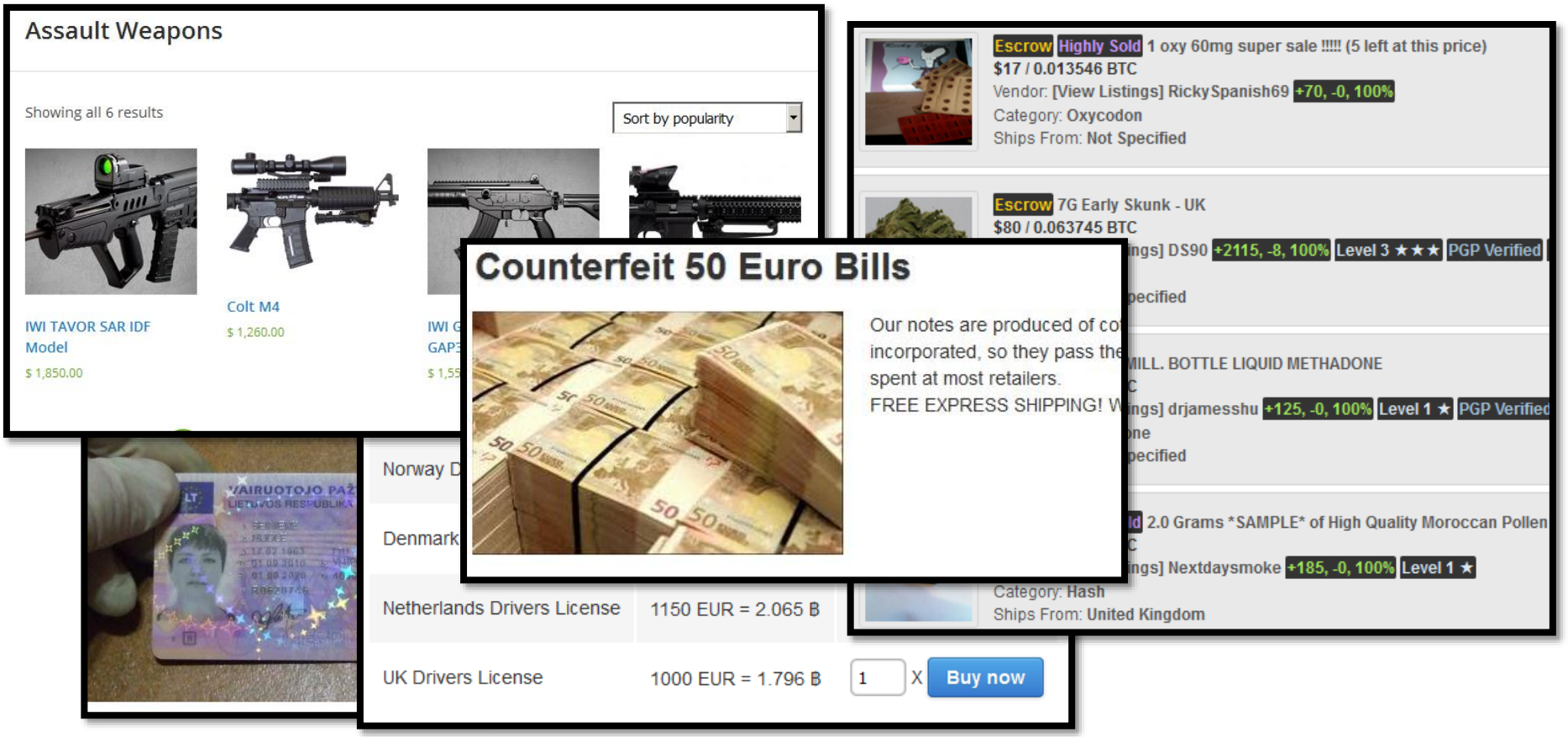
Traditional Criminal Vs. Cybercriminal



Cyber Crime
Cyber Crime - Forms/Techniques

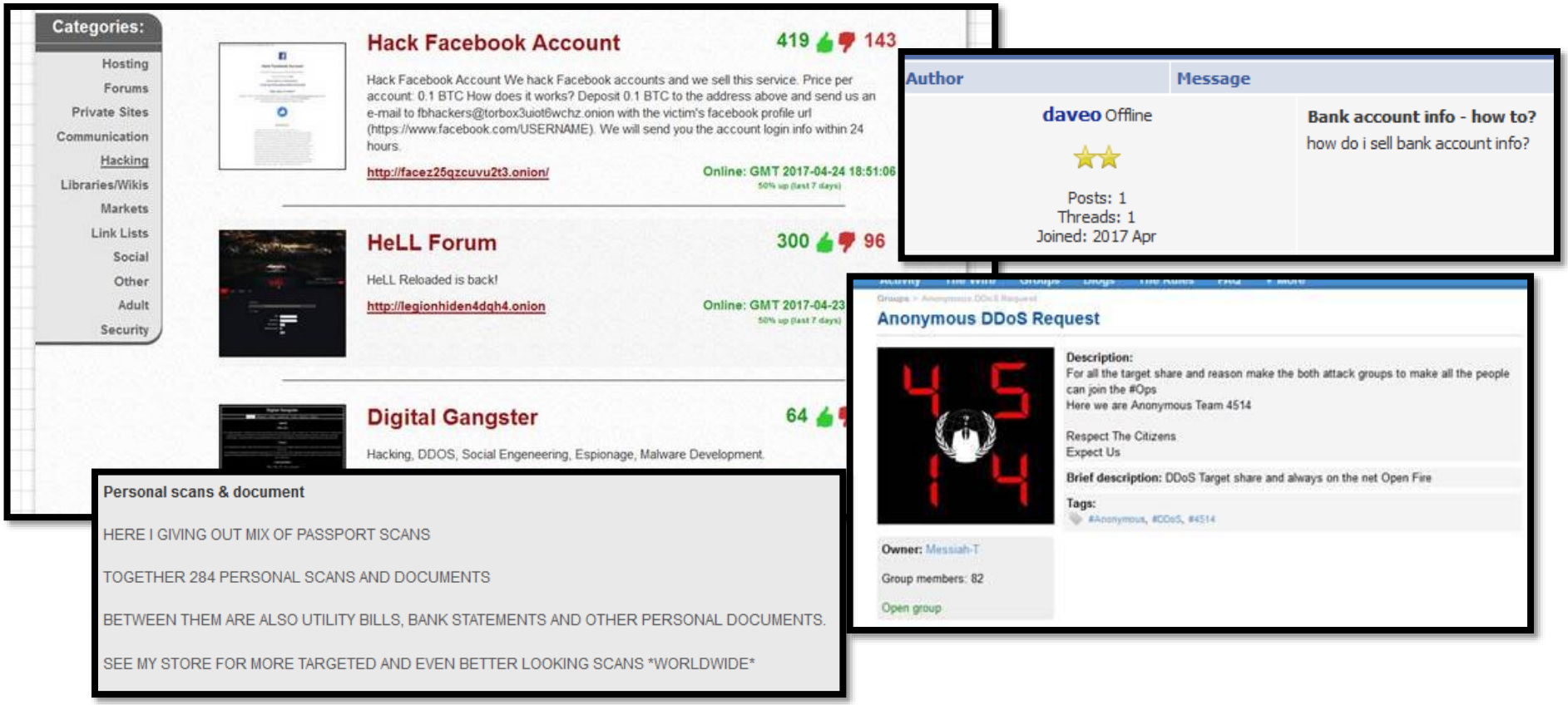
Cyber Terrorism	Identity Theft	Espionage	Cyberattack	Cyber Bullying
Hacking	Fake Mobile Apps	Piracy	Phishing/ Vishing	Crimeware
Cyber-squatting	Ransomware	Extortion	Social Engineering	Web Jacking/ Hoax Email
Pharming	DDoS	Fake Job Offers	Salami Slicing	Cryptomining

Cyber Crime
The Dark/Deep Web – Things that can be found…

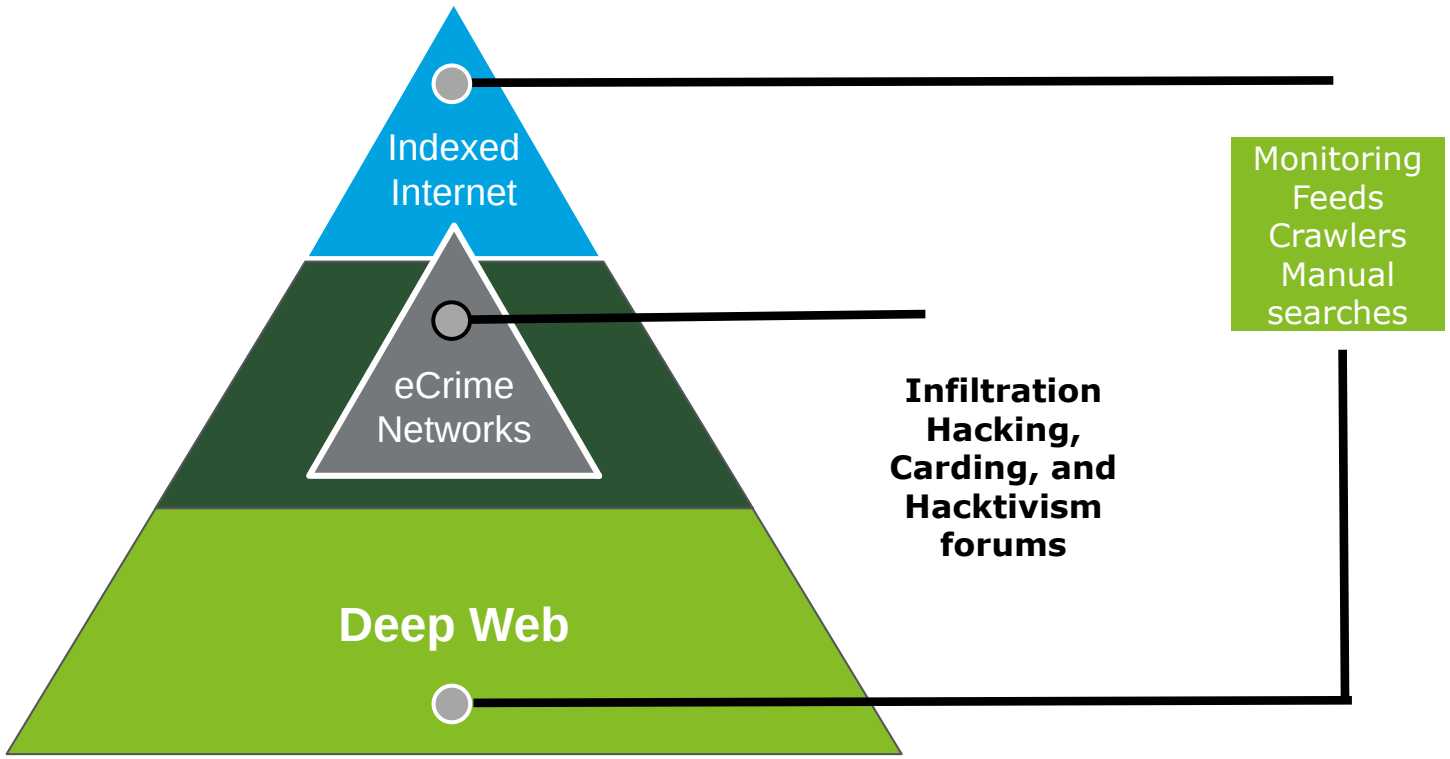


Intelligence acquisition
(Sources)

Cyber Crime
The Dark/Deep Web – Things that can be found

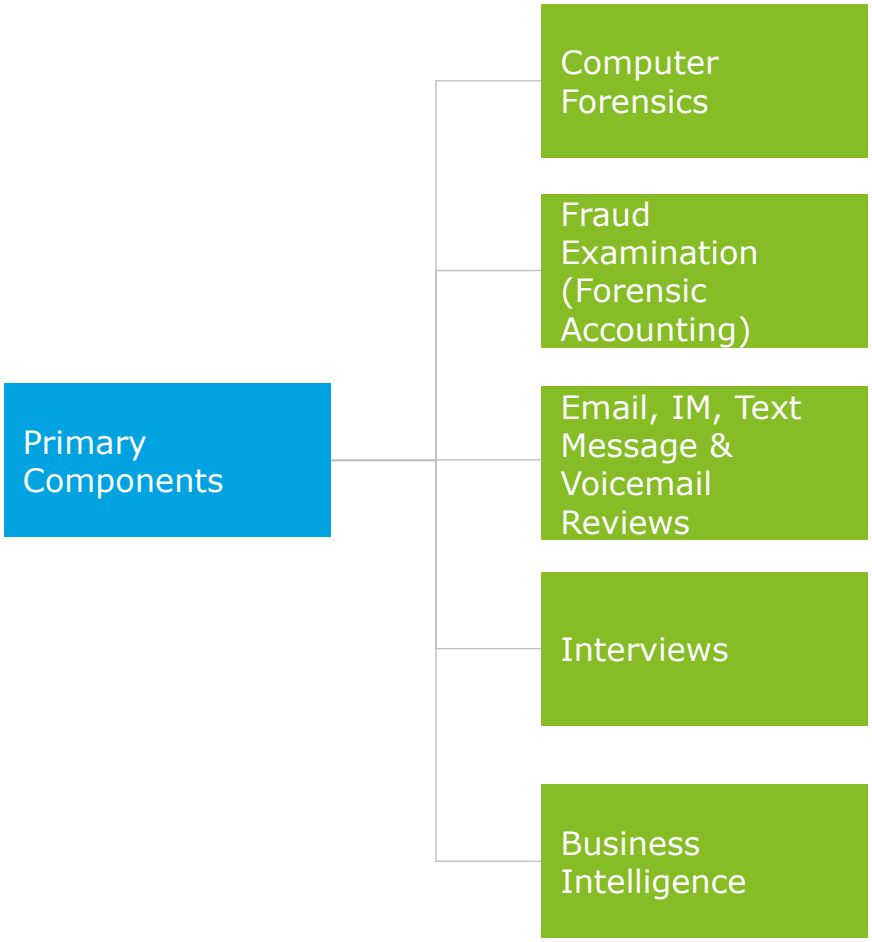


Intelligence acquisition
(Sources)



The Dark/Deep Web

Cyber Crime
Typical Approach



- Electronic discovery & data collection
- Data analytics

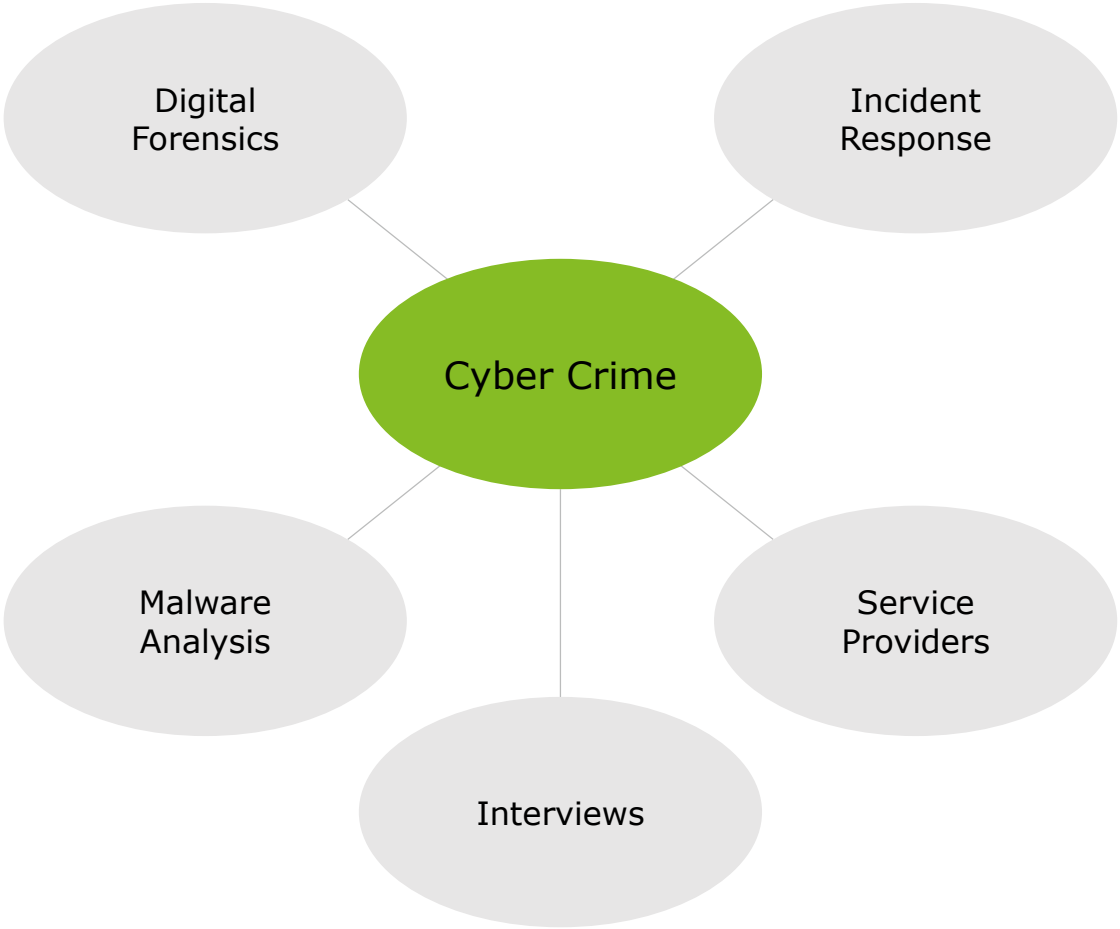
- Detailed review of documents & data
- Fraud examination techniques
- Information-seeking & administration-seeking interviews

- Keyword searches
- Analysis and screening of hit rates
- Document review/2nd level review

- Questions (incorporate findings from document review process)
- Interview techniques
- Documentation and analysis of responses

- Individual/company background search

Cyber Crime
Ideal Approach



Cyber Crime
Challenges

Cyber Crime

Cyber Crime
Recent engagements

1

In early 2017, Deloitte Cyber Incident response (CIR) personnel was contacted by a software company to assist with ongoing incident response activities involving unusual behaviour detected on one of their servers.

As a result of this analysis, Deloitte was able to identify major points of interest regarding the timeline of a malware infection, portions of the communication activity initiated by the malware, and its general activities on the network.

Our analysis, based on the behavioural indicators from the malware analysis suggests that the malware packages appear to be relatively common and indicate that they were all related to a single hacker group named “legenda”.

2

Deloitte assisted a major manufacturing client to investigate a case of fraudulent activity on their accounting system. Deloitte investigated the people, process and technology parts of the business.

By analysing system logs, we were able to identify access times and people involved in the fraud.

Deloitte was able to pinpoint the fraudulent activity to an employee within the client’s organization

Some wins…despite the challenges (Deloitte)

In September 2018, Deloitte investigated a ransomware infection at a major manufacturing client in SA via their subsidiary in the US

Cyber Crime
Trending

Ransomware
Wannacry…Petya

Cyber Crime
Trending

Cryptomining

Cyber Crime
Trending

Business Email Compromise

Questions

Deloitte.