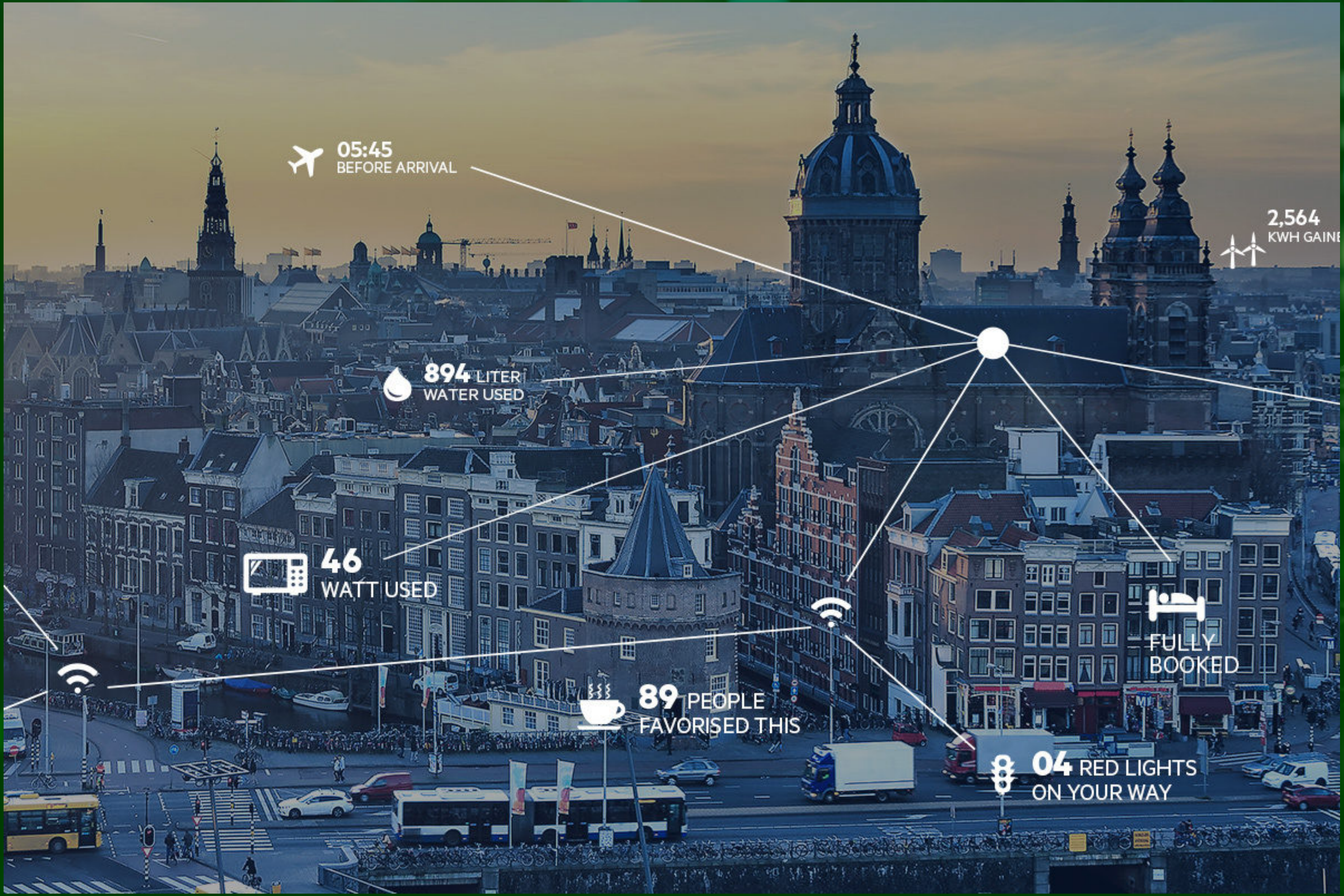
Collaboration in the Cyber Security Defence

Oscar Koeroo – Security advisor

KPN CISO :: Strategy & Policy

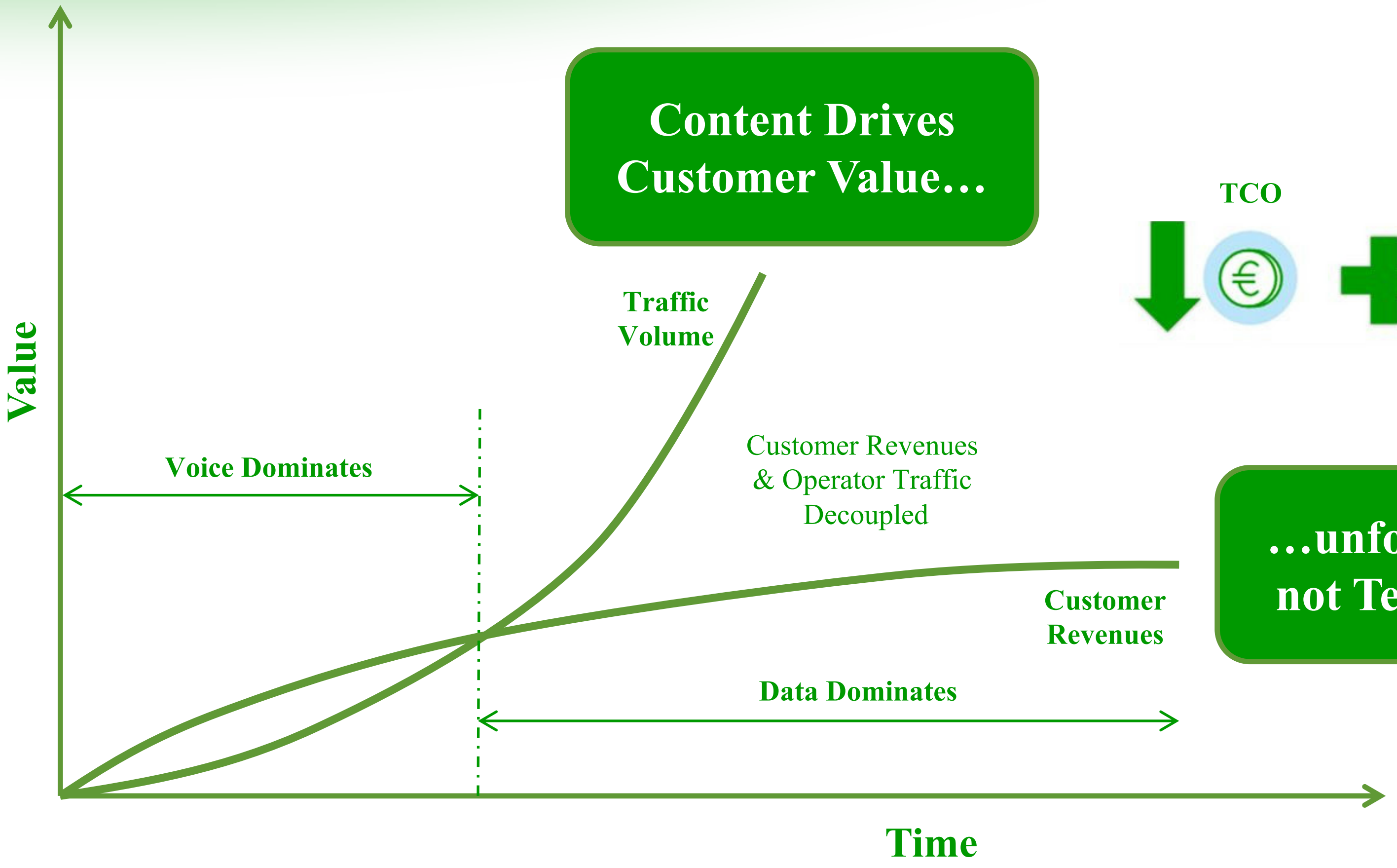
KPN


05:45 BEFORE ARRIVAL
2,564 KWH GAINE
894 LITER WATER USED
46 WATT USED
FULLY BOOKED
89 PEOPLE FAVORISED THIS
04 RED LIGHTS ON YOUR WAY

“To keep KPN reliable and secure and trusted by customers, partners and society”

Why We Need To Transform

From a Telecom Operator into an “Integrated Connectivity Provider”



Content Drives Customer Value…

TCO + NPS

…unfortunately not Telco Value

Transformation Through Technology

Organization, way of working, services and cost structure

kpn **Transforms into**

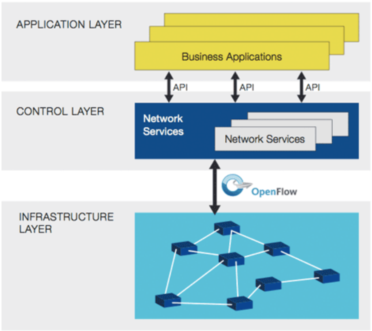
TCO ↓ € ✚ NPS ↑

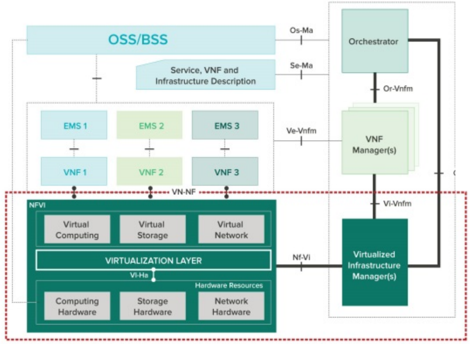
Agile / OTT like player

Telco unlike Customer Service

TCO < 50% / Quality > 2x

Using **Software Defined Networking** and **Network function Virtualization** architecture





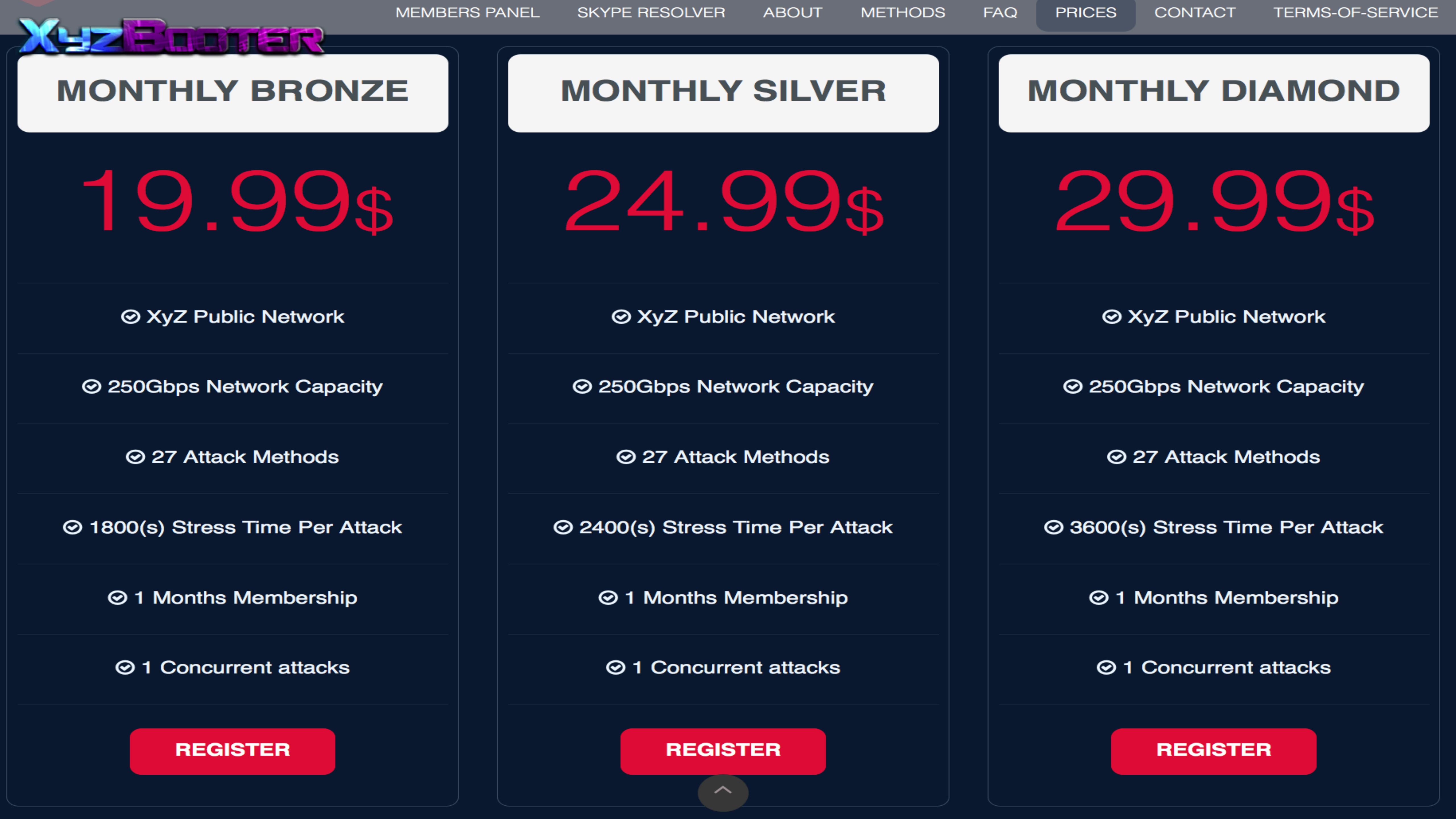
Attacks can’t always be prevented.
Focus on detection and proper resolution

Regin: Top-tier espionage tool enables stealthy surveillance
Symantec Security Response
Anonymous
those innocent killed, the anonymous of all the planet have decided to declare war on you terrorists
PASSWORD
WANNA CRY
Petya Ransomware
PRESS ANY KEY!
TalkTalk
Brighter Phone & Broadband
will rise 卍 We will destroy 卍
belgacom

```
sh-3.2$ env
rable' bash
vulnerable
this is a t
```

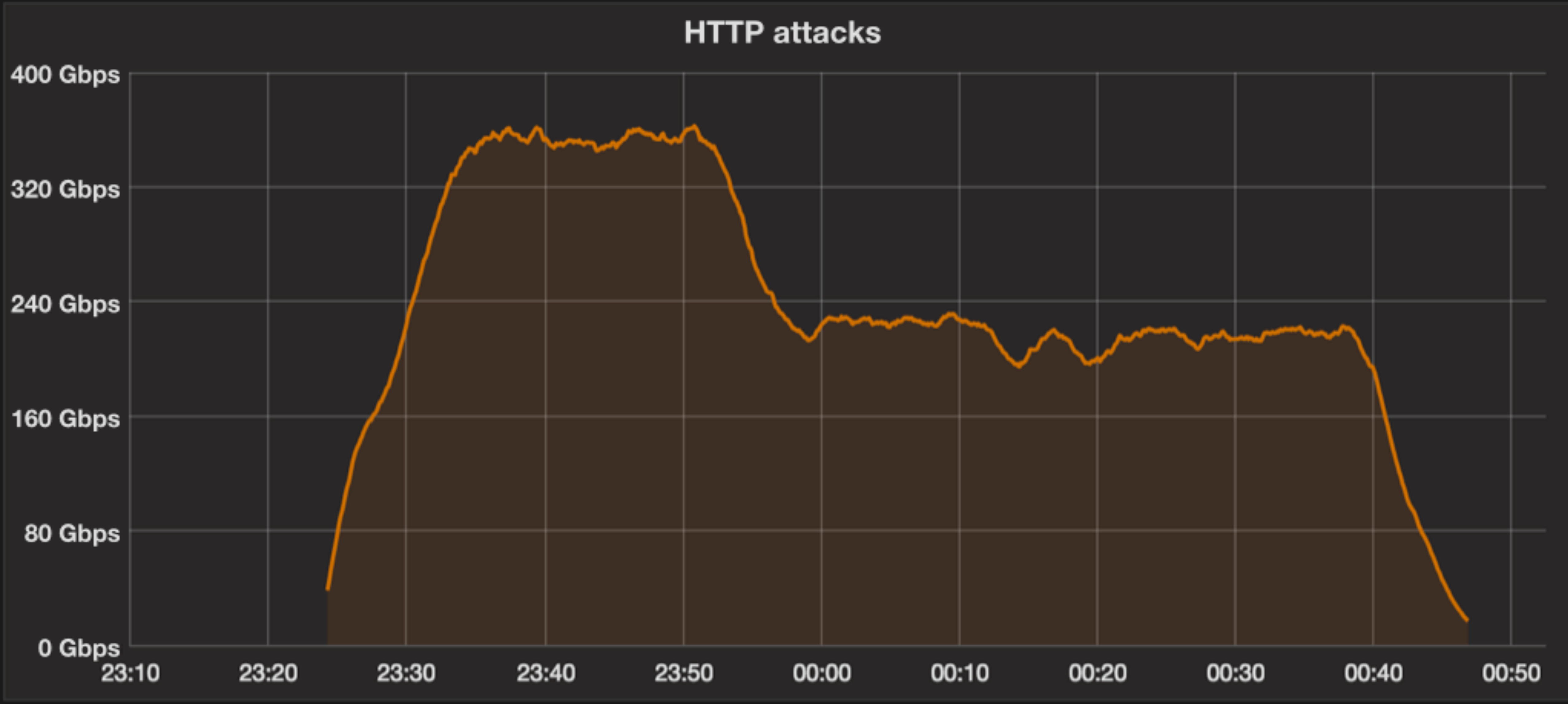
Different type of attackers

Actors	Motivation	Threat vector	Impact
Individual Hacker (KPN 2012)	– Opportunistic – Disenfranchised	– Opportunistic vulnerabilities – Insider	– Integrity of systems and data – Reputational and Brand loss – Regulatory
Hacktivists (ZIGGO ATTACK, Panama Papers)	– Targeted – Ideological – Political cause – Malicious havoc	– Compromise of 3rd Party & Service Provider – Volume, Targeted attack – Opportunistic vulnerabilities	– Disruption of operations – Defacement of public sites – Reputational and Brand loss
Cyber Criminal (Talk, Talk, $1bn Carbanak)	– Illicit gain – Fraud – Identity Theft – Competitive Intelligence	– Insider – Data Breach – Intellectual Property theft	– Customer Privacy – Financial impact – Intellectual Property loss
State Actor (Belgacom, SONY)	– Geopolitical target – National Security gain – Disrupt others Critical Infra – Economic Espionage	– Advance Persistent Threat (time/assets) – SCADA/ ICS – 3rd Party & Service Provider	– Critical Infra damage – Intellectual Property theft – Economic & Political destabilization



MONTHLY BRONZE	MONTHLY SILVER	MONTHLY DIAMOND
19.99$	24.99$	29.99$
✓ XyZ Public Network	✓ XyZ Public Network	✓ XyZ Public Network
✓ 250Gbps Network Capacity	✓ 250Gbps Network Capacity	✓ 250Gbps Network Capacity
✓ 27 Attack Methods	✓ 27 Attack Methods	✓ 27 Attack Methods
✓ 1800(s) Stress Time Per Attack	✓ 2400(s) Stress Time Per Attack	✓ 3600(s) Stress Time Per Attack
✓ 1 Months Membership	✓ 1 Months Membership	✓ 1 Months Membership
✓ 1 Concurrent attacks	✓ 1 Concurrent attacks	✓ 1 Concurrent attacks

100k IP-cameras infected with MIRAI

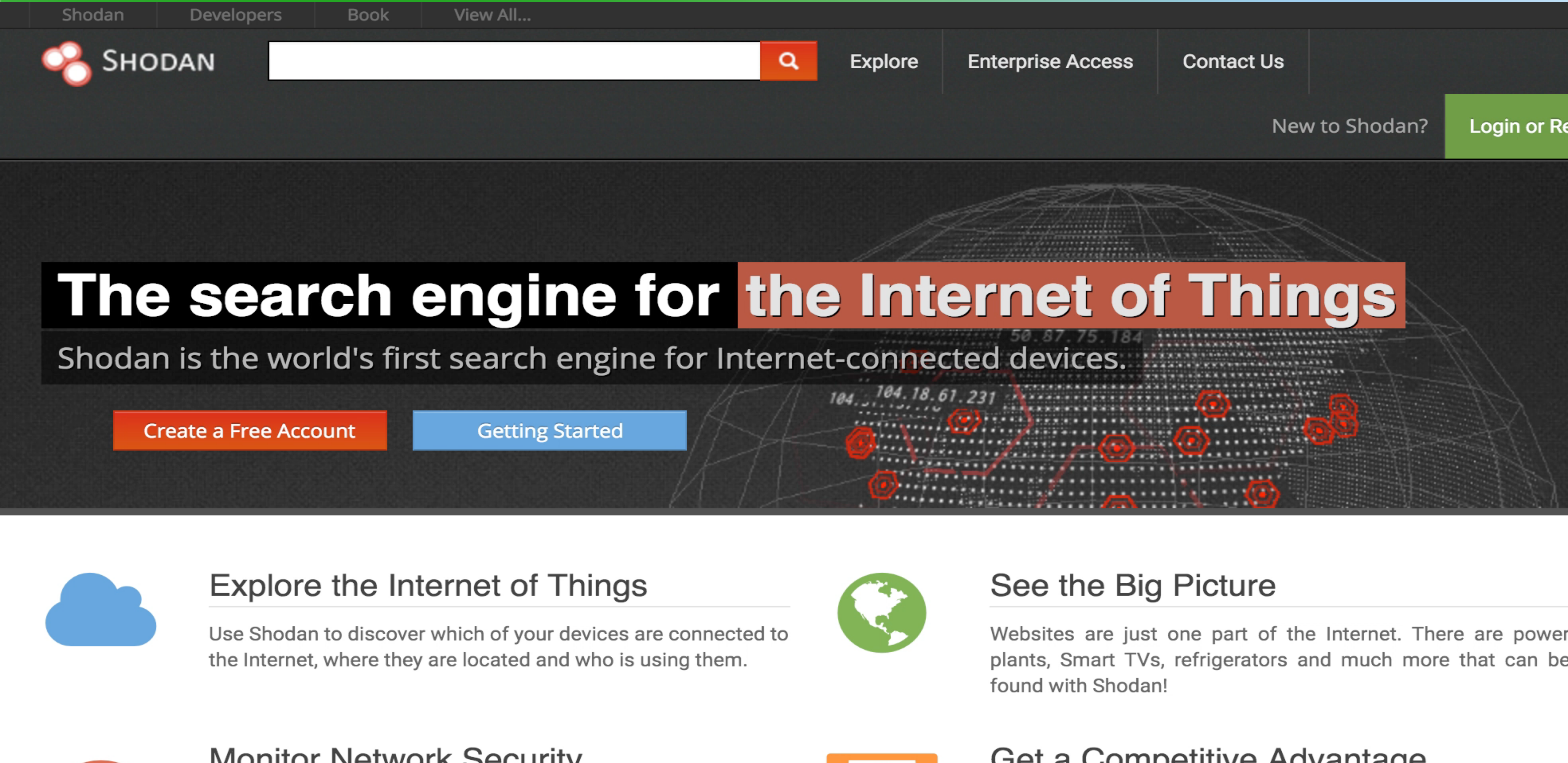


IoT
Attack surface expansion

- Increased deployments
- Highly diverse build quality
- Low/no physical security
- Hyper connectivity

How we look at ourselves: security monitoring at a SOC

The world can observe your weaknesses in detail



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

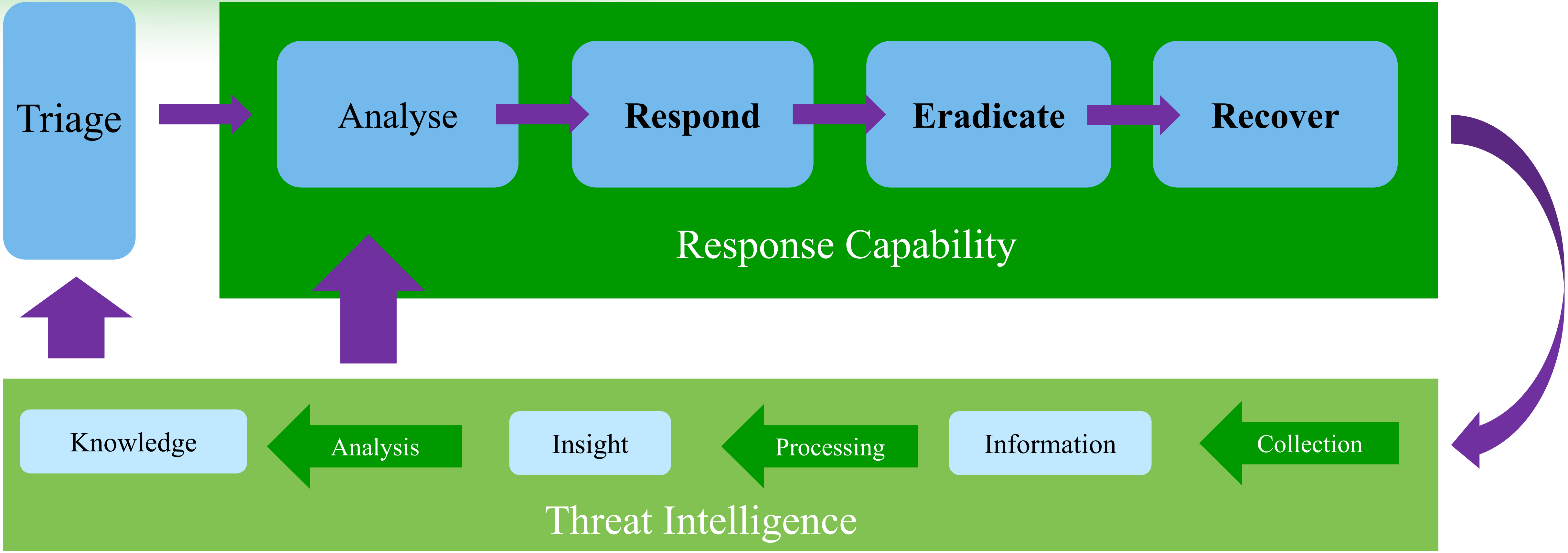
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Get a Competitive Advantage

Why you need Threat Intelligence

Incident Response process


Triage

Analyse

Respond

Eradicate

Recover

Response Capability

Knowledge

Analysis

Insight

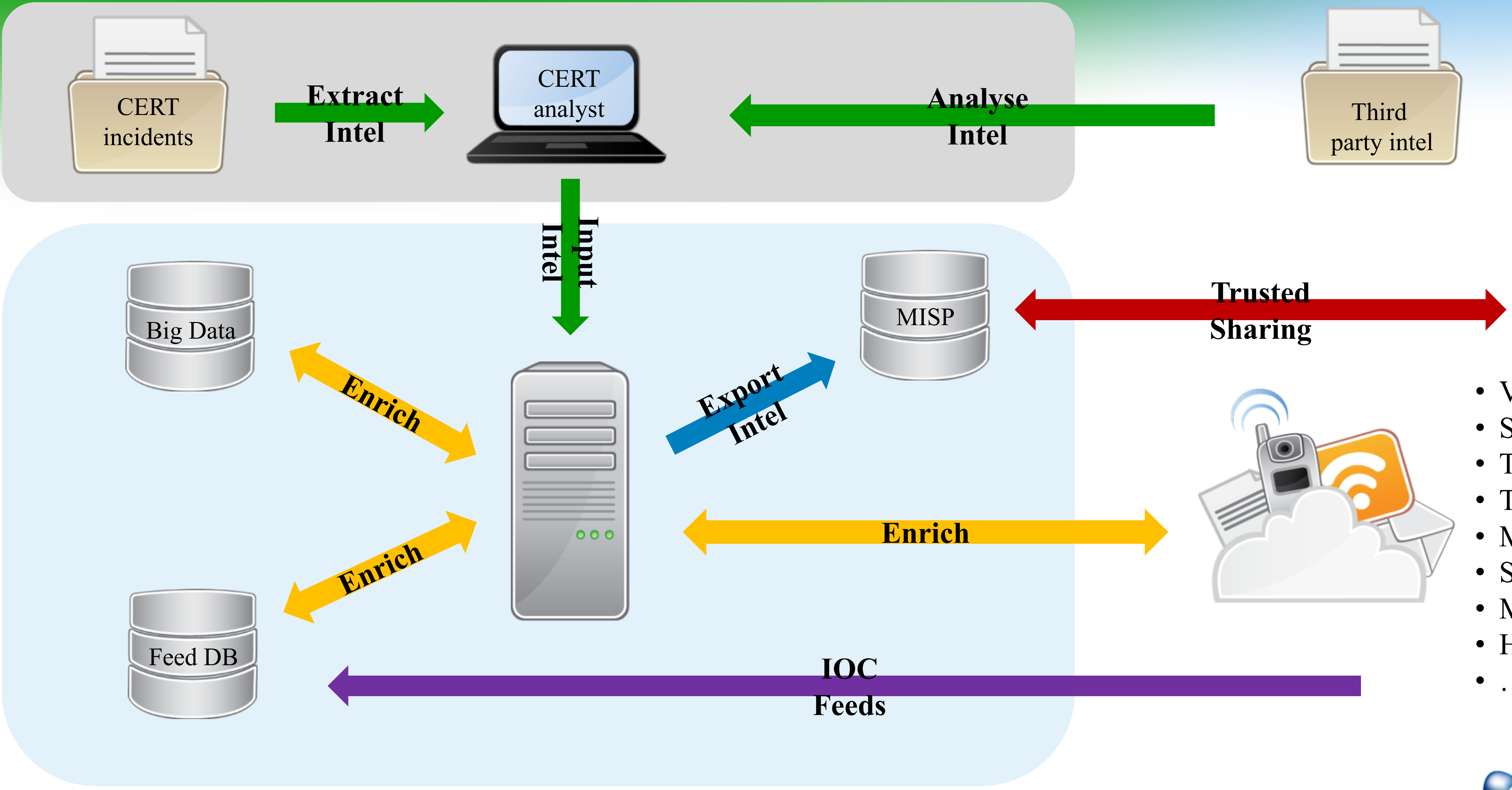
Processing

Information

Collection

Threat Intelligence

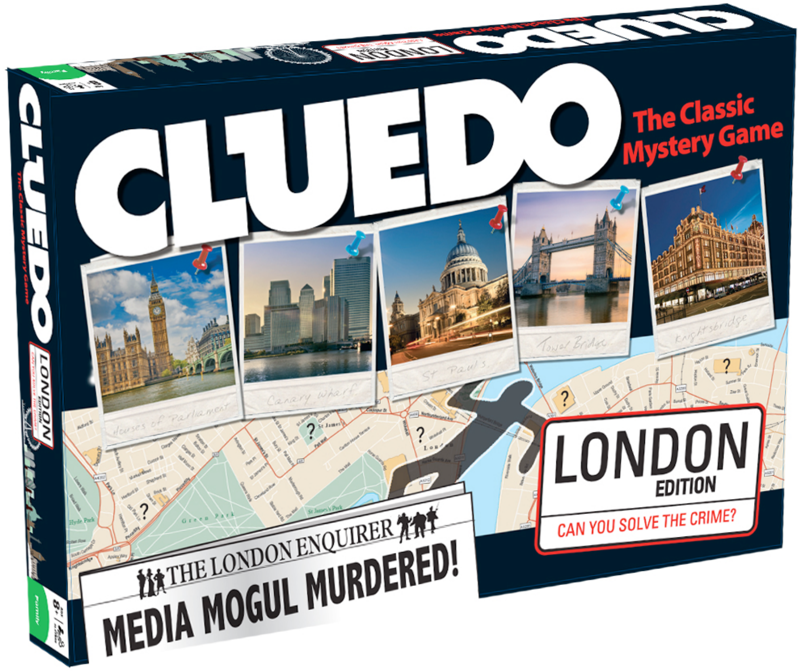
Threat Intelligence architecture



- VirusTotal
- Shodan
- ThreatCrowd
- ThreatMiner
- Malwr
- ShadowServer
- MISP
- Honeypots
- …

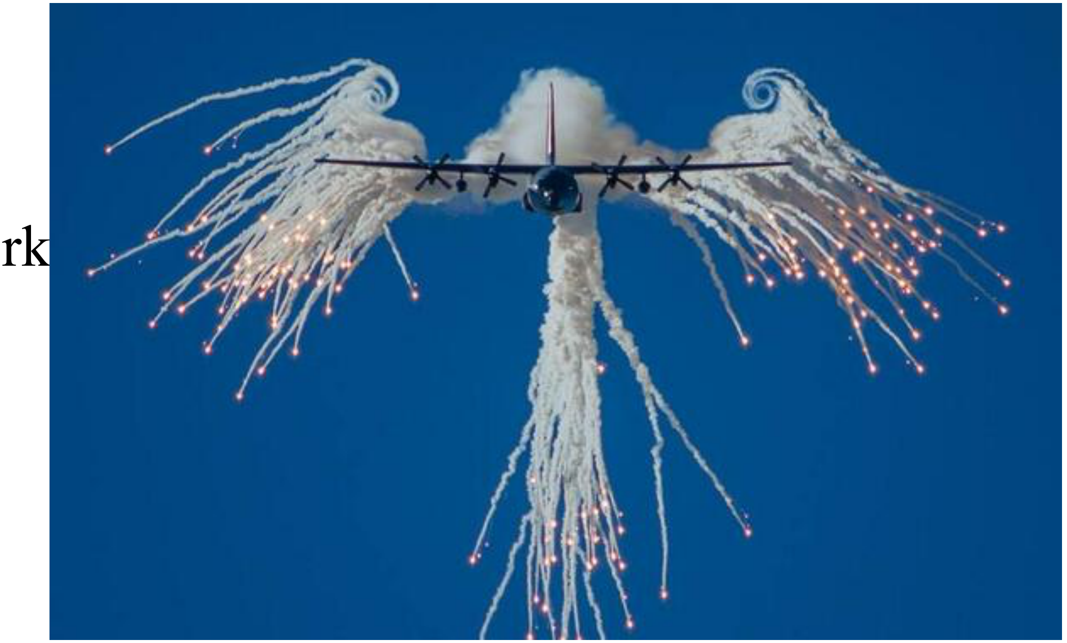
The attackers are not rapidly changing their techniques
They do return more often and improve existing skills

- Proper forensic analysis can take weeks
- Attackers can hide their tracks
- Attackers can disrupt with easy attacks
- Attackers are agile

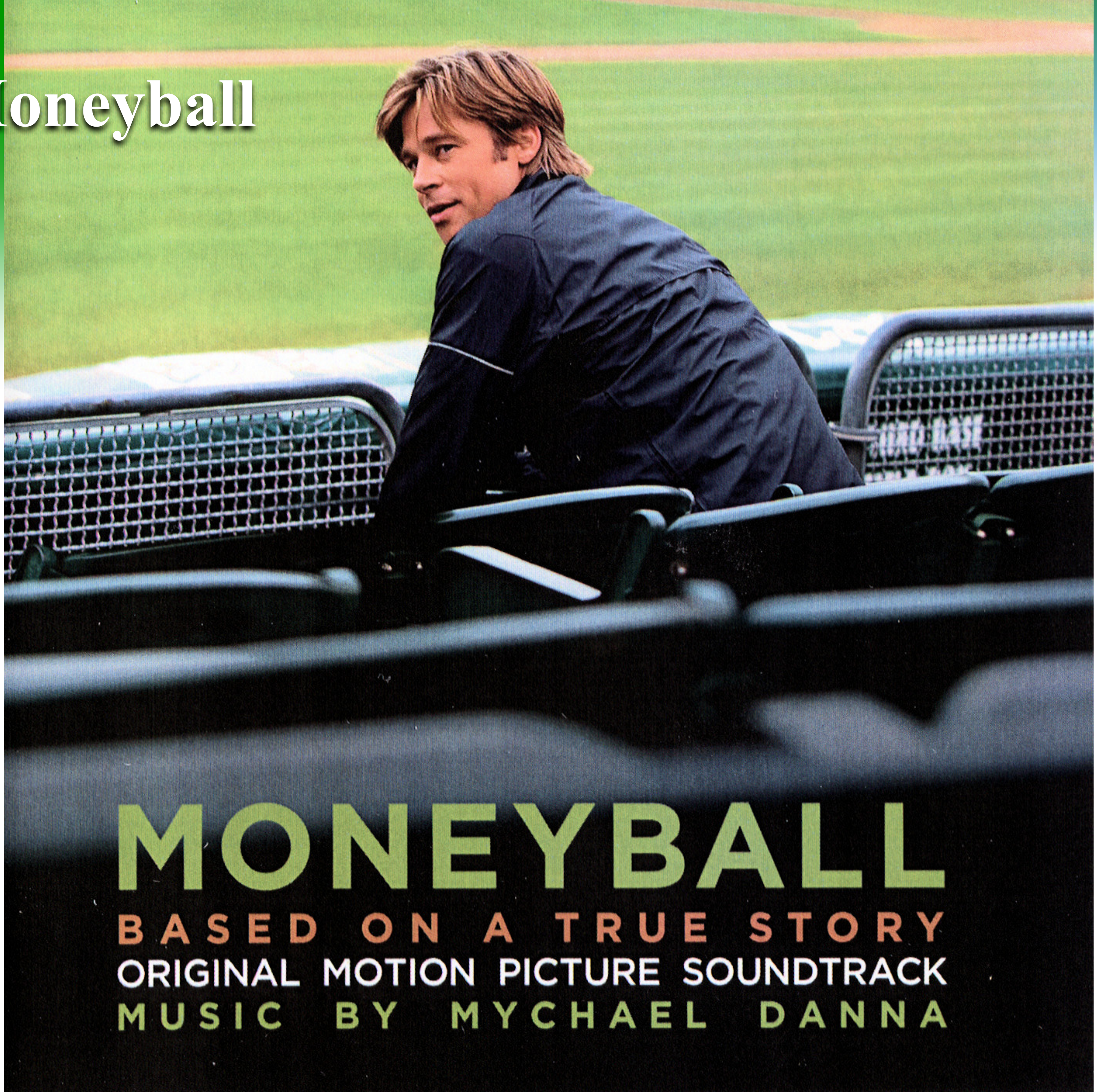


What we wish to have in our future network

- (Plan) Sharing information with peers in a standardized and structured way
  - STIXX, TAXII, CyBox to share (contextual) information and IoCs
- (Do) Take a decision on what to do.
  - Templated or semi-automated
  - Keep human control in the automated loop
- (Do) Fitting countermeasure deployment in our network
  - FlowSpec/filter, scrub, null-routing, or other
  - Reconfiguration of the network
  - Dynamically add different monitoring for analyses
  - Adaptive segmentation
- (Check) Verify effectiveness



Security Moneyball



FIGHT FOR THE USER