PCCW Global®

CRYPTEIA NETWORKS
a PCCW Global company

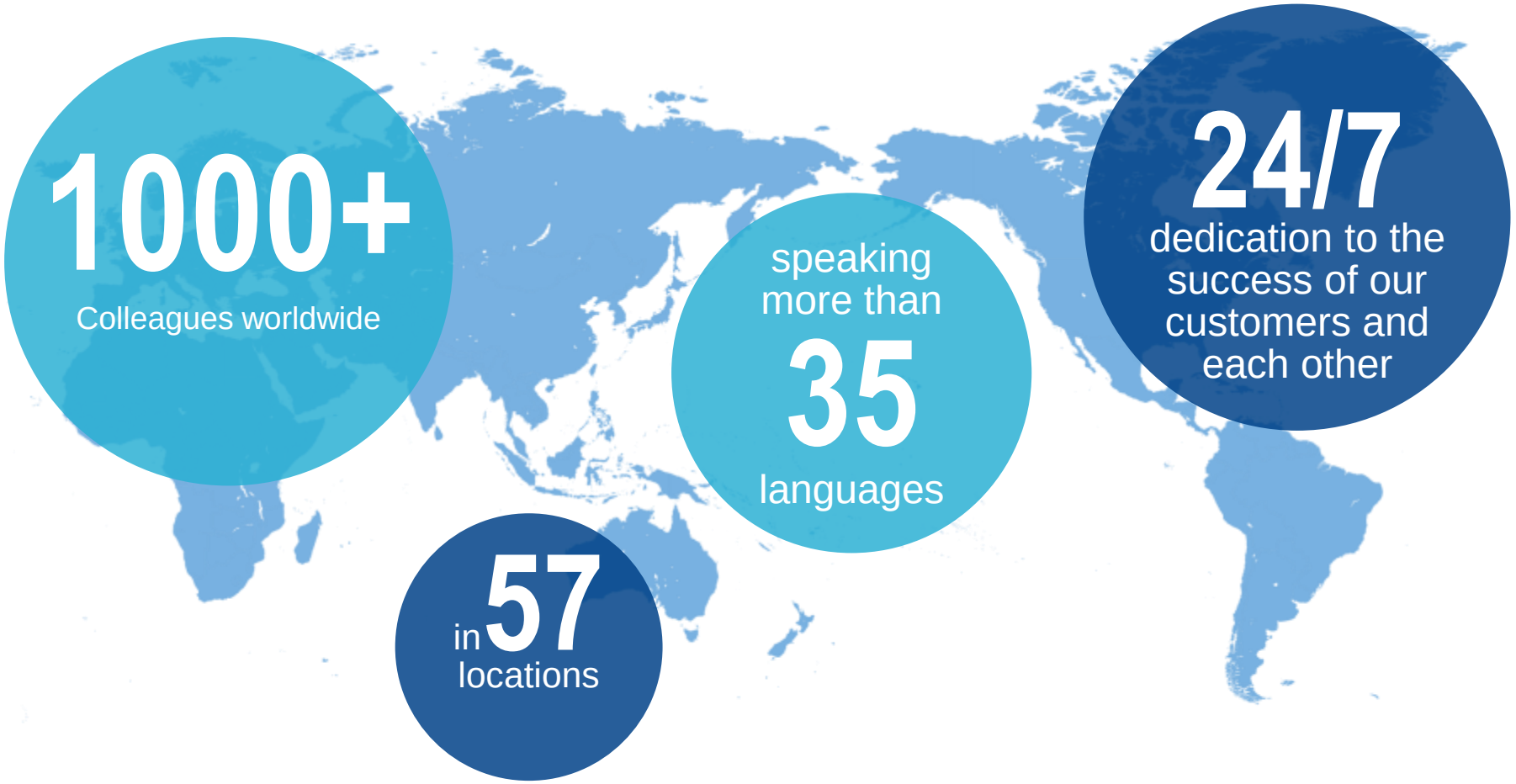
Threat Management Evolution

Paris Mermigkas. Security Content Researcher, MSDS, R&D

April 2016

HKT Here To Serve a PCCW-HKT Group member

Our Global Team



Core PCCW Global Network Capability

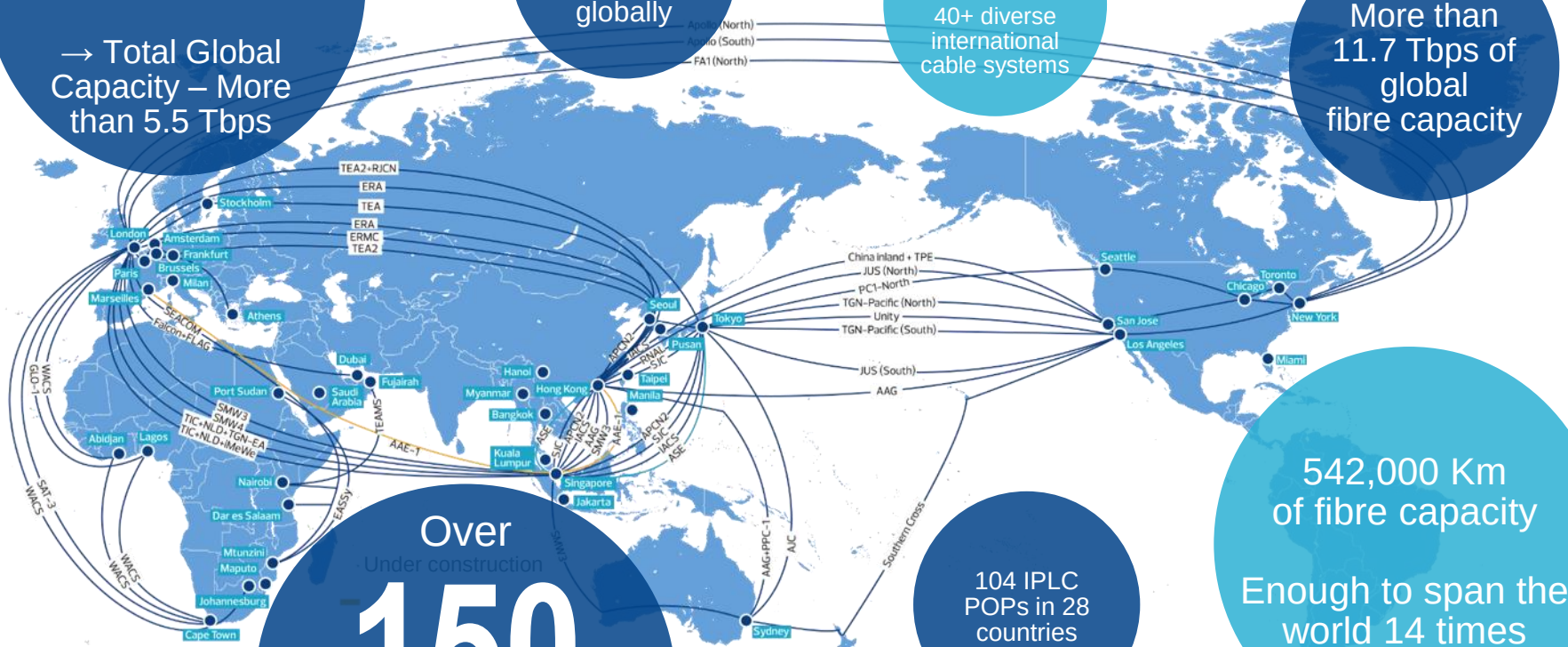
AS3491 is consistently ranked in the top 10 for Global Peering

→ Total Global Capacity – More than 5.5 Tbps

Over 7 billion voice minutes p.a. carried globally

Fully resilient network with investments in 40+ diverse international cable systems

More than 11.7 Tbps of global fibre capacity



Over
Under construction
150
countries and 3,000 cities

104 IPLC POPs in 28 countries

542,000 Km of fibre capacity

Enough to span the world 14 times

Crypteia Networks

PCCW Global acquired Crypteia Networks in 2014

Crypteia Networks was founded as a Security-as-a-Service provider focused on real-time event analysis & management

It developed MOREAL to proactively combat known and unknown threats to network security within an enterprise and give enterprises efficient access to security services via its cloud-based model

Awards

CRYPTEIA NETWORKS
a PCCW Global company

The Cost of Cybercrime

$3 trillion

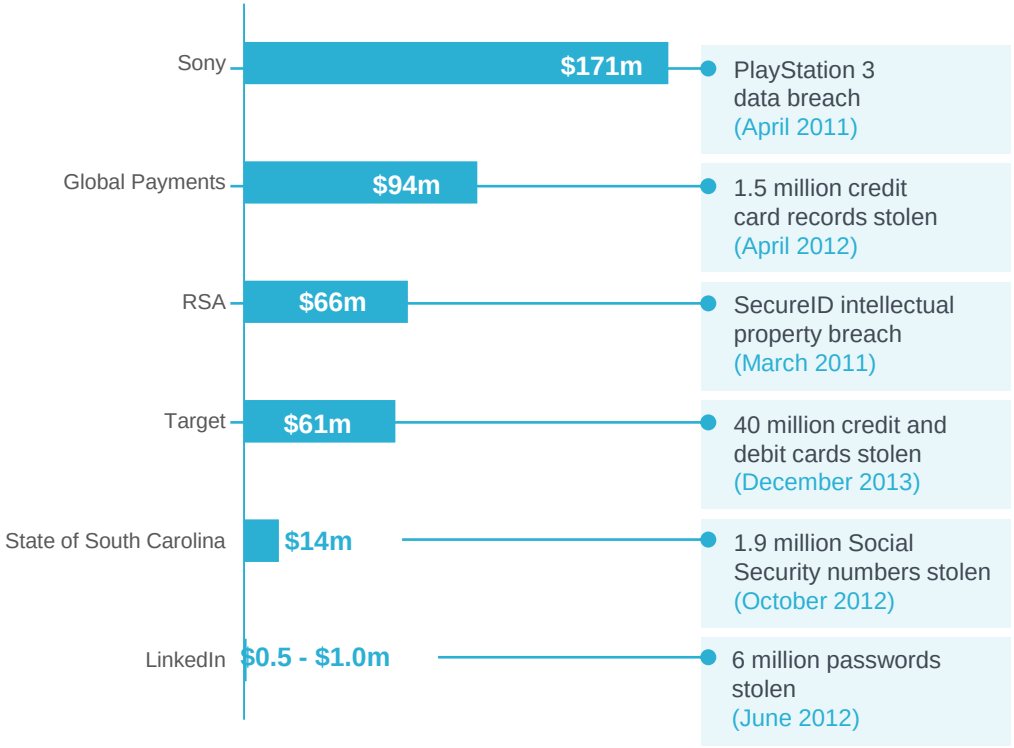
Cybercrime Cost

Source: ISACA

$67 billion

Annual Security Investments

Source: Gartner



Network Threat Management

Network threats may be categorized as:

- Threats you know about.
- Threats you don't know about.
- Threats you only find out about after a compromise.

Most security services rely on recognizing known threats rather than new or constantly changing threats.

Our Threat Management Service continuously scans for threats in real-time, self-learns, and provides actionable threat identification.

It is designed to identify known, unknown and even threats that have compromised your security but have yet to do harm to your organization

What is MOREAL?

MOREAL is a solution for identifying network security threats in real-time and providing actionable information for combating attacks on an organisation.

Self-Learning Threat Database

Proactive Real-Time Threat Identification

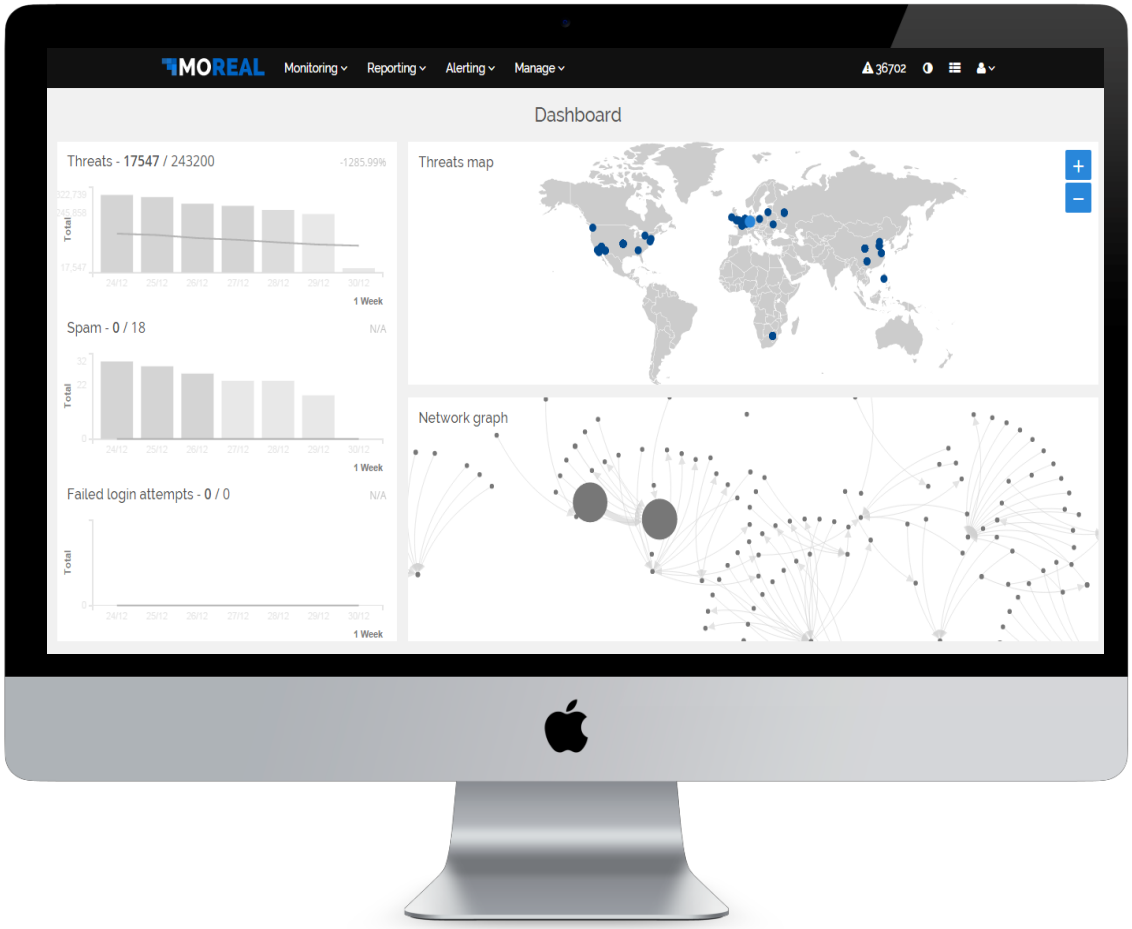
Efficient non-intrusive deployment

Scalable Cloud-Based Security

MOREAL mines data from existing network elements to identify known and unknown threats and protect your organization from revenue loss and reputation damage

The Intelligence MOREAL Provides

- View in browser.
- Identified network threats on single screen
  - Multi-vendor support.
- Alerts graded by severity.
  - Includes recommended counter measures.
    - Automatic counter measures possible using ACL, SNORT or YARA
- Customizable reports.
- Network forensics on retained log history.
  - Log retention period specified by customer.
  - Post compromise analysis.

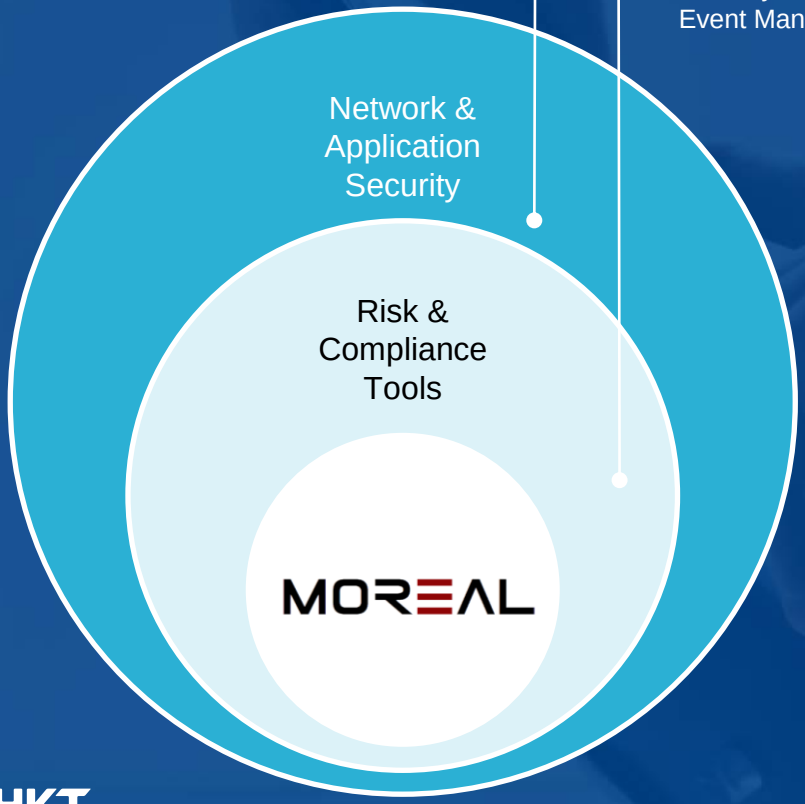


A New Layer of Network Defense

Responsive security - Moving from Prevention to Detection

- Unified Threat Management, Next Generation Firewalls, Secure Web Gateways, Intrusion Detection Systems, Intrusion Prevention Systems
- Web Application Firewall, Denial of Service, etc.

- Vulnerability Assessment
- Security Information and Event Management, etc.



A new layer of defence, complementing existing ones and maximizing value of logs already generated & collected

Non-intrusive and an OS independent solution for rapid deployment

Threat aggregation and behavioural analysis identifies threats in their infancy

Real-time mitigation recommendations

Expands the visibility of existing security systems and hardware

Expands the lifespan of existing security solutions, driving cost efficiency

Security Operation Centers

7X24 Security Operation Centers

- Proactive monitoring
- Emergency Response & Incident Handling Teams
- Security Research Team

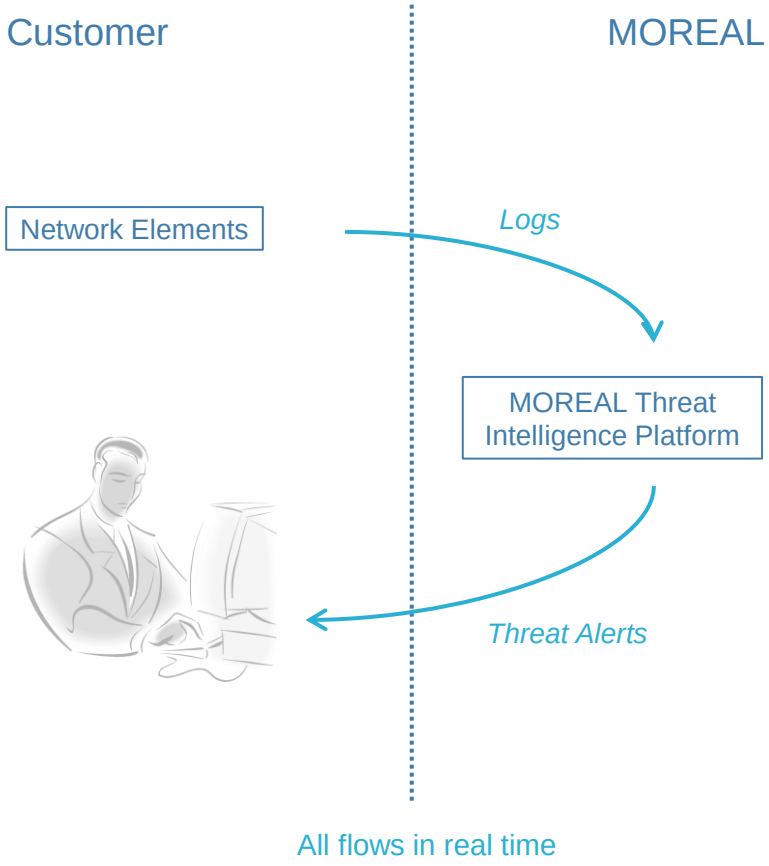
SOC: Athens, Herndon & Hong Kong

DC: Amsterdam, London, Dallas, Los Angeles, Singapore & Hong Kong

5 Steps to Recognizing Cyber Attack Patterns

1. MOREAL continuously receives logs from customer Network Elements.
2. MOREAL correlates the logs between Network Elements to get a “big picture” of all network activity.
3. MOREAL checks network activity behaviour with external threat intelligence and identifies threats.
4. MOREAL advises customer of threat and recommended remedial action.
5. MOREAL provides “SINGLE SCREEN” consolidated view of all network threats.

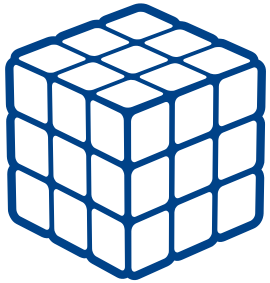
All this happens in REAL TIME



MOREAL Threat Identification Engine

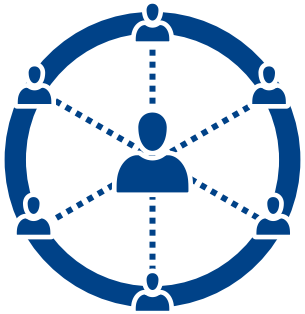
Threat DB

All threats indexed,
ready to be correlated



Threat Logic

Real-Time analysis
threat evolution



Behavioural Analytics

Prediction of threat paths with
high criticality & likelihood

A continuously updated threat database known as ***ThreatDB*** is maintained.

Baseline network flows per user, and other key metrics updated in real time are stored in the ***Behavioural Analytics*** engine.

Together these are combined in the Threat Logic module to produce ***network security threat alerts***.

The technology is self-learning and is able to identify new threats even if they have never been seen before.

MOREAL uses advanced big data analytics and machine learning.

Global Threat Intelligence

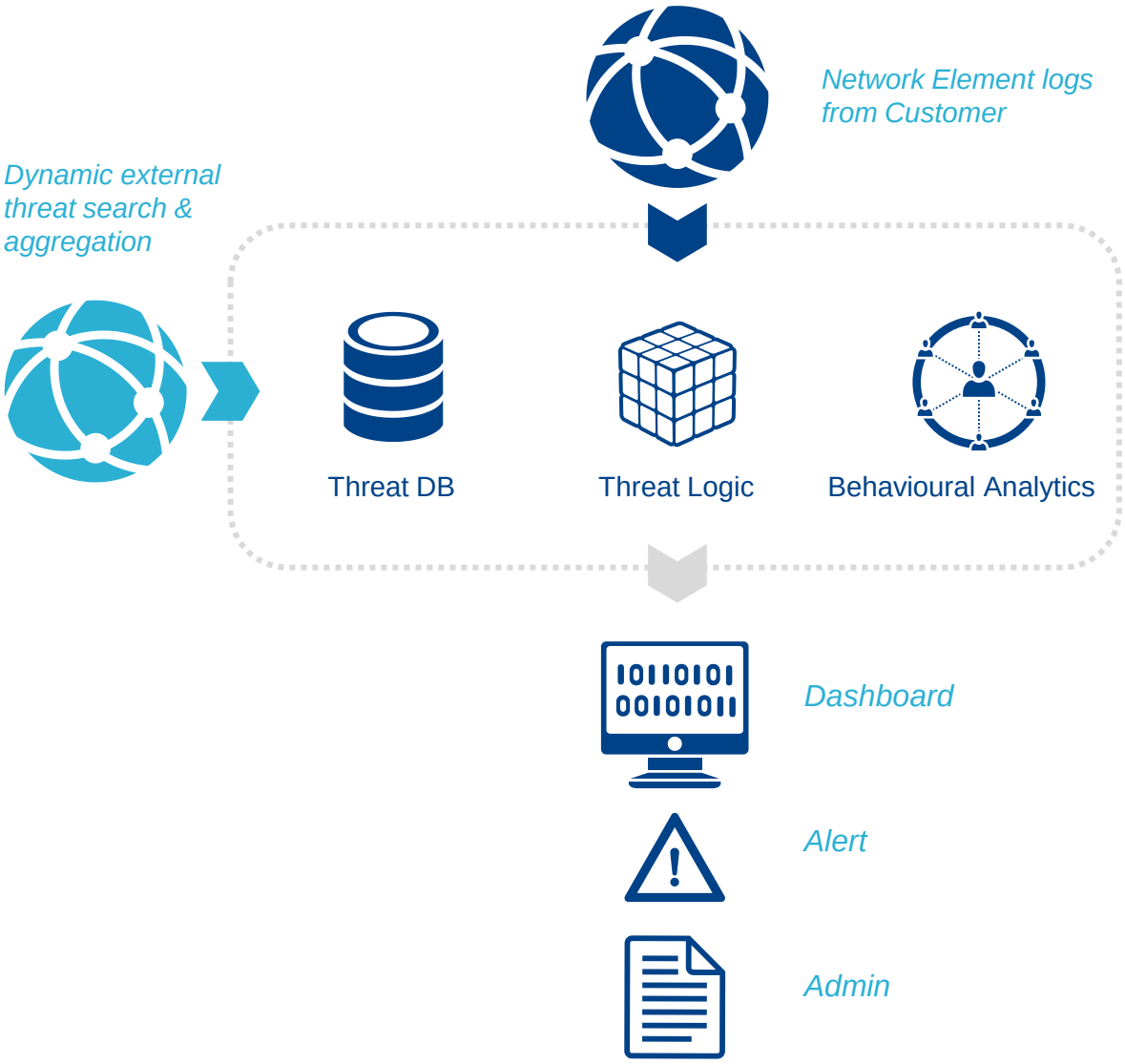
Threat DB is a database of global cyber attacks, constantly updated from multiple sources

Threat DB:
Threats normalized & indexed

Customers

CERTs Academia Industry Leaders Etc.

- ✓ *Security Research*
- ✓ *Incident Handling*
- ✓ *Feeds Normalization*



1. Network element logs are created and shared with MOREAL
2. Logs are correlated with the global threat database
3. Behavioural Analysis evaluates regular behaviour of that network and its users
4. Threat Logic scoring of the probability of threat
5. Real-Time analysis of threat and recommendations for mitigation
6. All steps are visible to the user via the dashboard
7. Threat alerts to customer via the dashboard, an email or SMS
8. Admin or PCCW Global SOC Takes Action

MOREAL Deployment Options

Cloud

Network Elements at the customers' site can directly send information to MOREAL cloud

On Premises

If, for regulatory reasons network data needs to remain on-site, an on-premises solution is also available. Logs remain on site.

The MOREAL Difference

Real-Time Intelligence

MOREAL gives you the ability to identify threats to your organization based on its data mining capabilities and traffic pattern recognition

Global Security

MOREAL has been deployed on PCCW Global's network and is capturing data on potential threats globally and on a daily basis

Enhancing Security Solutions

MOREAL extends the life of your existing security solutions and adds a layer of proactive and real-time threat intelligence

Long-Term Learning

MOREAL's threat database is continually learning and evolving to protect your organization from present and future threats

Thank you!

pmermigkas@crypteianetworks.com
pmermigkas@pccwglobal.com