12th July 2017

Protecting BT and our Customers …and a little bit of IPv6

Dave Harcourt, Chief Security Advisor

The digital opportunity and how to exploit it.

Rethink the cyber security threat.

As the threat of cyber attack grows, major corporations are struggling to keep pace with the tactics of criminal gangs, hacktivists, less ethical governments and maybe even cyber terrorists.

Ruthless entrepreneurs.

The 21st century cyber criminal is a ruthless and efficient entrepreneur, supported by a highly developed and rapidly evolving black market. Like any entrepreneur, the cyber attacker's intention is to make money – fast.

Take the fight to the attackers.

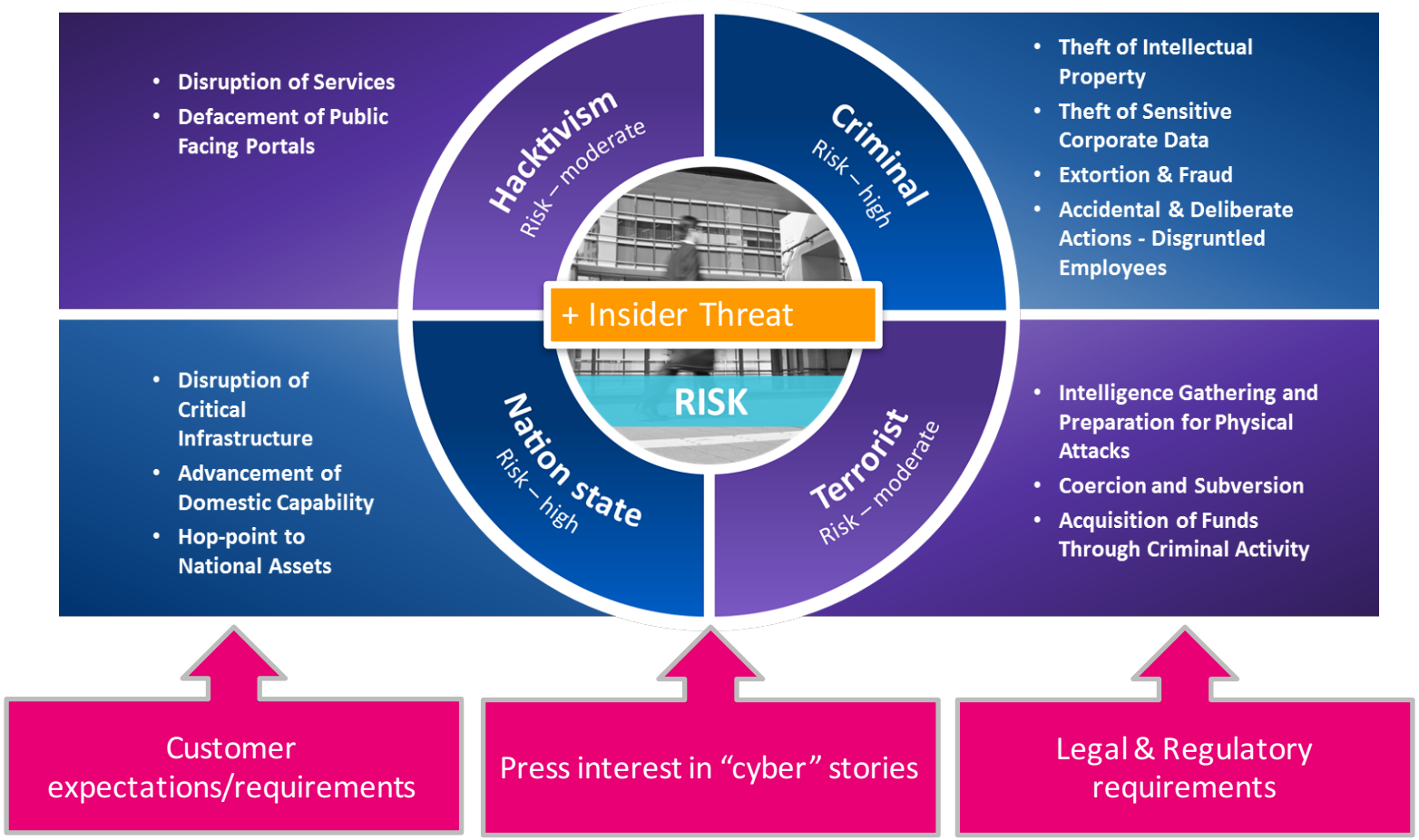
Businesses are struggling to keep up with cyber attackers, not least because procurement cycles are failing to keep pace with the efficiency of the shadow market. A change in approach and mind-set is both required and long overdue.

The need for speed and agility.

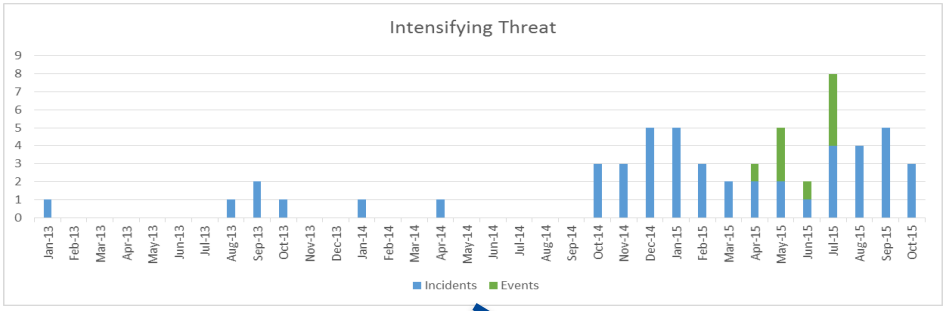
To succeed, we need our own cyber security organisations to be as creative and agile as their opponents. Businesses will also have to harness innovative technologies and approaches.

Risk and opportunity are two sides of the same coin. Throughout every global region, country and industry, digital innovation is creating new opportunities to drive efficiencies, serve customers better and increase profits & economic growth. **But that innovation can bring risk.**

Protecting BT & Customers from the Global Threat Landscape

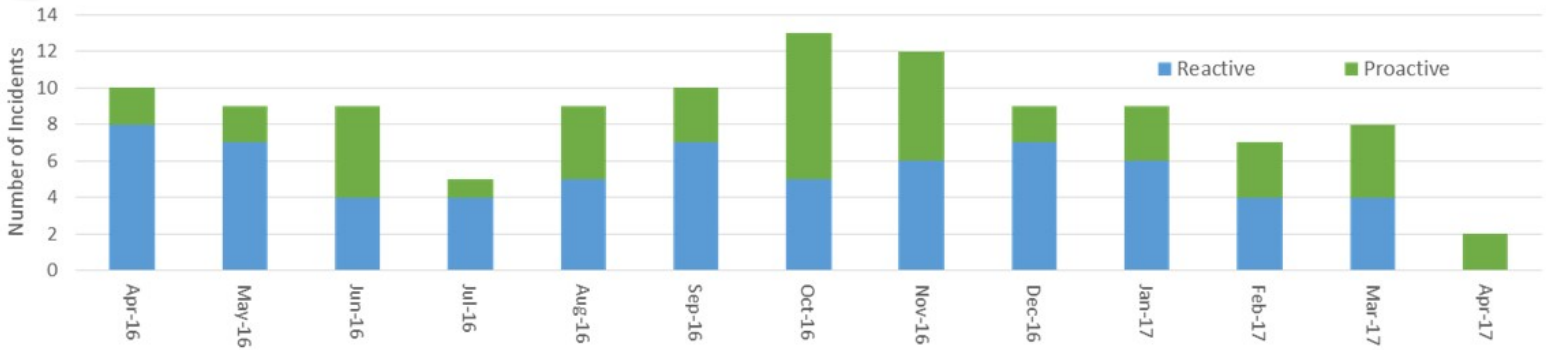


Sustained & Intensifying Cyber Threat



- >1000% increase in major cyber incidents
- Step change in complexity & sophistication of attacks

CYTADEL

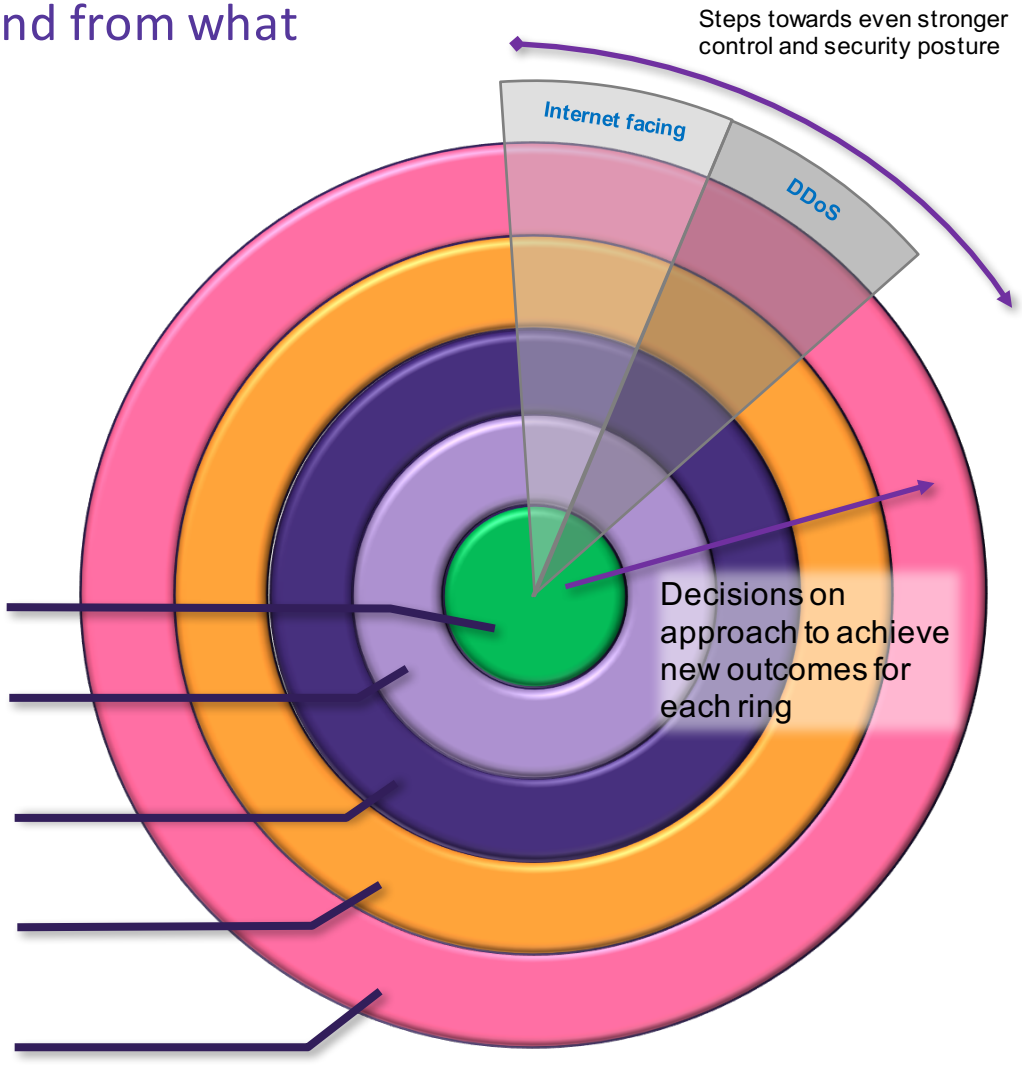


- Increasing the scope of protection and monitoring
- Matching the scale of Global DDoS threat
- Simplifying internal structure
- Increasing discovery, intelligence & insight

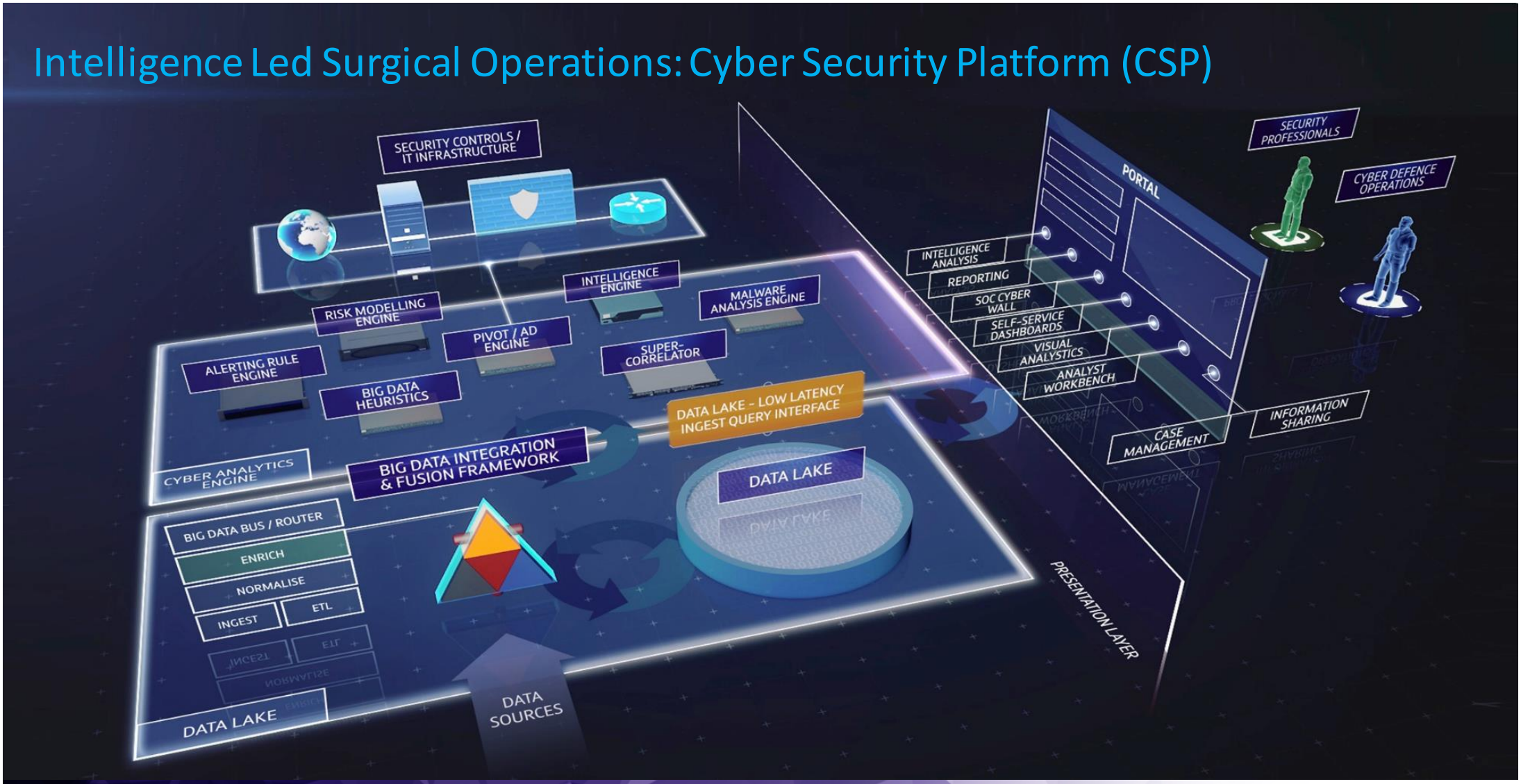
Understand what are you protecting – where and from what

Cyber Defensive Scope

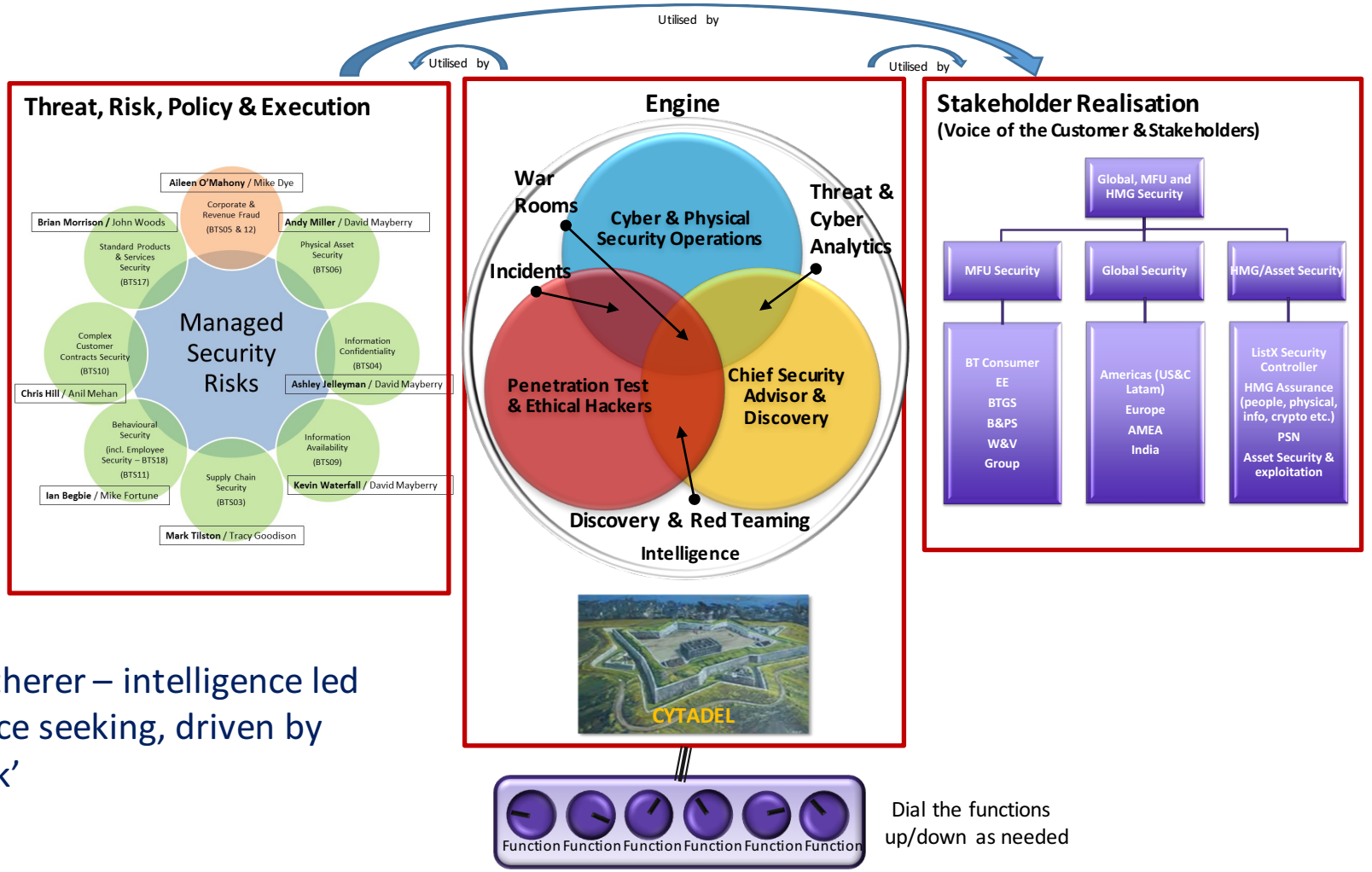
- BT's cyber defensive strategy must appropriately protect all elements of the target
- These range from core BT network and internal IT elements in the UK, through BT's subsidiaries, to non-UK domestic businesses
- Increasingly, third-party suppliers are used to provide critical services. We must ensure that these also have adequate protection capabilities
- Protection must also be afforded to IT and network services used to support customer solutions
- Some defensive measures are specific to a ring, whilst others are needed to protect multiple rings



Intelligence Led Surgical Operations: Cyber Security Platform (CSP)



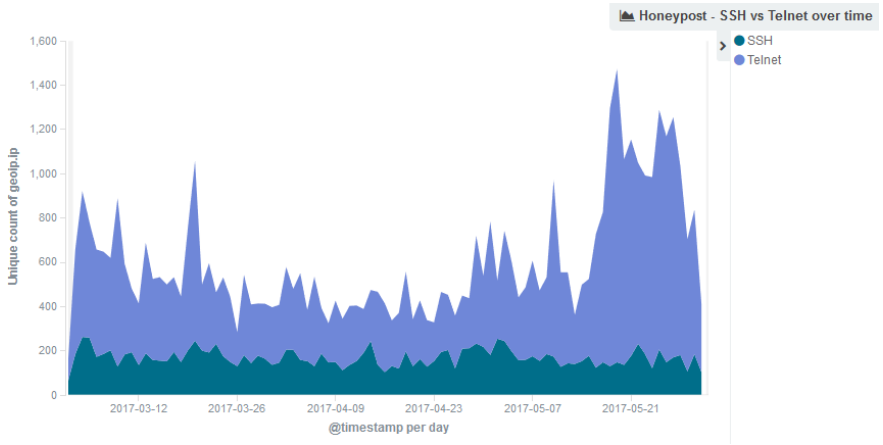
Protecting BT & Customers: **Being Hunter Gatherers**



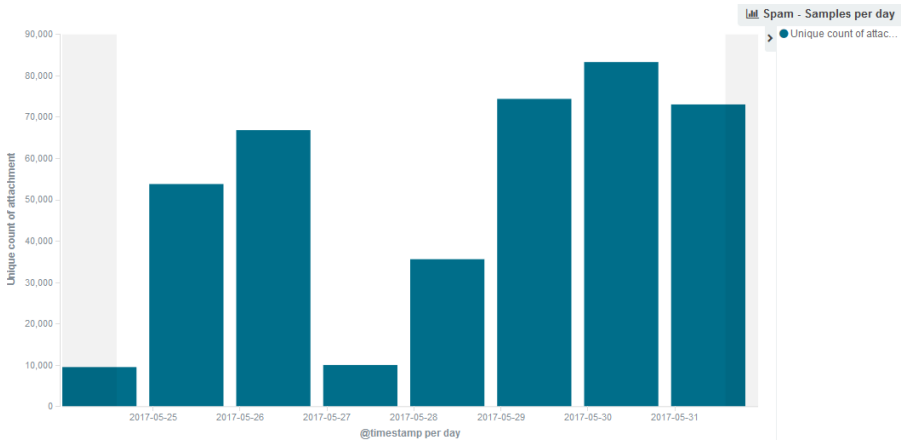
'a Hunter/Gatherer – intelligence led and intelligence seeking, driven by threat and risk'

Dial the functions up/down as needed

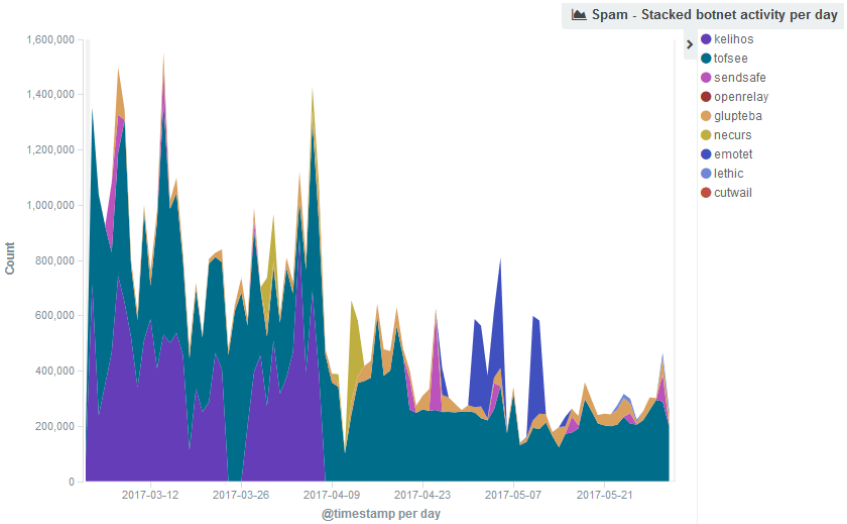
Threat Trends



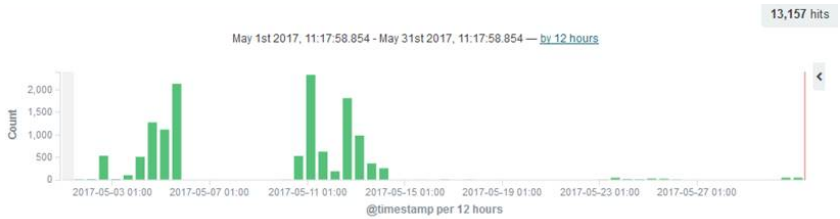
Unique count of telnet and SSH IPs seen attacking honeypots



Unique malware samples collected per day



Overall spam volumes per botnet



Malspam volumes targeting BT users over last 30 days

Global discovery and IPv6

IPv4: 32-bits long, provides **4,294,967,296** (4.3 billion) IP addresses

It is possible to scan all these in a reasonable period of time (days)

The world has officially run out of these addresses

IPv6: provides unique **340,282,366,920,938,463,463,374,607,431,768,211,456** (340 undecillion) addresses

The answer to IPv4 depletion

Good luck scanning all those!!

Tools like SHODAN have to find other techniques to discover and scan IPv6 hosts

… it's not practical to simply scan an entire IPv6 netblock!!

IPv6 in BT

BT owns IPv6 addressing around the world, some examples:

BGP ASN	Where	IPv6 allocation	Number of addresses
AS12541	BT Spain	2001:ac0:30fd::/48	1,208,925,819,614,629,174,706,176
AS2856	UK IPP	2a00:2380::/25	10,141,204,801,825,835,211,973,625,643,008
AS5400	BT Global	2001:740::/32 2a00:2000::/22	79,228,162,514,264,337,593,543,950,336 81,129,638,414,606,681,695,789,005,144,064
AS8968	BT Italy	2a02:4d80::/32	79,228,162,514,264,337,593,543,950,336

What can we do to find BT systems using IPv6?

Example methods:

- Some open-source tools exist (IPv6Walk)
- Examine BT DNS server zone files, looking at quad-A, or 'AAAA' records which are used by IPv6
- Inventories, asset management systems
- Passive DNS monitoring, to detect AAAA lookups being performed
- Netflow data capture
- pool.ntp.org?

Thank you