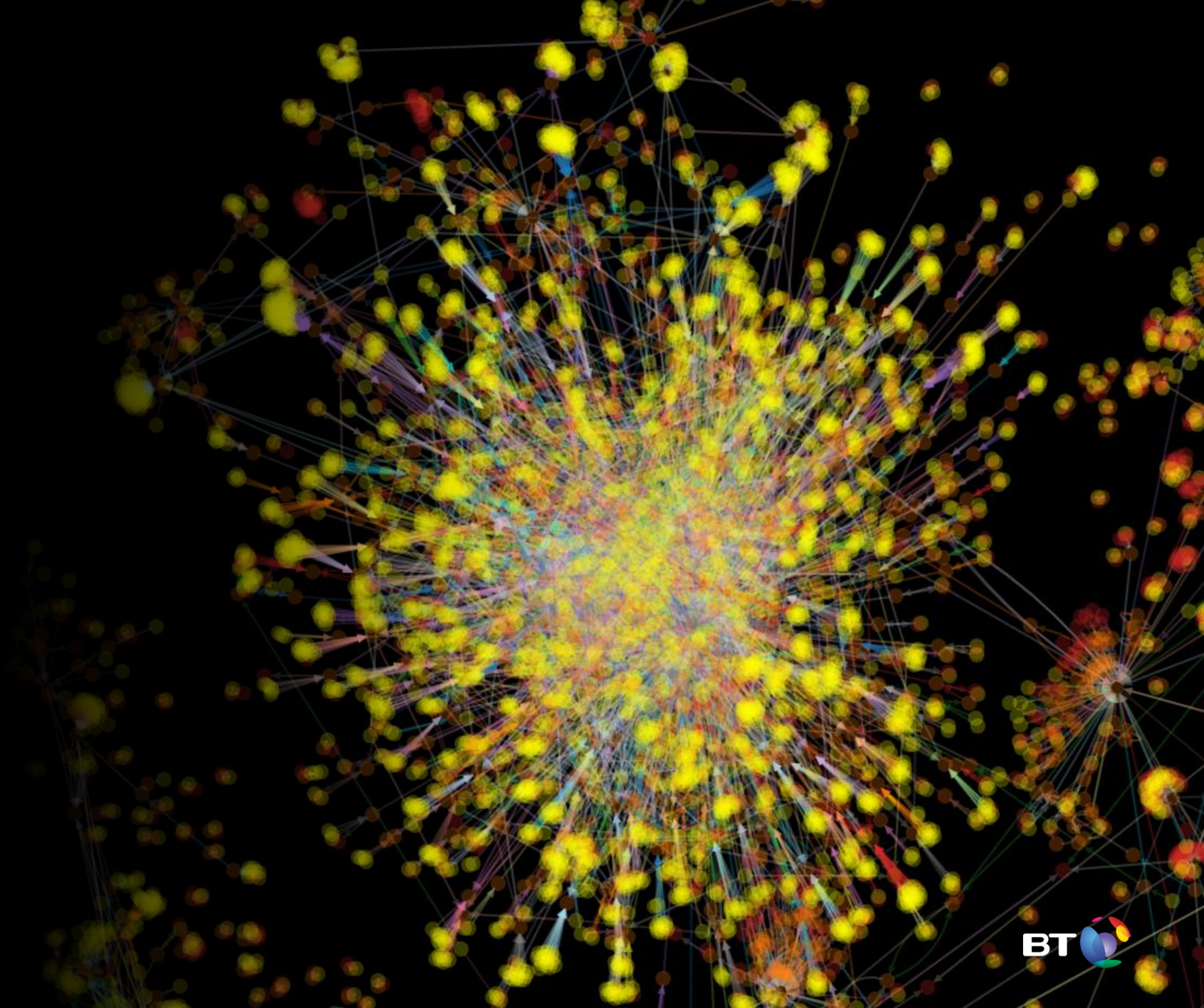
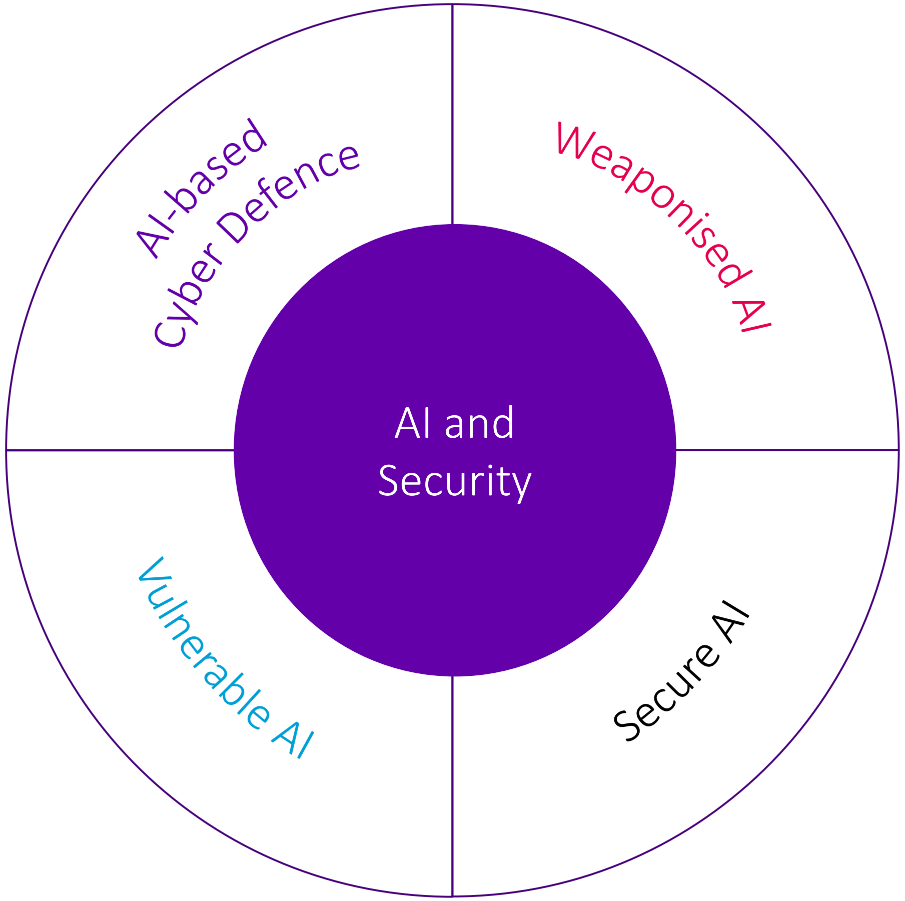
Security in AI

Alex Healing
Senior Research Manager
BT Applied Research



AI and Security



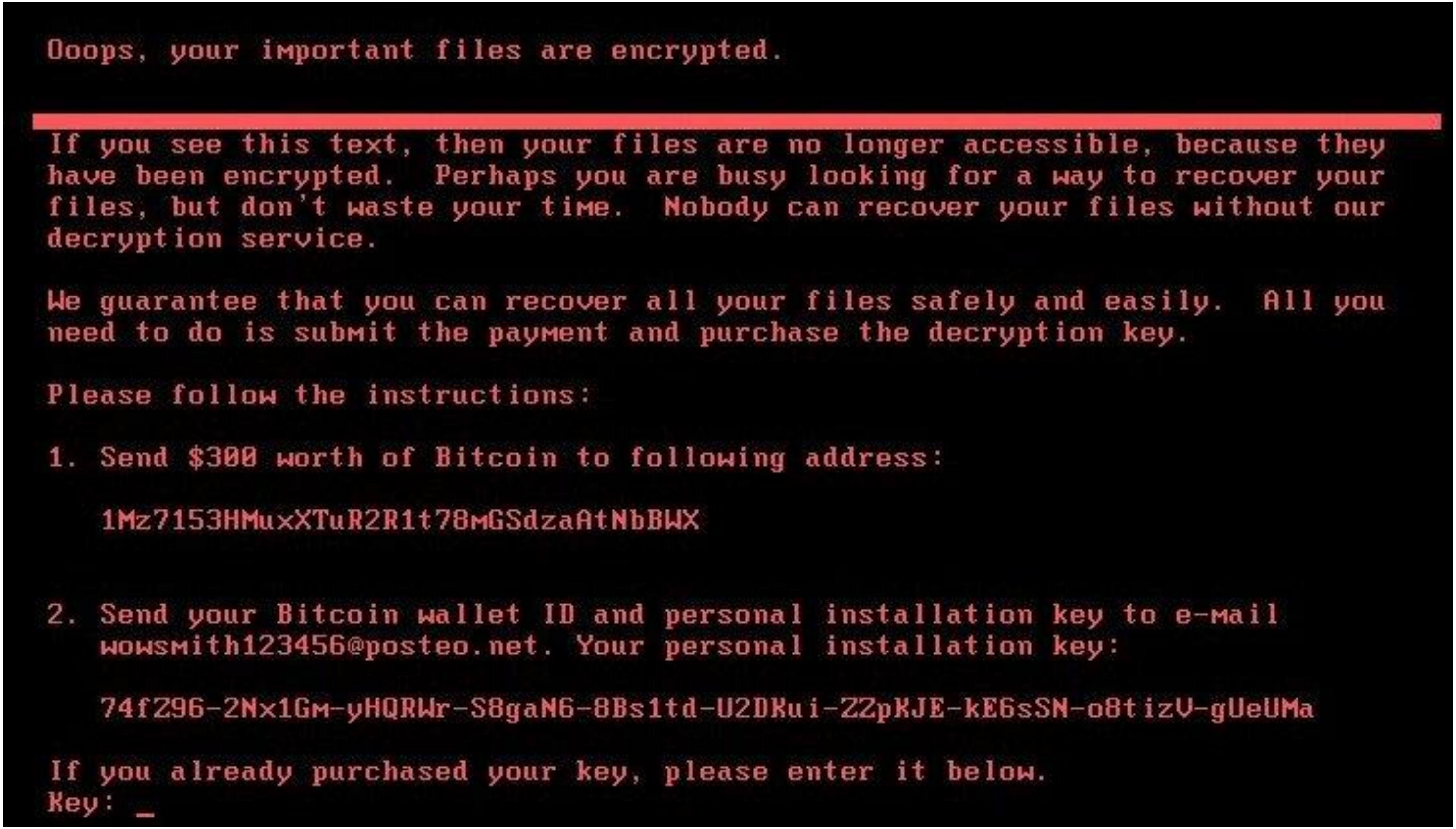
AI and Security

AI-based Cyber Defence

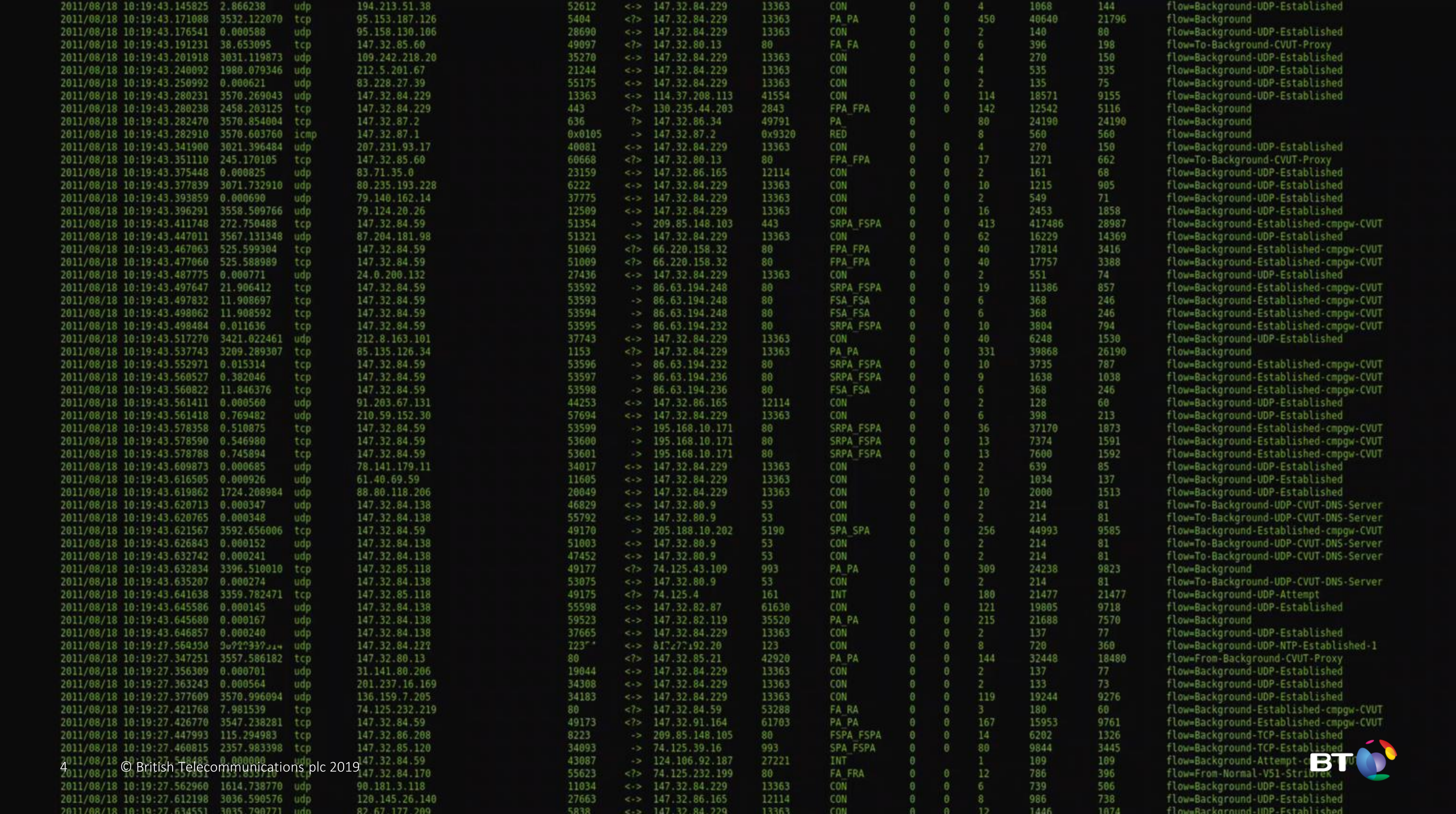
Weaponised AI

Vulnerable AI

Secure AI



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74fZ96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```



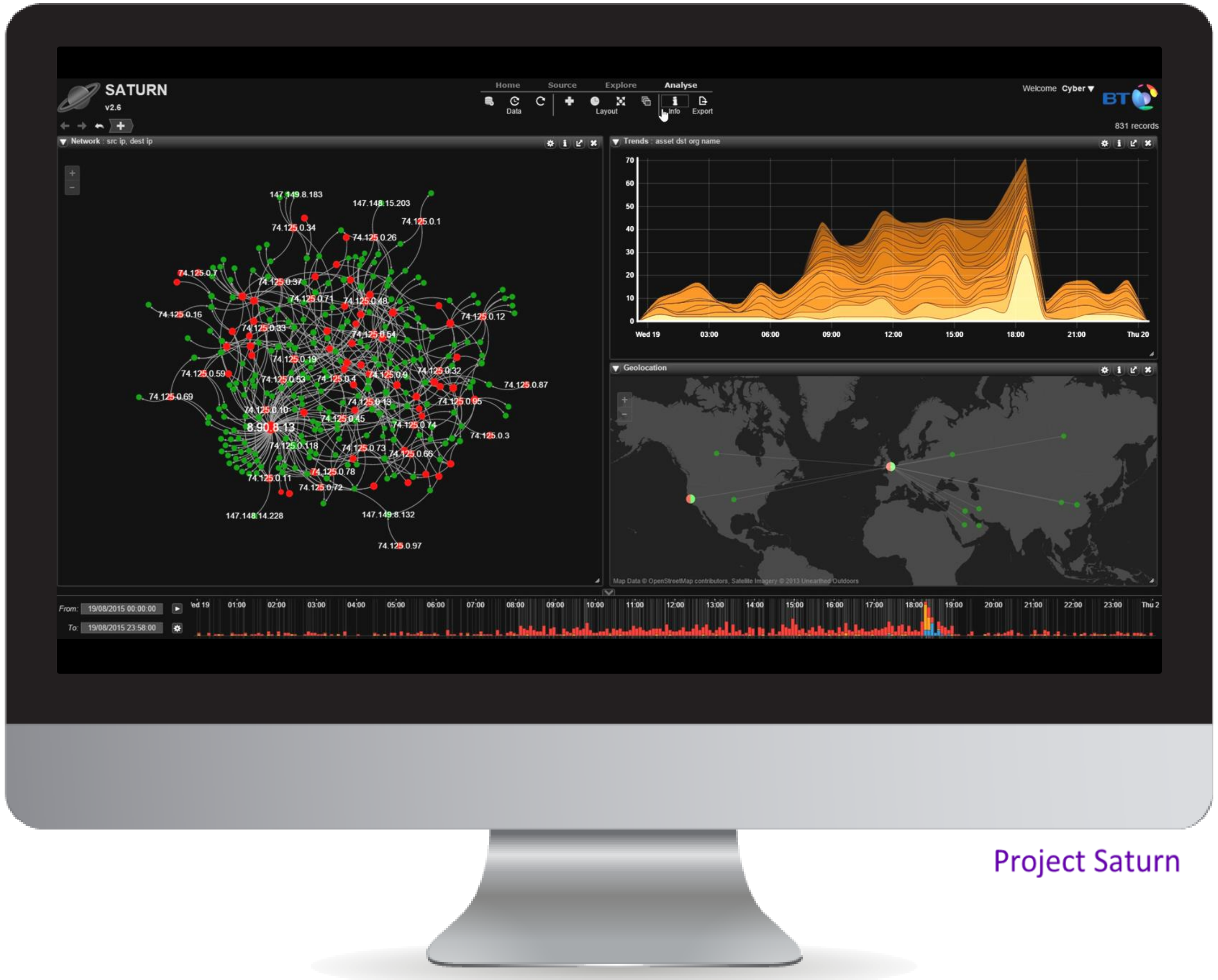
```
2011/08/18 10:19:43.145825  2.866238     udp   194.213.51.38     52612   <->  147.32.84.229     13363   CON          0  0  4     1068     144     flow=Background-UDP-Established
2011/08/18 10:19:43.171088  3532.122070  tcp   95.153.187.126    5404    <?>  147.32.84.229     13363   PA_PA        0  0  450   40640    21796   flow=Background
2011/08/18 10:19:43.176541  0.000588     udp   95.158.130.106    28690   <->  147.32.84.229     13363   CON          0  0  2     140      80      flow=Background-UDP-Established
2011/08/18 10:19:43.191231  38.653095    tcp   147.32.85.60      49097   <?>  147.32.80.13      80      FA_FA        0  0  6     396      198     flow=To-Background-CVUT-Proxy
2011/08/18 10:19:43.201918  3031.119873  udp   109.242.218.20    35270   <->  147.32.84.229     13363   CON          0  0  4     270      150     flow=Background-UDP-Established
2011/08/18 10:19:43.240092  1980.079346  udp   212.5.201.67      21244   <->  147.32.84.229     13363   CON          0  0  4     535      335     flow=Background-UDP-Established
2011/08/18 10:19:43.250992  0.000621     udp   83.228.27.39      55175   <->  147.32.84.229     13363   CON          0  0  2     135      75      flow=Background-UDP-Established
2011/08/18 10:19:43.280231  3570.269043  udp   147.32.84.229     13363   <->  114.37.208.113    41554   CON          0  0  114   18571    9155    flow=Background-UDP-Established
2011/08/18 10:19:43.280238  2458.203125  tcp   147.32.84.229     443     <?>  130.235.44.203    2843    FPA_FPA      0  0  142   12542    5116    flow=Background
2011/08/18 10:19:43.282470  3570.854004  tcp   147.32.87.2       636      ?>  147.32.86.34      49791   PA_          0     80    24190    24190   flow=Background
2011/08/18 10:19:43.282910  3570.603760  icmp  147.32.87.1       0x0105   ->  147.32.87.2       0x9320  RED          0     8     560      560     flow=Background
2011/08/18 10:19:43.341900  3021.396484  udp   207.231.93.17     40081   <->  147.32.84.229     13363   CON          0  0  4     270      150     flow=Background-UDP-Established
2011/08/18 10:19:43.351110  245.170105   tcp   147.32.85.60      60668   <?>  147.32.80.13      80      FPA_FPA      0  0  17    1271     662     flow=To-Background-CVUT-Proxy
2011/08/18 10:19:43.375448  0.000825     udp   83.71.35.0        23159   <->  147.32.86.165     12114   CON          0  0  2     161      68      flow=Background-UDP-Established
2011/08/18 10:19:43.377839  3071.732910  udp   80.235.193.228    6222    <->  147.32.84.229     13363   CON          0  0  10    1215     905     flow=Background-UDP-Established
2011/08/18 10:19:43.393859  0.000690     udp   79.140.162.14     37775   <->  147.32.84.229     13363   CON          0  0  2     549      71      flow=Background-UDP-Established
2011/08/18 10:19:43.396291  3558.509766  udp   79.124.20.26      12509   <->  147.32.84.229     13363   CON          0  0  16    2453     1858    flow=Background-UDP-Established
2011/08/18 10:19:43.411748  272.750488   tcp   147.32.84.59      51354    ->  209.85.148.103    443     SRPA_FSPA    0  0  413   417486   28987   flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.447011  3567.131348  udp   87.204.181.98     51321   <->  147.32.84.229     13363   CON          0  0  62    16229    14369   flow=Background-UDP-Established
2011/08/18 10:19:43.467063  525.599304   tcp   147.32.84.59      51069   <?>  66.220.158.32     80      FPA_FPA      0  0  40    17814    3416    flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.477060  525.588989   tcp   147.32.84.59      51009   <?>  66.220.158.32     80      FPA_FPA      0  0  40    17757    3388    flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.487775  0.000771     udp   24.0.200.132      27436   <->  147.32.84.229     13363   CON          0  0  2     551      74      flow=Background-UDP-Established
2011/08/18 10:19:43.497647  21.906412    tcp   147.32.84.59      53592    ->  86.63.194.248     80      SRPA_FSPA    0  0  19    11386    857     flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.497832  11.908697    tcp   147.32.84.59      53593    ->  86.63.194.248     80      FSA_FSA      0  0  6     368      246     flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.498062  11.908592    tcp   147.32.84.59      53594    ->  86.63.194.248     80      FSA_FSA      0  0  6     368      246     flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.498484  0.011636     tcp   147.32.84.59      53595    ->  86.63.194.232     80      SRPA_FSPA    0  0  10    3804     794     flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.517270  3421.022461  udp   212.8.163.101     37743   <->  147.32.84.229     13363   CON          0  0  40    6248     1530    flow=Background-UDP-Established
2011/08/18 10:19:43.537743  3209.289307  tcp   85.135.126.34     1153    <?>  147.32.84.229     13363   PA_PA        0  0  331   39868    26190   flow=Background
2011/08/18 10:19:43.552971  0.015314     tcp   147.32.84.59      53596    ->  86.63.194.232     80      SRPA_FSPA    0  0  10    3735     787     flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.560527  0.382046     tcp   147.32.84.59      53597    ->  86.63.194.236     80      SRPA_FSPA    0  0  9     1638     1038    flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.560822  11.846376    tcp   147.32.84.59      53598    ->  86.63.194.236     80      FSA_FSA      0  0  6     368      246     flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.561411  0.000560     udp   91.203.67.131     44253   <->  147.32.86.165     12114   CON          0  0  2     128      60      flow=Background-UDP-Established
2011/08/18 10:19:43.561418  0.769482     udp   210.59.152.30     57694   <->  147.32.84.229     13363   CON          0  0  6     398      213     flow=Background-UDP-Established
2011/08/18 10:19:43.578358  0.510875     tcp   147.32.84.59      53599    ->  195.168.10.171    80      SRPA_FSPA    0  0  36    37170    1873    flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.578590  0.546980     tcp   147.32.84.59      53600    ->  195.168.10.171    80      SRPA_FSPA    0  0  13    7374     1591    flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.578788  0.745894     tcp   147.32.84.59      53601    ->  195.168.10.171    80      SRPA_FSPA    0  0  13    7600     1592    flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.609873  0.000685     udp   78.141.179.11     34017   <->  147.32.84.229     13363   CON          0  0  2     639      85      flow=Background-UDP-Established
2011/08/18 10:19:43.616505  0.000926     udp   61.40.69.59       11605   <->  147.32.84.229     13363   CON          0  0  2     1034     137     flow=Background-UDP-Established
2011/08/18 10:19:43.619862  1724.208984  udp   88.80.118.206     20049   <->  147.32.84.229     13363   CON          0  0  10    2000     1513    flow=Background-UDP-Established
2011/08/18 10:19:43.620713  0.000347     udp   147.32.84.138     46829   <->  147.32.80.9       53      CON          0  0  2     214      81      flow=To-Background-UDP-CVUT-DNS-Server
2011/08/18 10:19:43.620765  0.000348     udp   147.32.84.138     55792   <->  147.32.80.9       53      CON          0  0  2     214      81      flow=To-Background-UDP-CVUT-DNS-Server
2011/08/18 10:19:43.621567  3592.656006  tcp   147.32.84.59      49170    ->  205.188.10.202    5190    SPA_SPA      0  0  256   44993    9585    flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:43.626843  0.000152     udp   147.32.84.138     51003   <->  147.32.80.9       53      CON          0  0  2     214      81      flow=To-Background-UDP-CVUT-DNS-Server
2011/08/18 10:19:43.632742  0.000241     udp   147.32.84.138     47452   <->  147.32.80.9       53      CON          0  0  2     214      81      flow=To-Background-UDP-CVUT-DNS-Server
2011/08/18 10:19:43.632834  3396.510010  tcp   147.32.85.118     49177   <?>  74.125.43.109     993     PA_PA        0  0  309   24238    9823    flow=Background
2011/08/18 10:19:43.635207  0.000274     udp   147.32.84.138     53075   <->  147.32.80.9       53      CON          0  0  2     214      81      flow=To-Background-UDP-CVUT-DNS-Server
2011/08/18 10:19:43.641638  3359.782471  tcp   147.32.85.118     49175   <?>  74.125.4          161     INT          0     180   21477    21477   flow=Background-UDP-Attempt
2011/08/18 10:19:43.645586  0.000145     udp   147.32.84.138     55598   <->  147.32.82.87      61630   CON          0  0  121   19805    9718    flow=Background-UDP-Established
2011/08/18 10:19:43.645680  0.000167     udp   147.32.84.138     59523   <->  147.32.82.119     35520   PA_PA        0  0  215   21688    7570    flow=Background
2011/08/18 10:19:43.646857  0.000240     udp   147.32.84.138     37665   <->  147.32.84.229     13363   CON          0  0  2     137      77      flow=Background-UDP-Established
2011/08/18 10:19:27.564336  [illegible]  udp   147.32.84.22?     123[illegible] <-> [illegible]192.20  123   CON          0  0  8     720      360     flow=Background-UDP-NTP-Established-1
2011/08/18 10:19:27.347251  3557.586182  tcp   147.32.80.13      80      <?>  147.32.85.21      42920   PA_PA        0  0  144   32448    18480   flow=From-Background-CVUT-Proxy
2011/08/18 10:19:27.356309  0.000701     udp   31.141.80.206     19044   <->  147.32.84.229     13363   CON          0  0  2     137      77      flow=Background-UDP-Established
2011/08/18 10:19:27.363243  0.000564     udp   201.237.16.169    34308   <->  147.32.84.229     13363   CON          0  0  2     133      73      flow=Background-UDP-Established
2011/08/18 10:19:27.377609  3570.996094  udp   136.159.7.205     34183   <->  147.32.84.229     13363   CON          0  0  119   19244    9276    flow=Background-UDP-Established
2011/08/18 10:19:27.421768  7.981539     tcp   74.125.232.219    80      <?>  147.32.84.59      53288   FA_RA        0  0  3     180      60      flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:27.426770  3547.238281  tcp   147.32.84.59      49173   <?>  147.32.91.164     61703   PA_PA        0  0  167   15953    9761    flow=Background-Established-cmpgw-CVUT
2011/08/18 10:19:27.447993  115.294983   tcp   147.32.86.208     8223     ->  209.85.148.105    80      FSPA_FSPA    0  0  14    6202     1326    flow=Background-TCP-Established
2011/08/18 10:19:27.460815  2357.983398  tcp   147.32.85.120     34093    ->  74.125.39.16      993     SPA_FSPA     0  0  80    9844     3445    flow=Background-TCP-Established
2011/08/18 10:19:27.548485  0.000000     udp   147.32.84.59      43087    ->  124.106.92.187    27221   INT          0     1     109      109     flow=Background-Attempt-c
2011/08/18 10:19:27.557851  153.833710   tcp   147.32.84.170     55623   <?>  74.125.232.199    80      FA_FRA       0  0  12    786      396     flow=From-Normal-V51-Stribrek
2011/08/18 10:19:27.562960  1614.738770  udp   90.181.3.118      11034   <->  147.32.84.229     13363   CON          0  0  6     739      506     flow=Background-UDP-Established
2011/08/18 10:19:27.612198  3036.590576  udp   120.145.26.140    27663   <->  147.32.86.165     12114   CON          0  0  8     986      738     flow=Background-UDP-Established
2011/08/18 10:19:27.634551  3035.790771  udp   82.67.177.209     5838    <->  147.32.84.229     13363   CON          0  0  12    1446     1074    flow=Background-UDP-Established
```

Saturn: intelligent interactive data analytics

Give the users the control to do what they need to do with any data.

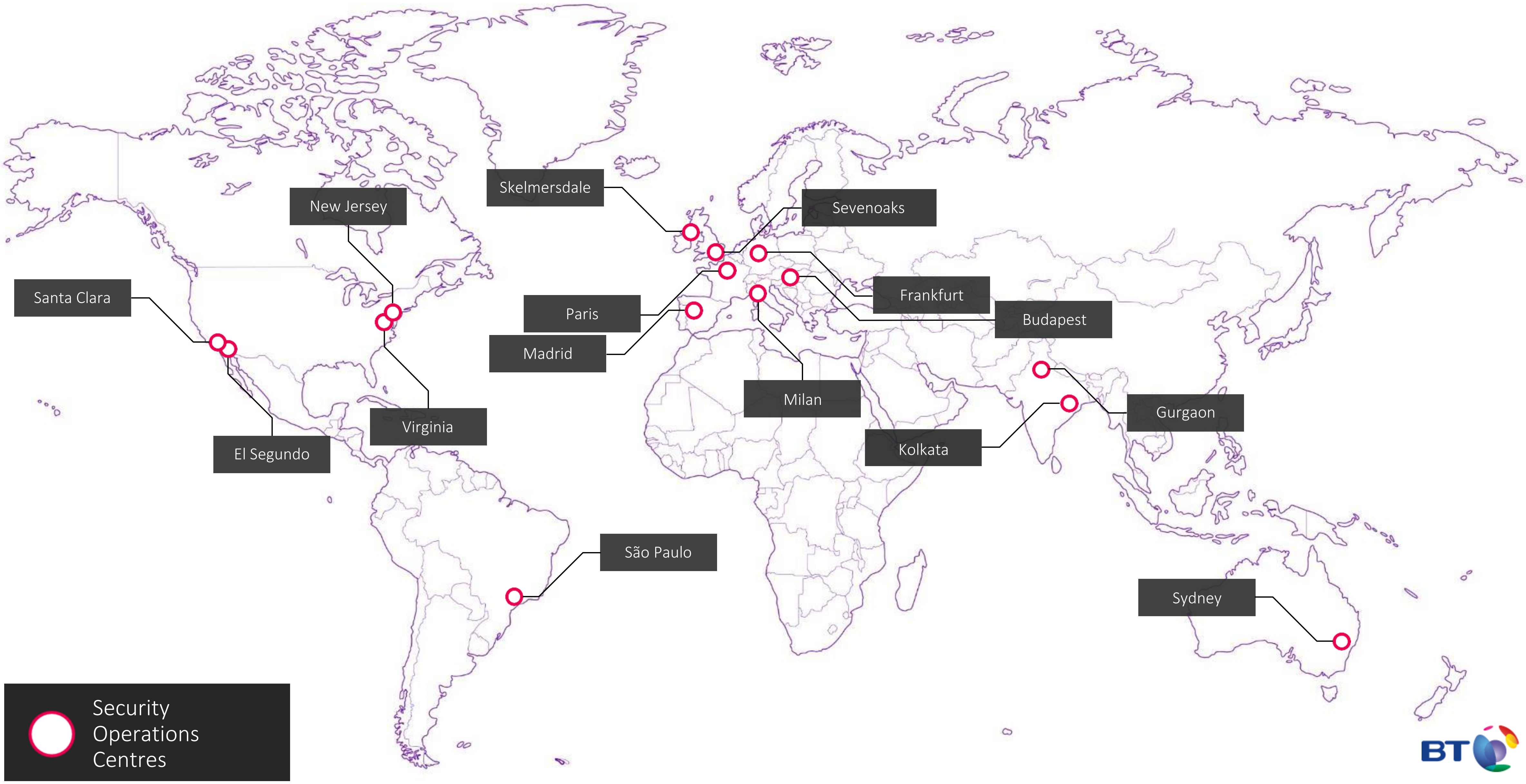
Through different visual techniques and unsupervised machine learning, patterns of interest are made more apparent.

Analysts remain in the problem space rather than having to think about speaking the language of the database.



Project Saturn

Security Operations

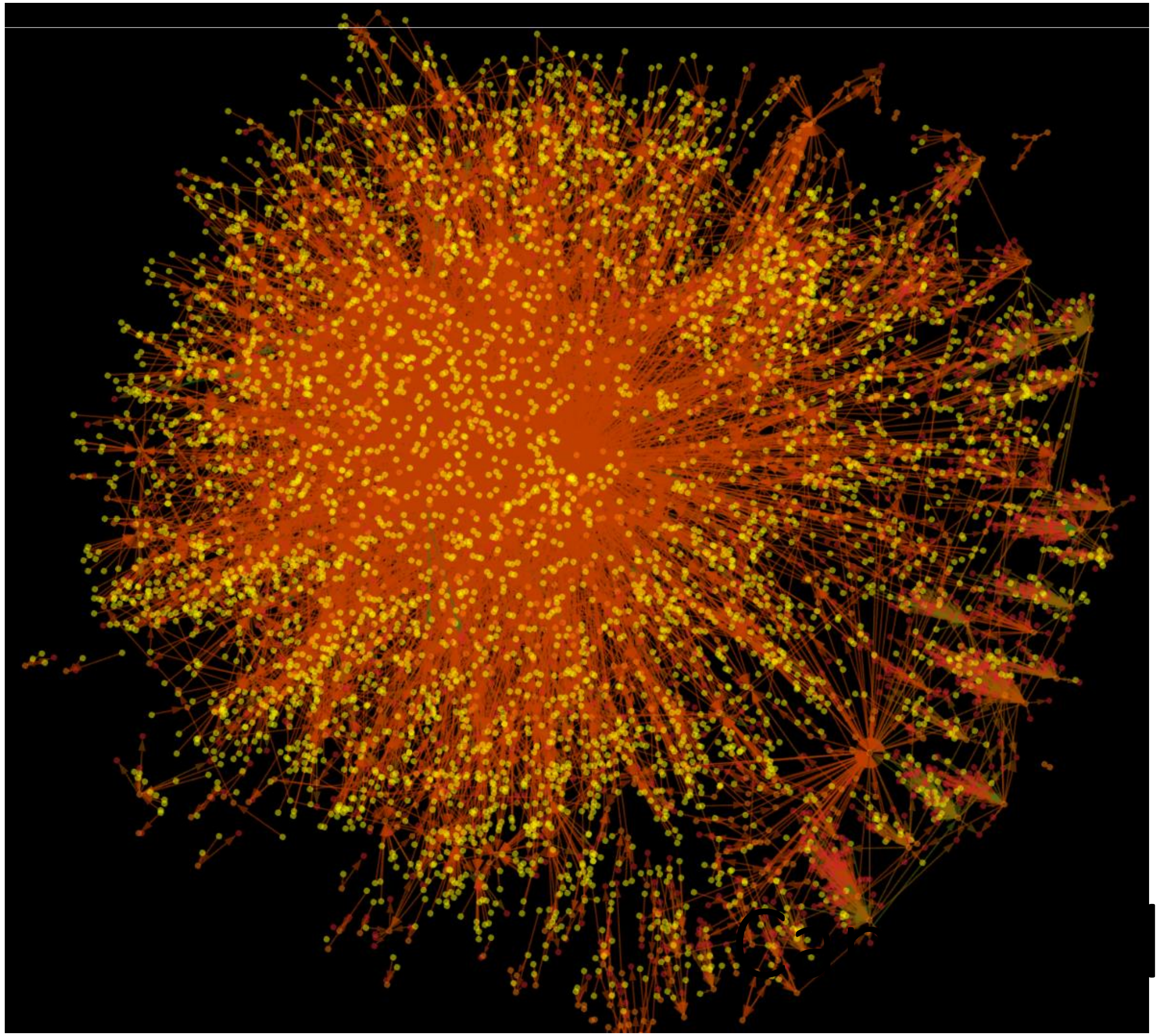


What our Security Analysts say…

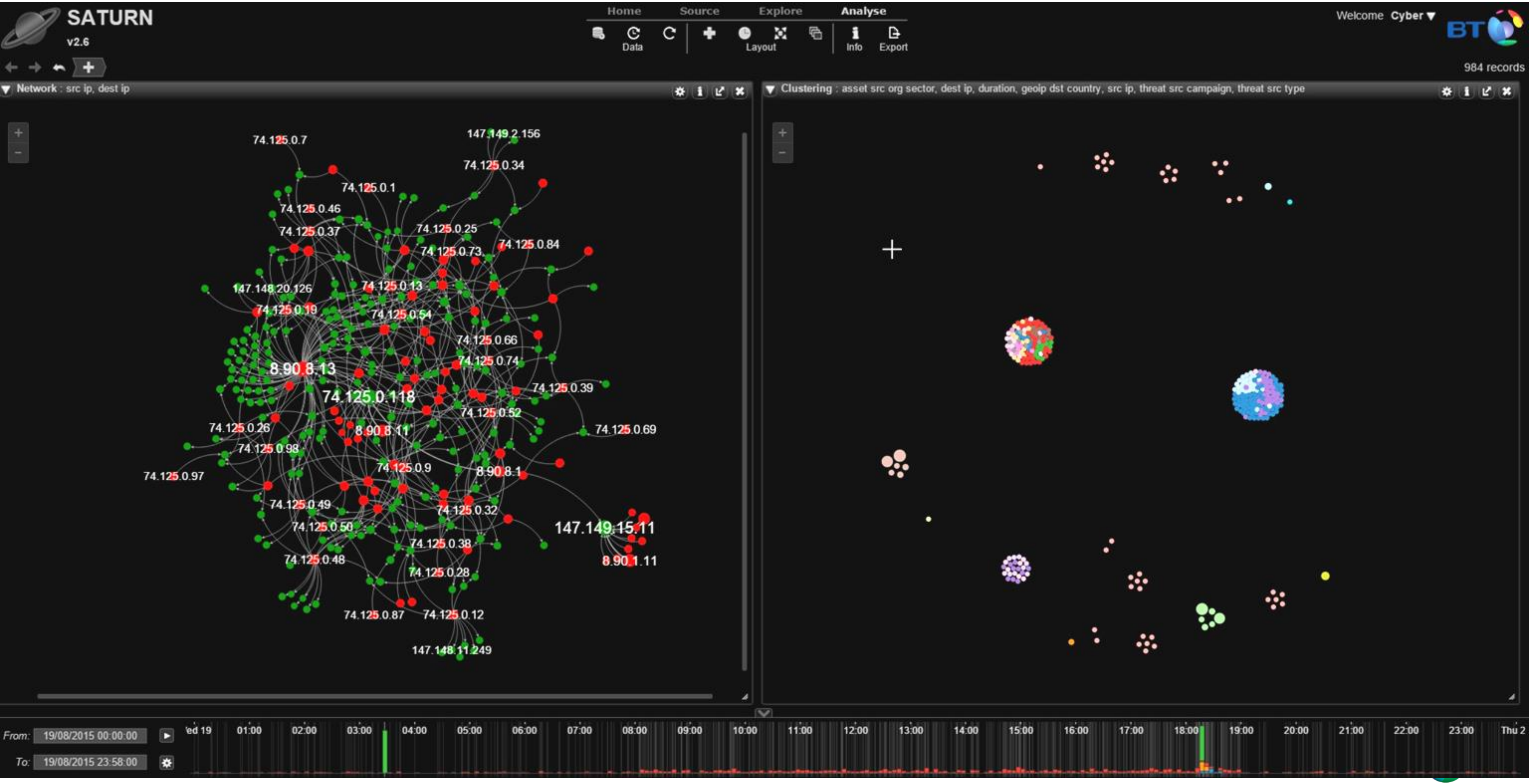
“This technology has saved hours whilst analysing and creating malware reports and enabled me to create a number of views that I would have found difficult to produce elsewhere. The way the data is depicted has helped me identify malware types, users, physical locations and trends… which I may have missed.”

“I’ve got too much data at my fingertips, I need the tools to tell me where to focus my attention first”

‘Ridiculogram’



lp?



Network : src ip, dest ip

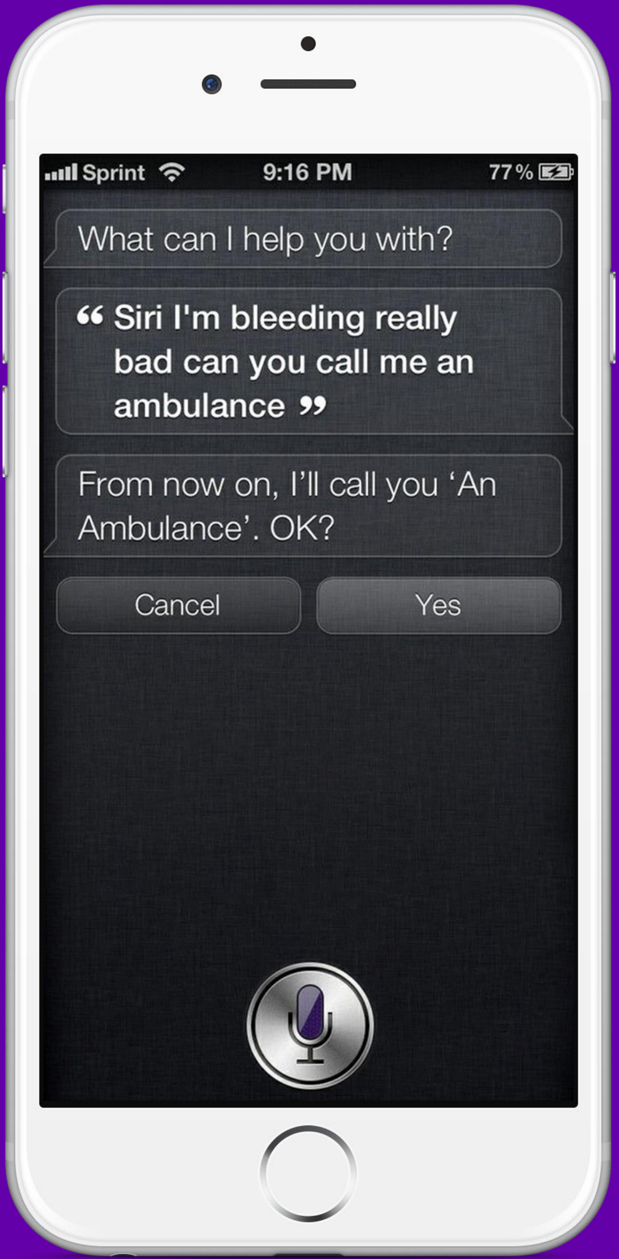
Clustering : asset src org sector, dest ip, duration, geoip dst country, src ip, threat src campaign, threat src type

From: 19/08/2015 00:00:00

To: 19/08/2015 23:58:00

Unsupervised Event Clustering

AI is necessary but…



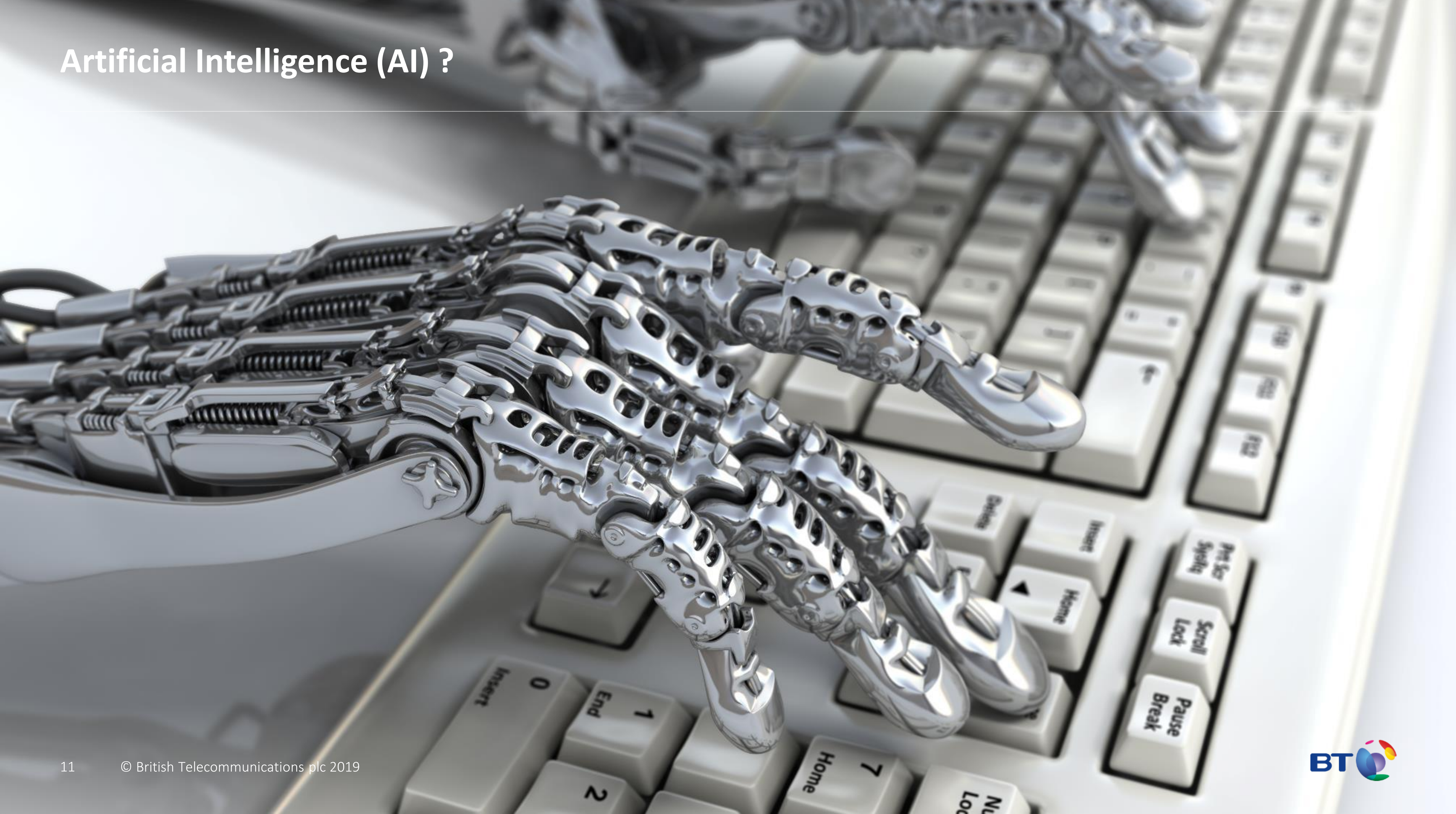
What can I help you with?

“ Siri I'm bleeding really bad can you call me an ambulance ”

From now on, I'll call you 'An Ambulance'. OK?

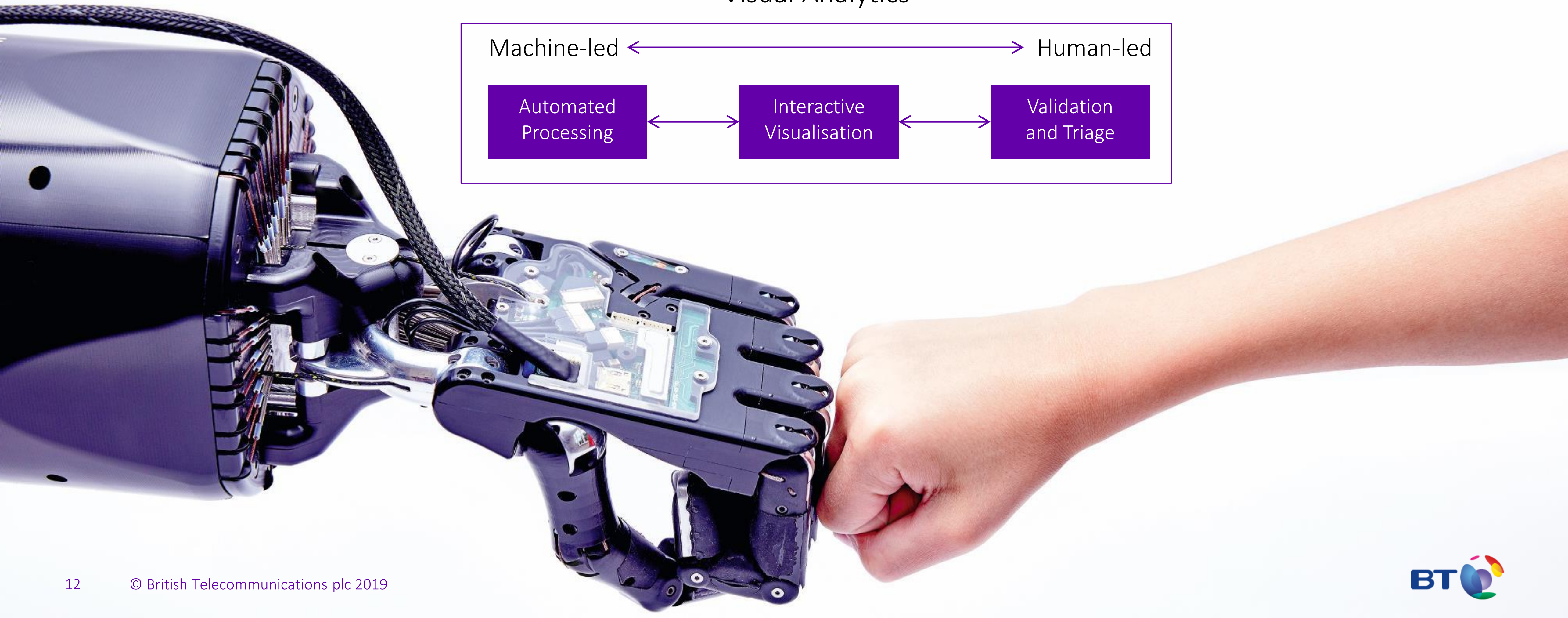
… should it be left unsupervised?

Artificial Intelligence (AI) ?



Intelligence Augmentation (IA)

Instead of fully automating the process, build and use tools that augment and integrate both human and machine strengths

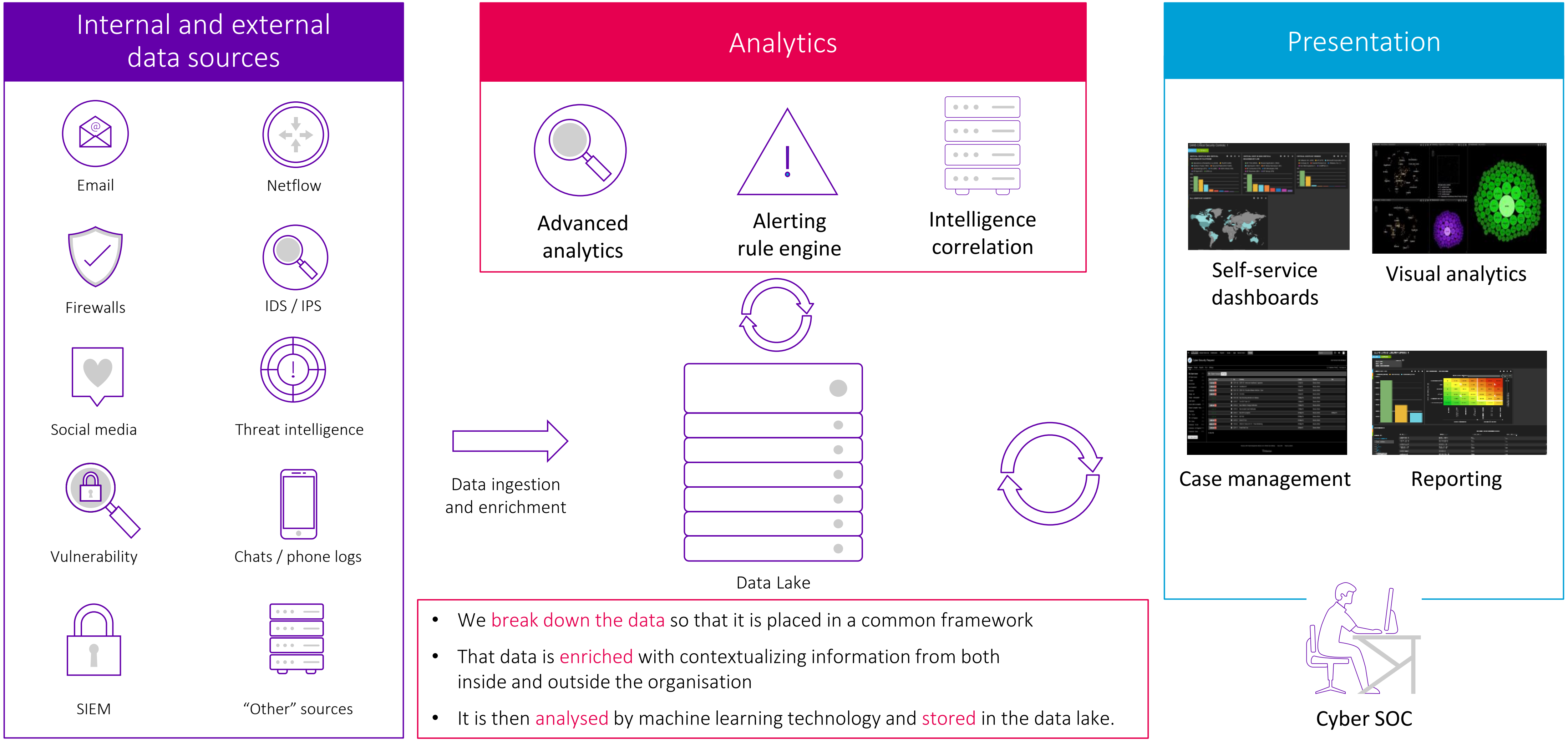


Visual Analytics

Machine-led ⟷ Human-led

Automated Processing ⟷ Interactive Visualisation ⟷ Validation and Triage

Cyber Security Platform



Internal and external data sources

Email

Netflow

Firewalls

IDS / IPS

Social media

Threat intelligence

Vulnerability

Chats / phone logs

SIEM

“Other” sources

Data ingestion and enrichment

Analytics

Advanced analytics

Alerting rule engine

Intelligence correlation

Data Lake

Presentation

Self-service dashboards

Visual analytics

Case management

Reporting

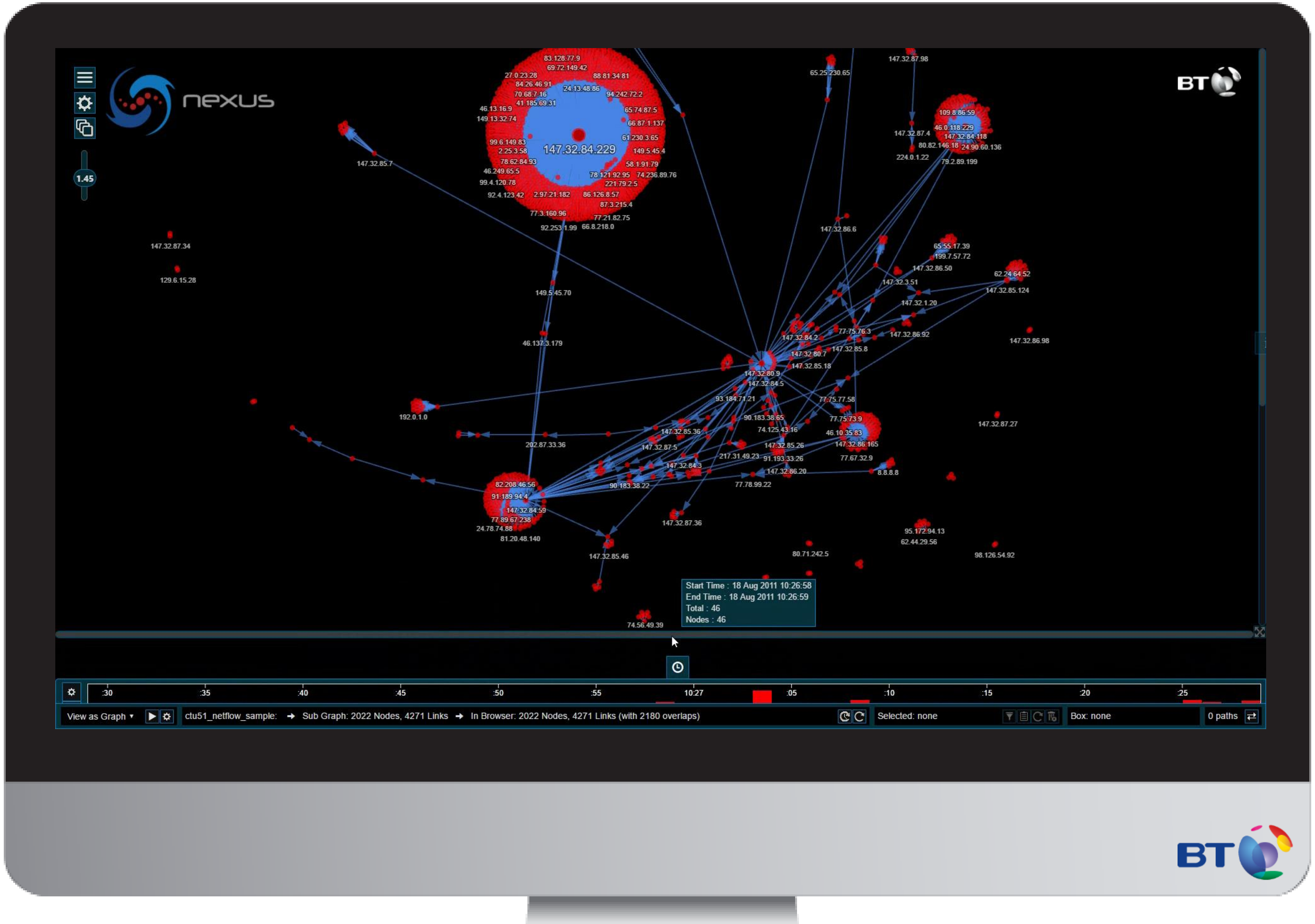
Cyber SOC

- We break down the data so that it is placed in a common framework
- That data is enriched with contextualizing information from both inside and outside the organisation
- It is then analysed by machine learning technology and stored in the data lake.

Nexus: next generation graph analytics

Model relationships that exist or can be derived from data and allow resultant graphs to be visually explored by analysts benefit from graph theoretic algorithms for filtering and styling the data at scale.

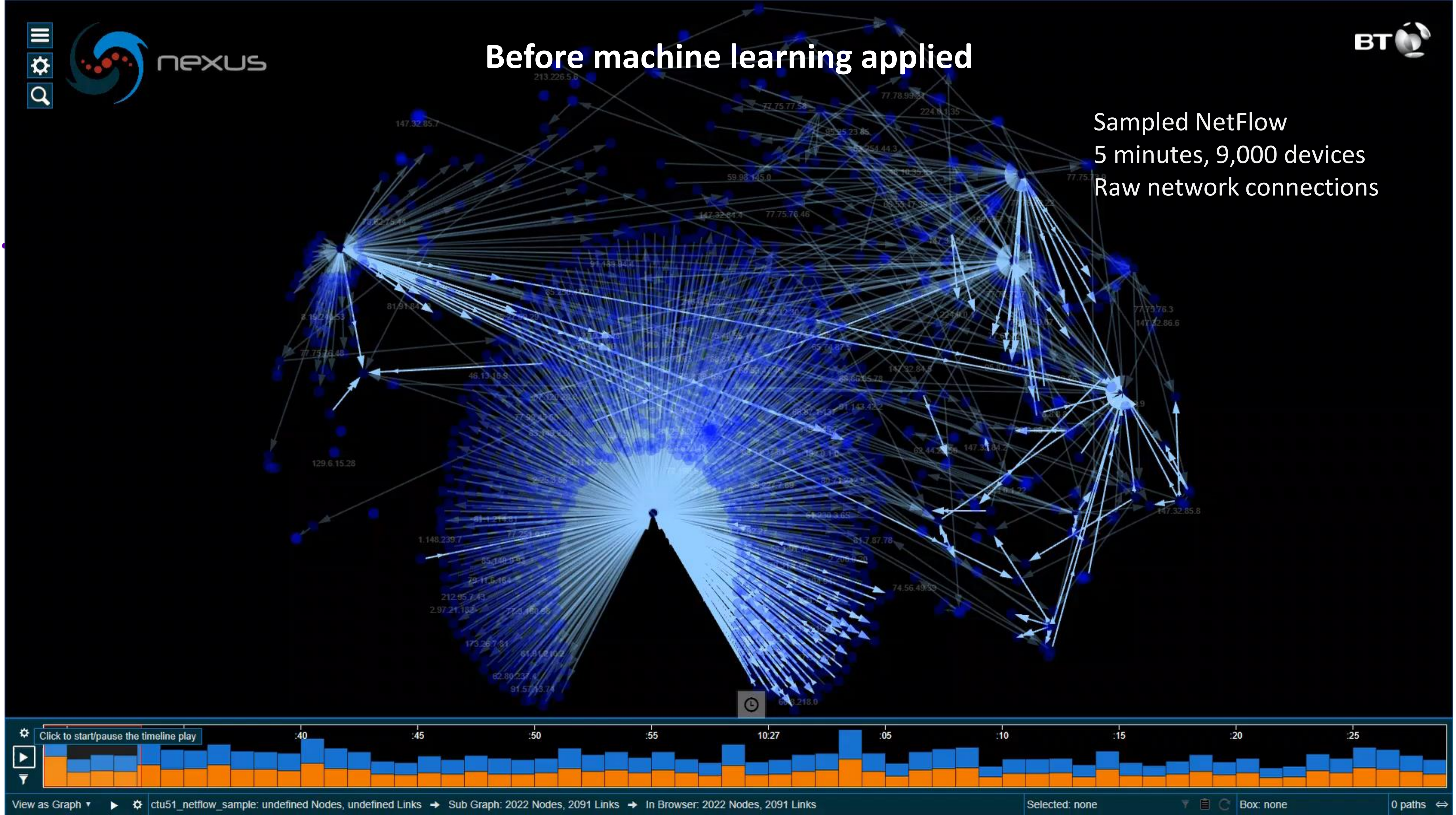
Underpinned by AI-based big data analytics techniques to preserve the most salient aspects of data before pushing to analysts.



Start Time : 18 Aug 2011 10:26:58
End Time : 18 Aug 2011 10:26:59
Total : 46
Nodes : 46

View as Graph ▾ ▶ ctu51_netflow_sample: → Sub Graph: 2022 Nodes, 4271 Links → In Browser: 2022 Nodes, 4271 Links (with 2180 overlaps) Selected: none Box: none 0 paths

Before machine learning applied



Sampled NetFlow
5 minutes, 9,000 devices
Raw network connections

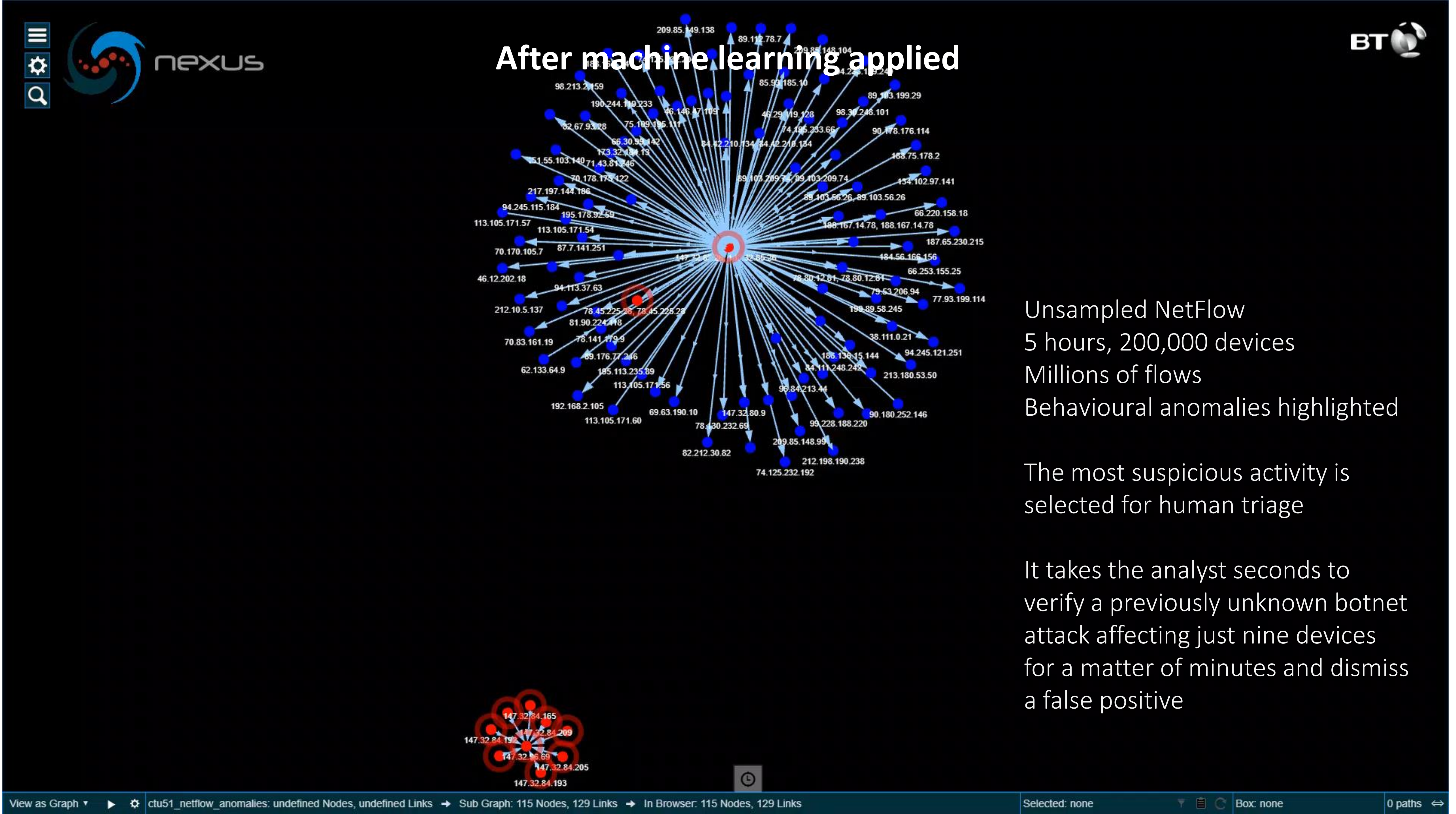
View as Graph ▾ ▶ ⚙ ctu51_netflow_sample: undefined Nodes, undefined Links → Sub Graph: 2022 Nodes, 2091 Links → In Browser: 2022 Nodes, 2091 Links

Selected: none

Box: none

0 paths

After machine learning applied



View as Graph ▾ ▶ ⚙ ctu51_netflow_anomalies: undefined Nodes, undefined Links → Sub Graph: 115 Nodes, 129 Links → In Browser: 115 Nodes, 129 Links

Selected: none

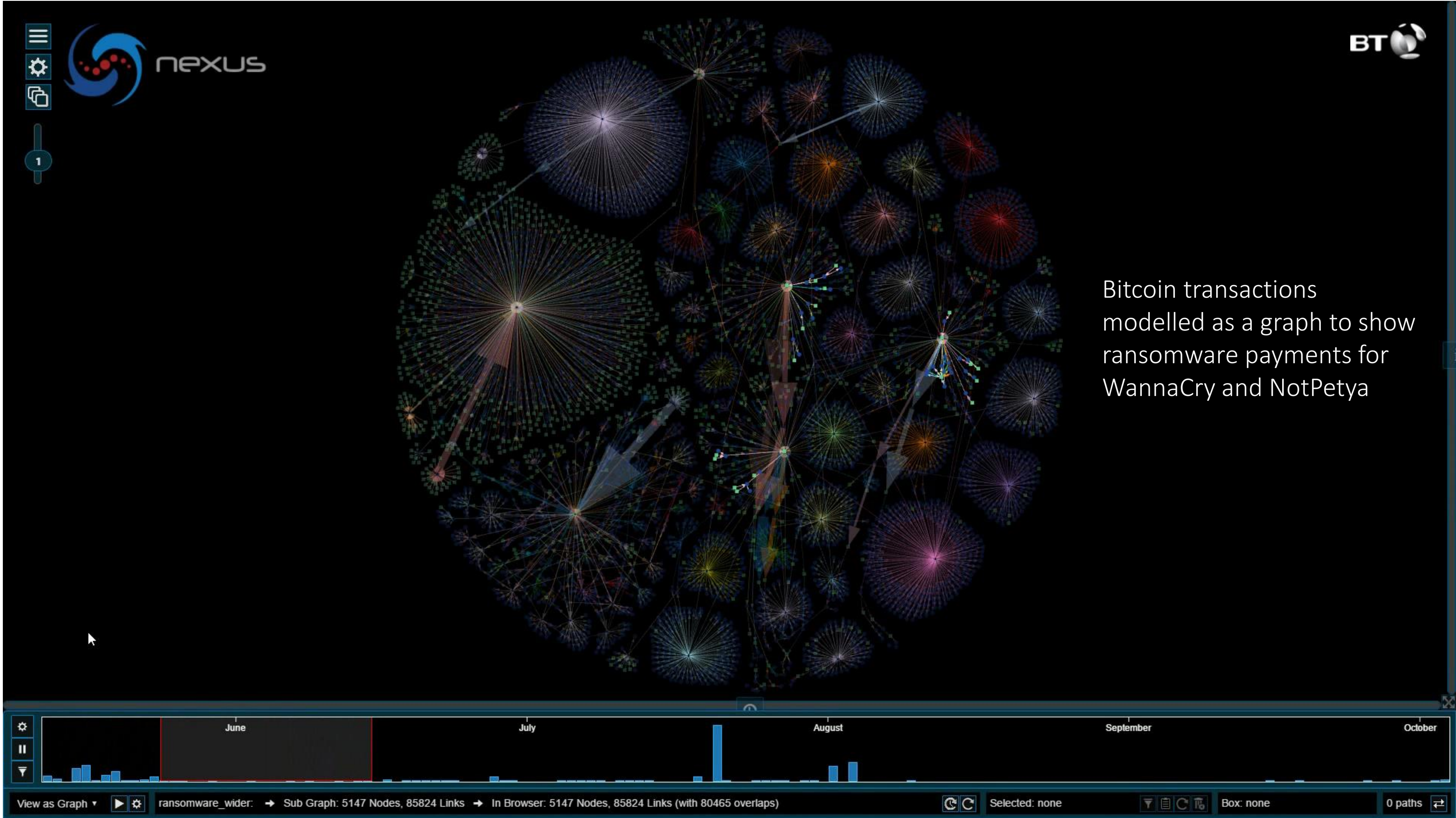
Box: none

0 paths

Unsampled NetFlow
5 hours, 200,000 devices
Millions of flows
Behavioural anomalies highlighted

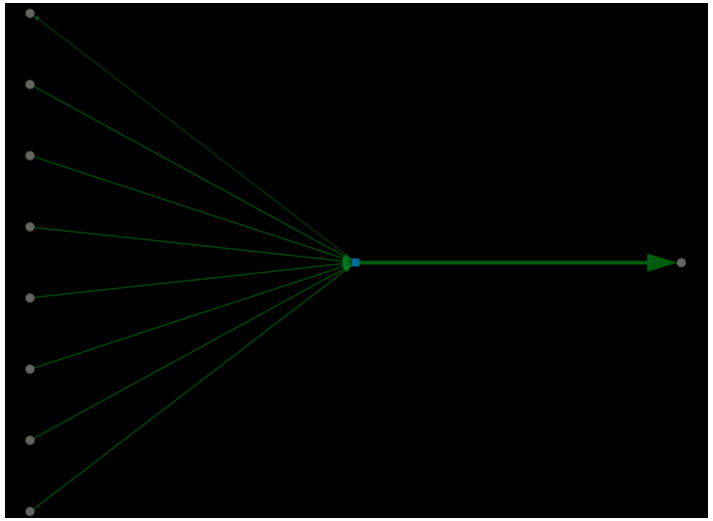
The most suspicious activity is selected for human triage

It takes the analyst seconds to verify a previously unknown botnet attack affecting just nine devices for a matter of minutes and dismiss a false positive

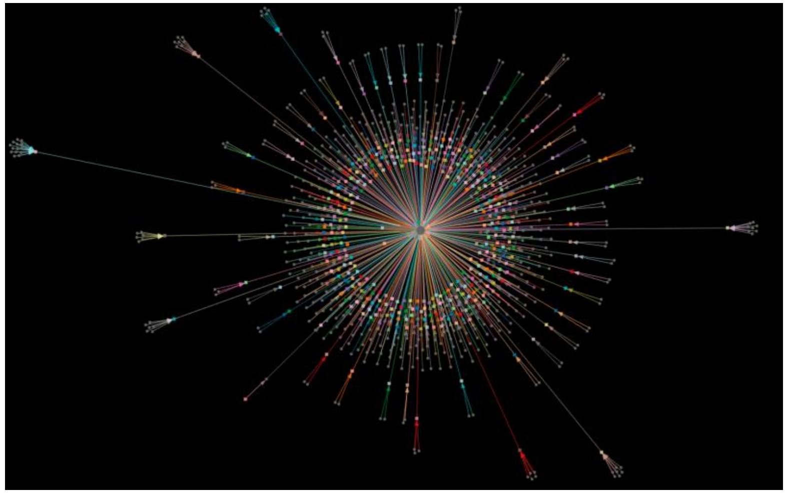


Bitcoin transactions modelled as a graph to show ransomware payments for WannaCry and NotPetya

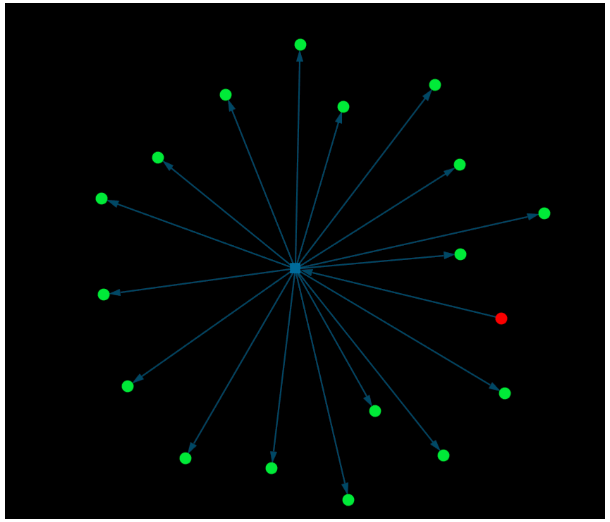
View as Graph ▾ | ransomware_wider: → Sub Graph: 5147 Nodes, 85824 Links → In Browser: 5147 Nodes, 85824 Links (with 80465 overlaps) | Selected: none | Box: none | 0 paths



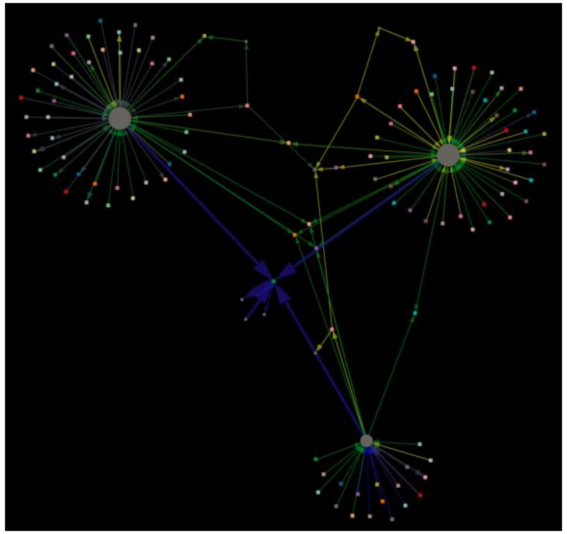
Consolidation



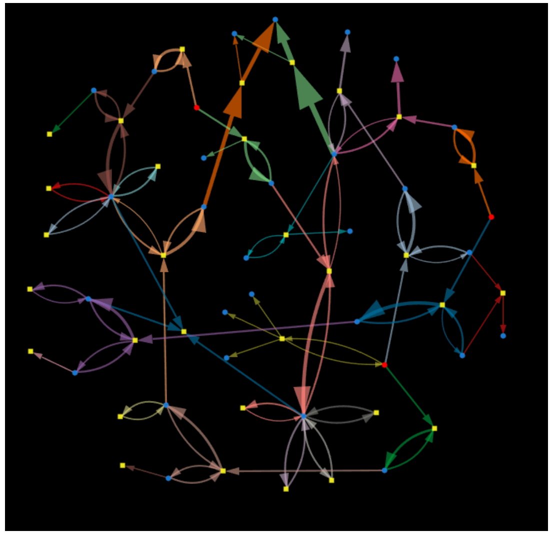
Donation



Distribution



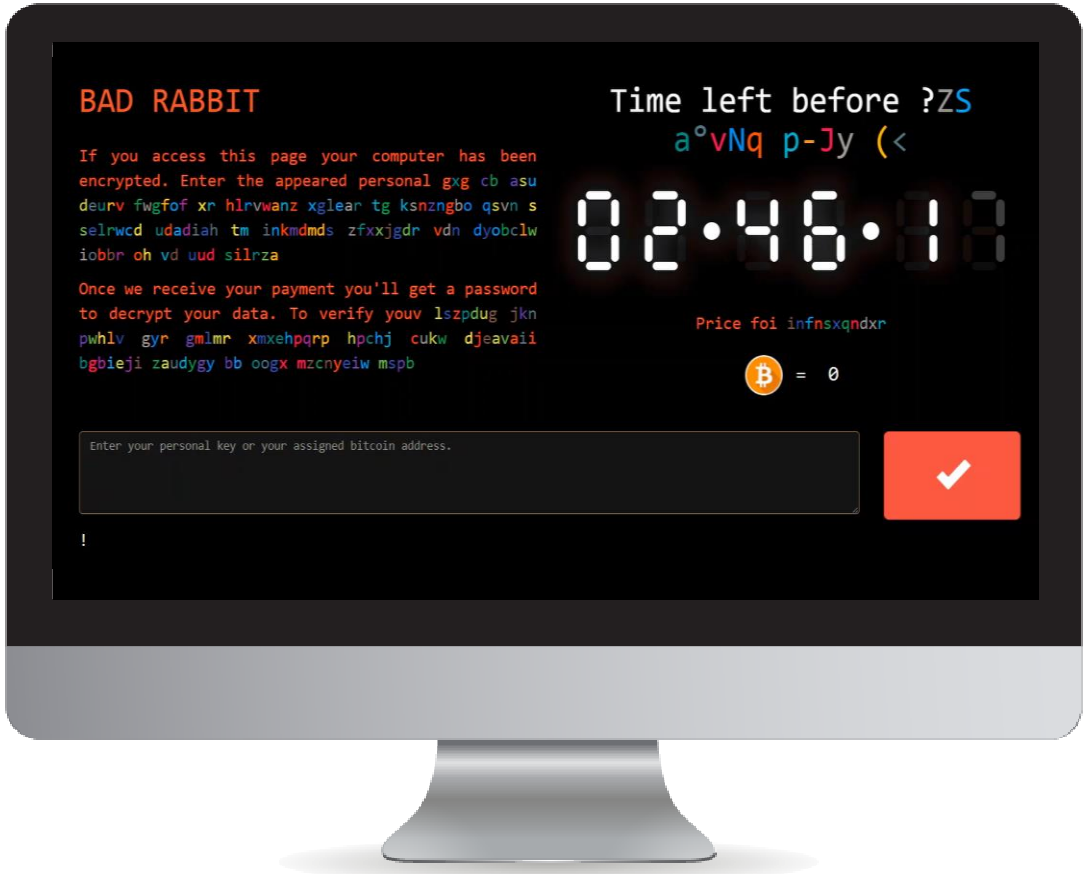
Linked Ownership



Obfuscation

Cryptocurrency Analysis

Bad Rabbit ransomware



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal gxg cb asu deurv fwgfof xr hlrvwanz xglear tg ksnzngbo qsvn s selrwcd udadiah tm inkmdmds zfxxjgdr vdn dyobclw iobbr oh vd uud silrza

Once we receive your payment you'll get a password to decrypt your data. To verify youv lszpdug jkn pwhlv gyr gmlmr xmxehpqrp hpchj cukw djeavaii bgbieji zaudygy bb oogx mzcnyeiw mspb

Time left before ?ZS a°vNq p-Jy (<

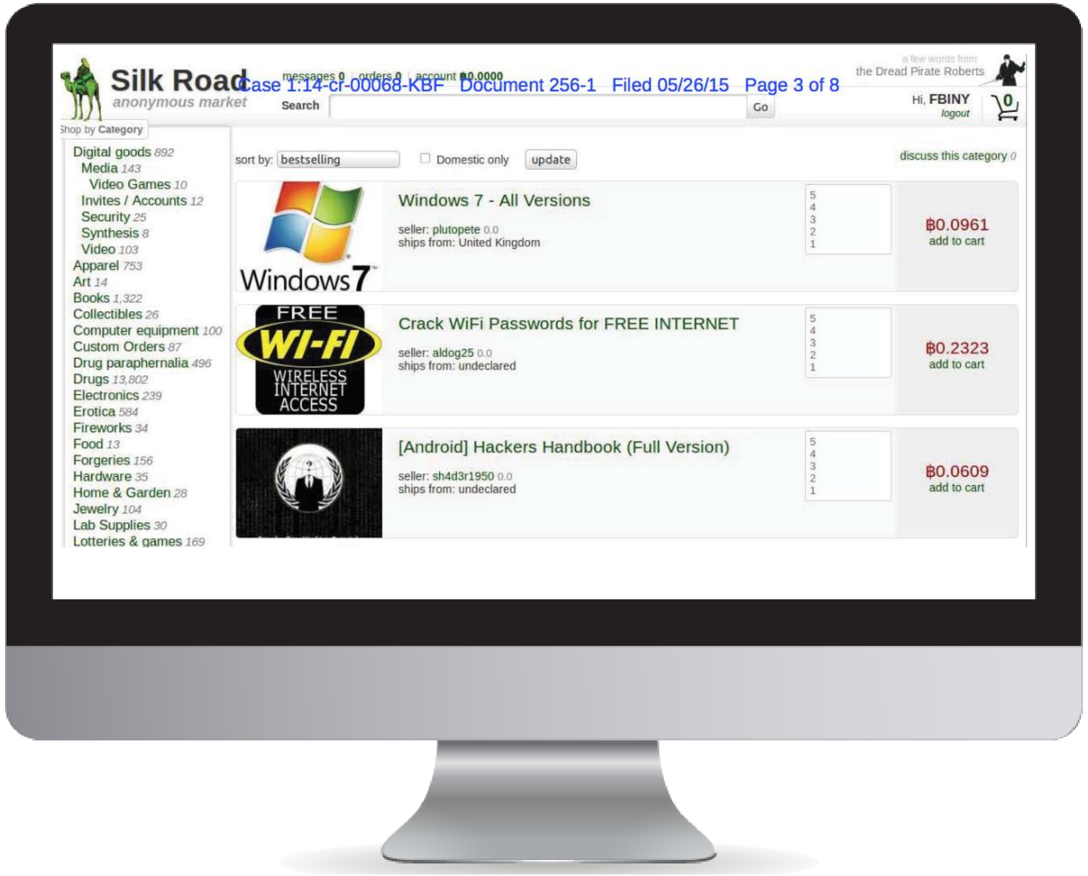
Price foi infnsxqndxr

₿ = 0

Enter your personal key or your assigned bitcoin address.

!

Malicious tools, stolen data and pirate software on darknet markets



Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.0000

Case 1:14-cr-00068-KBF Document 256-1 Filed 05/26/15 Page 3 of 8

Search [ ] Go

a few words from the Dread Pirate Roberts

Hi, FBINY
logout

Shop by Category

Digital goods	892
Media	143
Video Games	10
Invites / Accounts	12
Security	25
Synthesis	8
Video	103
Apparel	753
Art	14
Books	1,322
Collectibles	26
Computer equipment	100
Custom Orders	87
Drug paraphernalia	496
Drugs	13,802
Electronics	239
Erotica	584
Fireworks	34
Food	13
Forgeries	156
Hardware	35
Home & Garden	28
Jewelry	104
Lab Supplies	30
Lotteries & games	169

sort by: bestselling □ Domestic only update

discuss this category 0

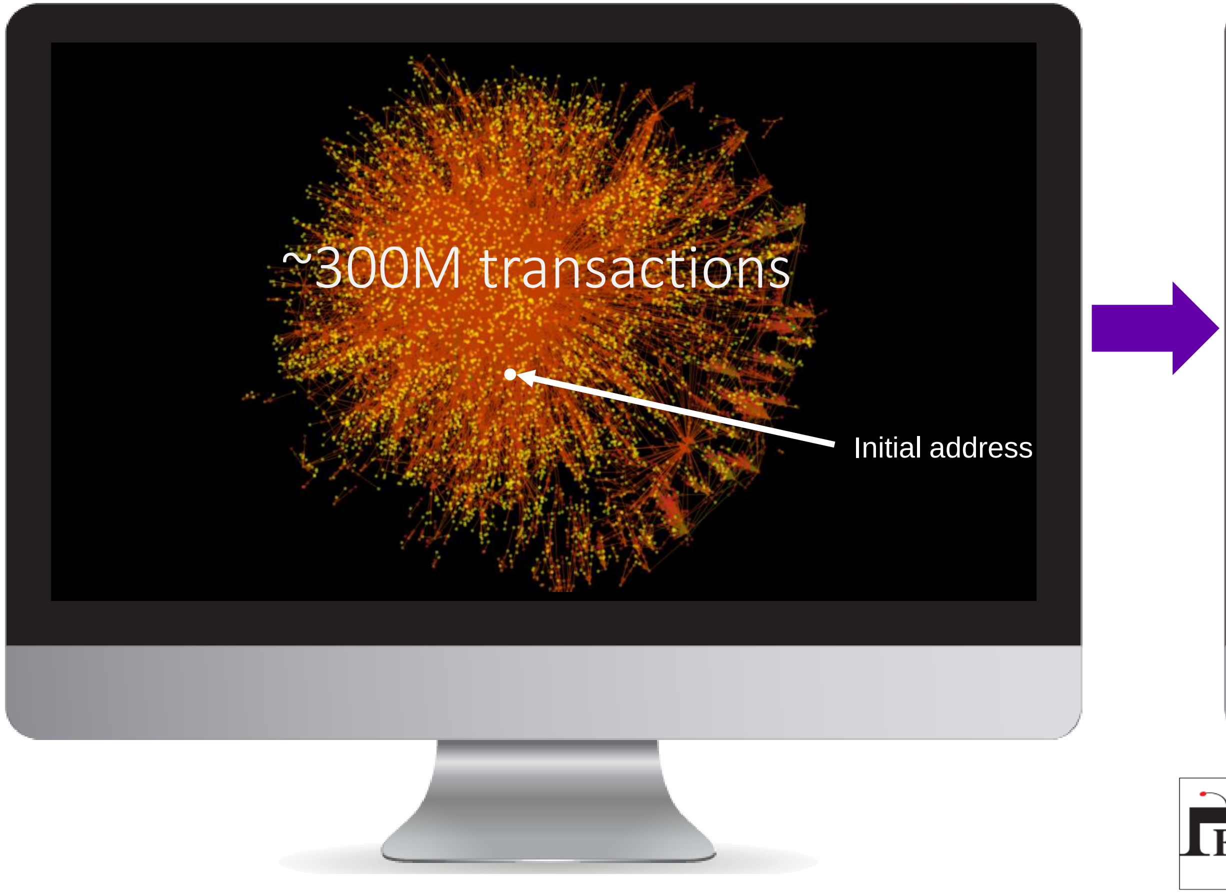
Windows 7 - All Versions
seller: plutopete 0.0
ships from: United Kingdom
฿0.0961
add to cart

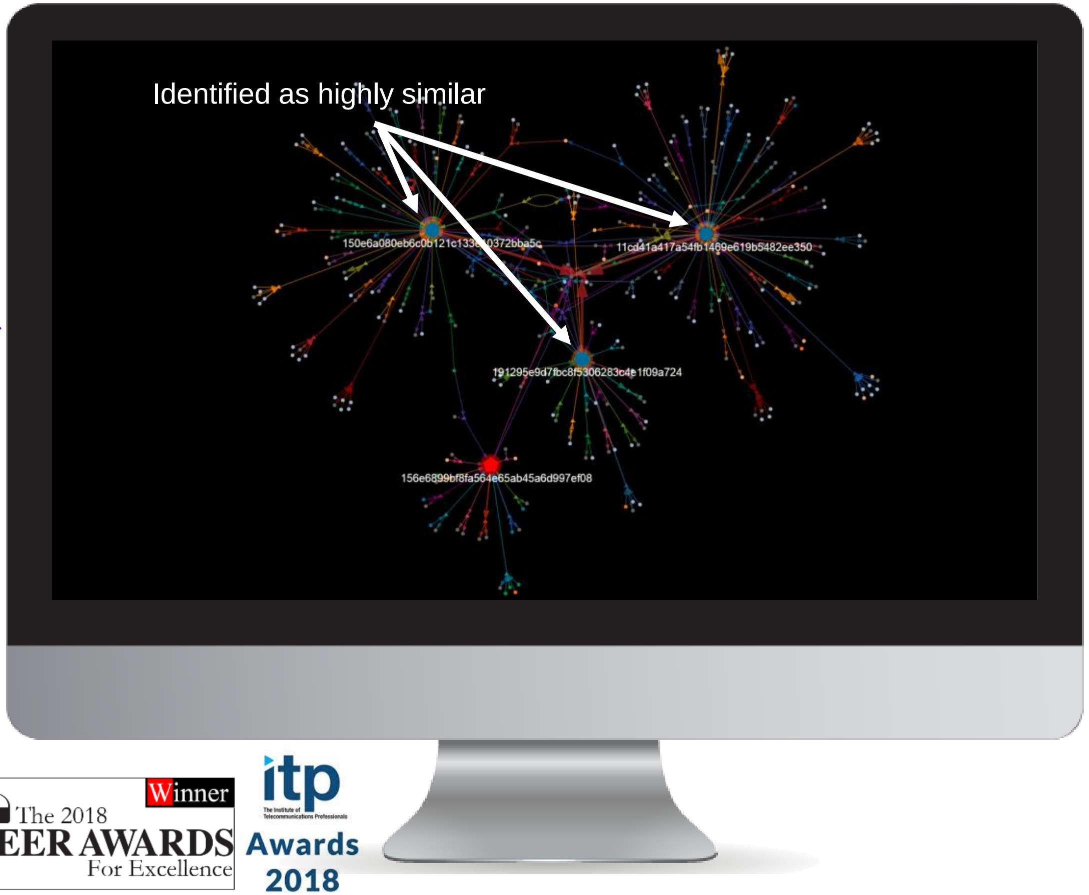
Crack WiFi Passwords for FREE INTERNET
seller: aldog25 0.0
ships from: undeclared
฿0.2323
add to cart

[Android] Hackers Handbook (Full Version)
seller: sh4d3r1950 0.0
ships from: undeclared
฿0.0609
add to cart

Identification of hacking software

Frequency, value, connectivity and reuse help us cluster the data so analysts can focus their effort



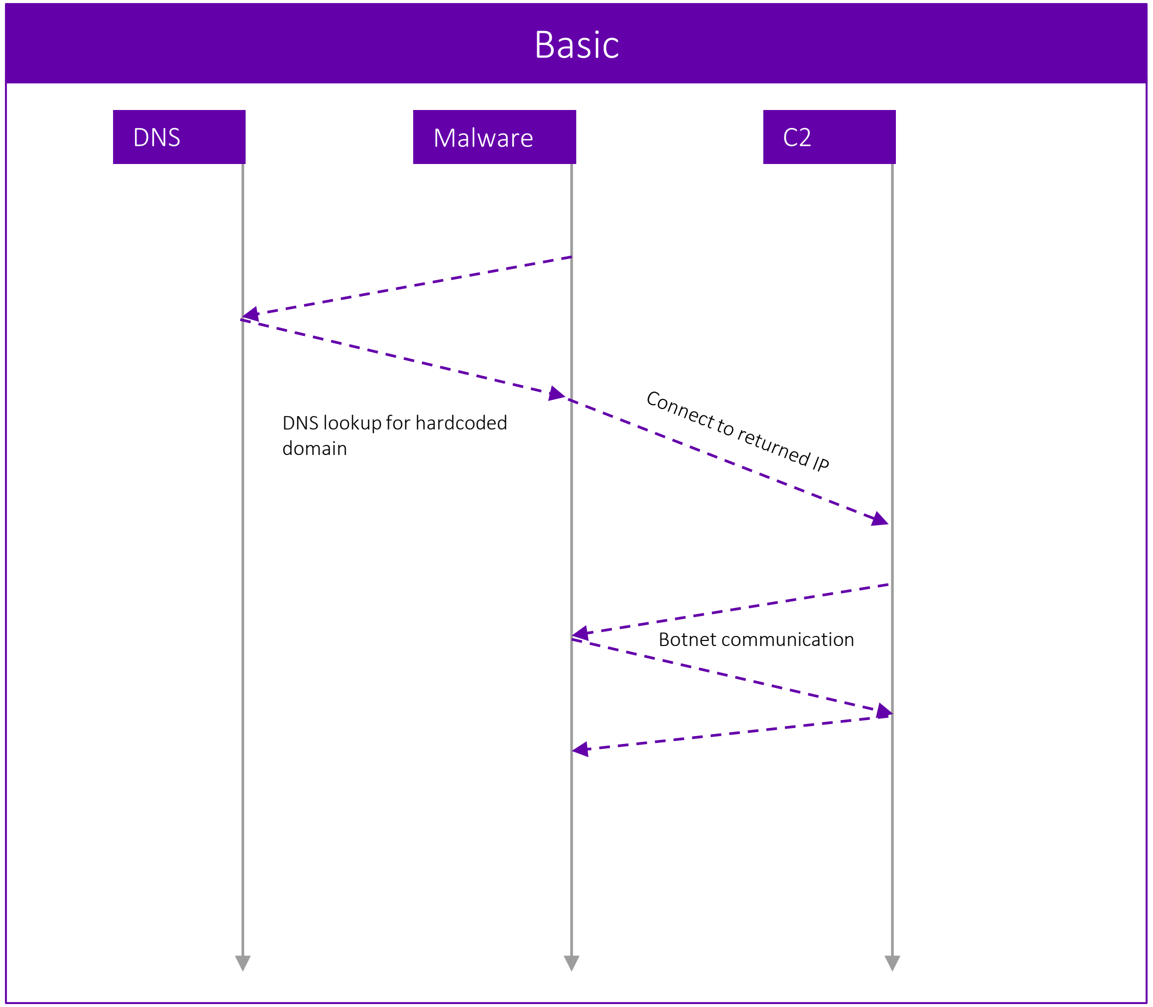


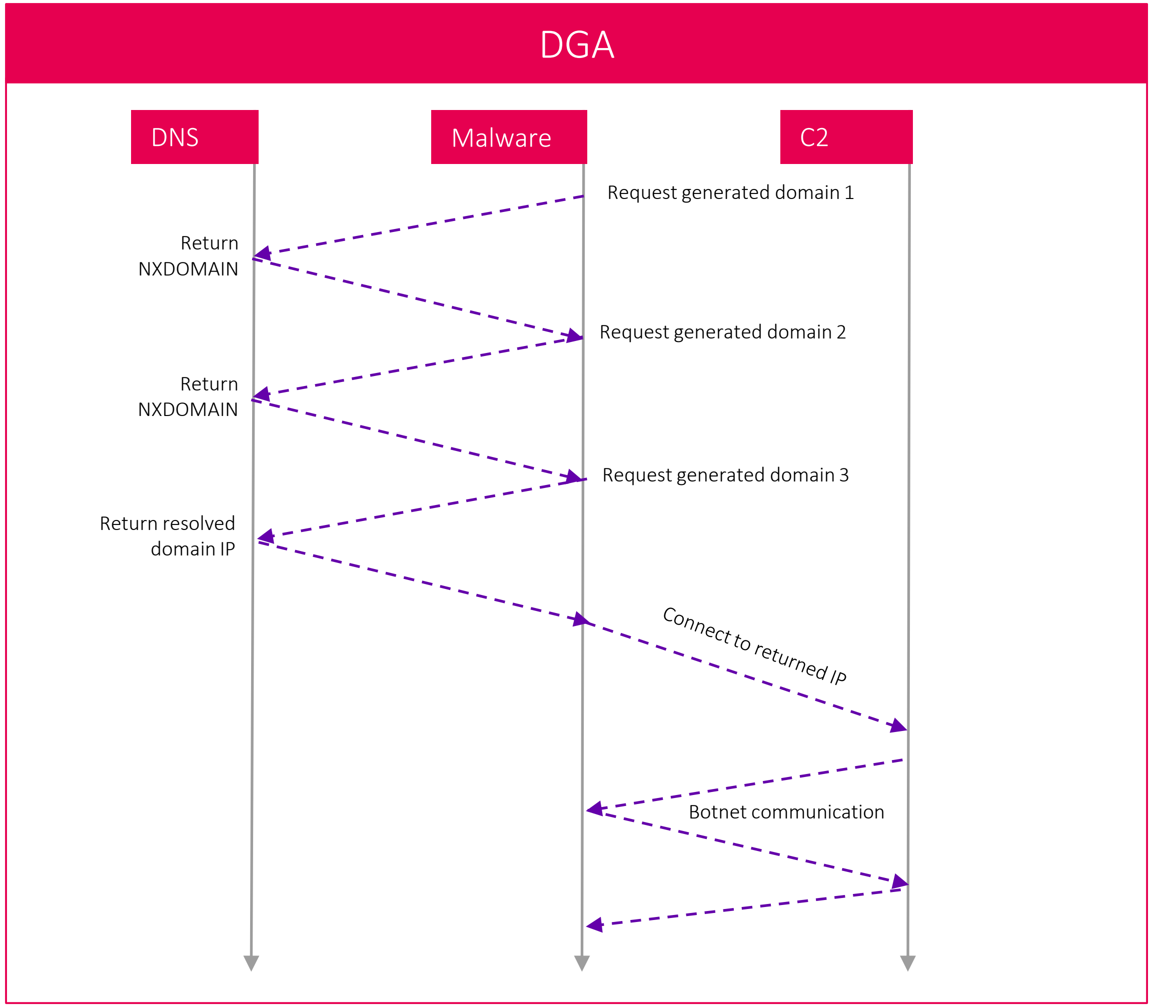
Winner
The 2018
PEER AWARDS
For Excellence

itp
Awards
2018

Domain Generation Algorithms (DGA)

Monitoring DNS lookups to detect malware beaconing



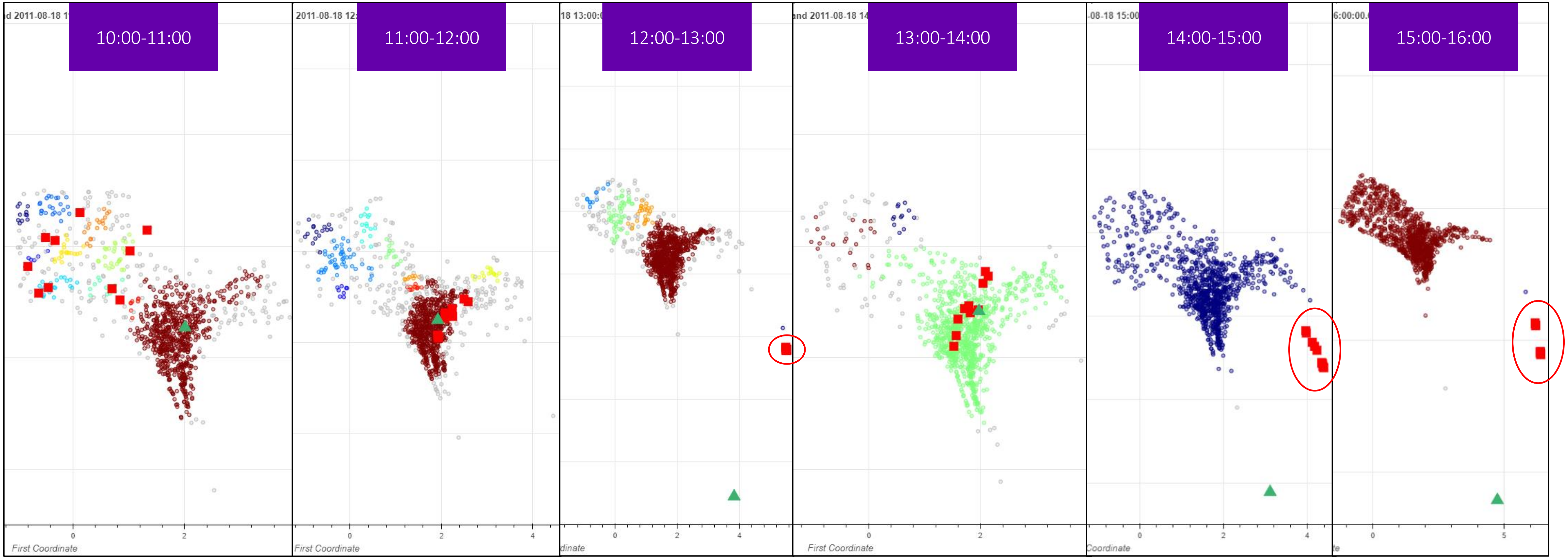

DGA
DNS
Malware
C2
Request generated domain 1
Return NXDOMAIN
Request generated domain 2
Return NXDOMAIN
Request generated domain 3
Return resolved domain IP
Connect to returned IP
Botnet communication

DGA Domains

Benign	Conficker	Matsnu	Ramdo	Zeus
google	uhbqolxf	scoreadmireluckapplyfitcouple	cikiugcaqcegsimg	1vz89zm5b2e981bgfhqdzbke3m
facebook	gzhwfdwnjrg	plentyclubplatewatermiss	gqsasakyqmywuigy	1jjcgb11mmtru8r7xsa1xqk8zh
youtube	oyxiufvc	benefitnarrowtowersliphabit	kuiacymwmsowiasw	hxl1z91goi06z14uh54c1o1gj0v
baidu	ufaqzt	accountmoveseemsmartconcert	skimmesmkyccouea	u2tdjf1gart7d1hp83wcvr3uaw
yahoo	cejzf	drawermodelattemptreview	cieyaaccueseescm	1vm442615psvw16ivh963emjo8

Deep Learning to Detect Network Anomalies

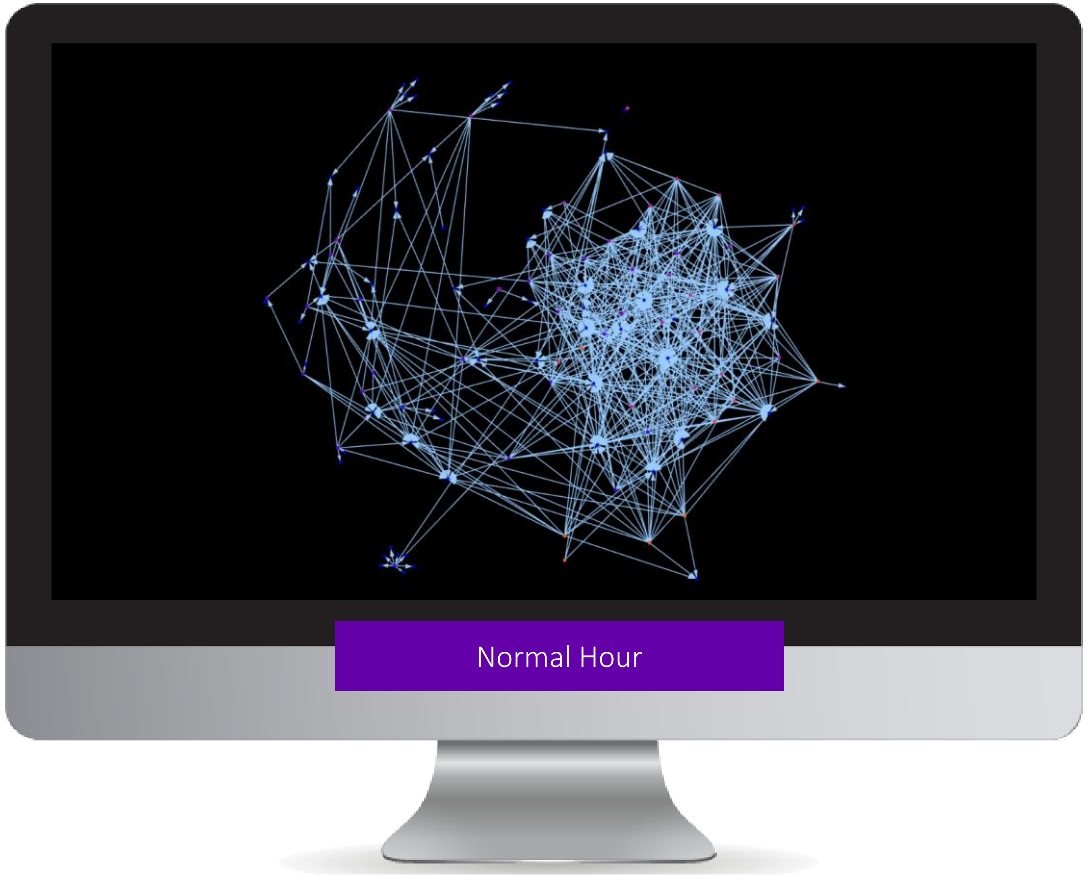
Hosts positioned according to their behaviour, e.g. connecting hosts, destination ports, flow size, …



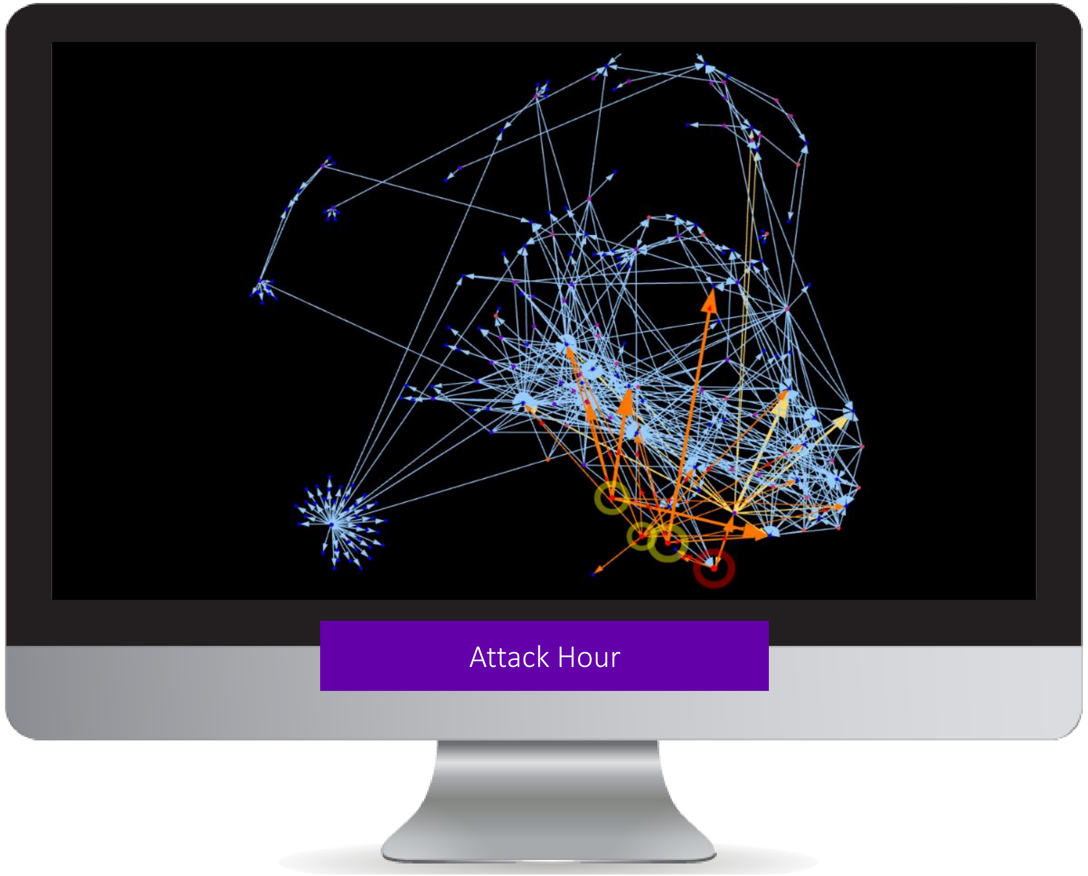
🟥 Botnet computer ▲ Victim computer

Contextualising Anomalies using Nexus

Suspicious vs Malicious



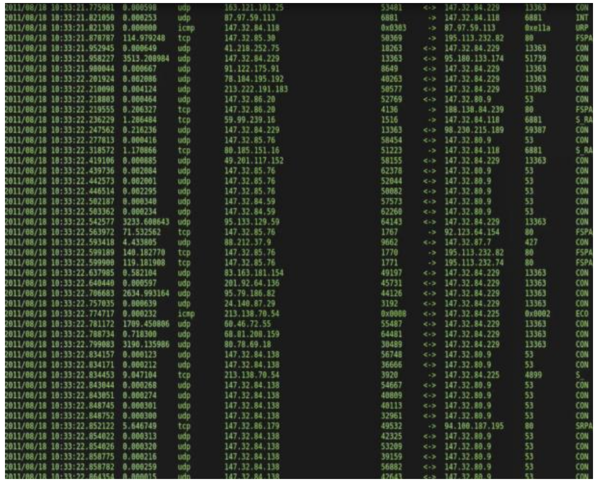
Normal Hour



Attack Hour

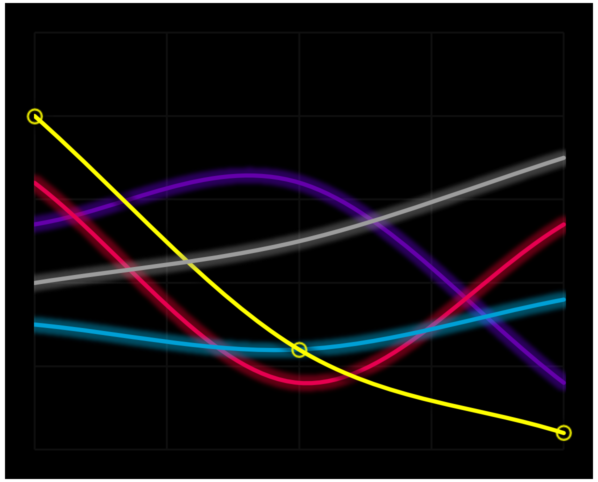
Machine Assisted Cyber Threat Hunting

Data layer

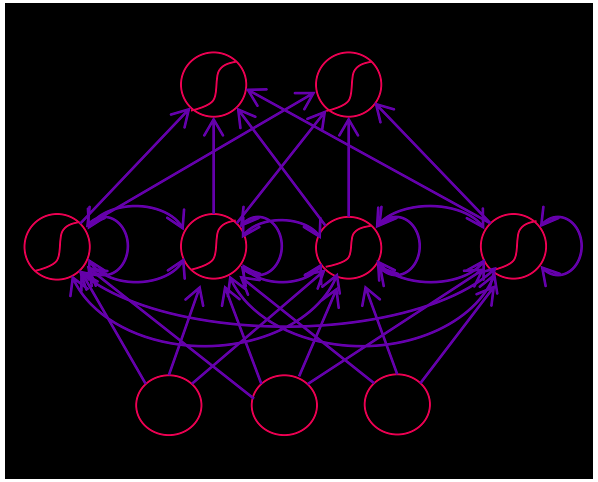


```
2011/08/18 10:33:21.775981  0.000598     udp      163.121.101.25       53481     <->  147.32.84.229     13363     CON
2011/08/18 10:33:21.821050  0.000253     udp      87.97.59.113         6881       ->  147.32.84.118     6881      INT
2011/08/18 10:33:21.821303  0.000000     icmp     147.32.84.118        0x0303     ->  87.97.59.113      0xe11a    URP
2011/08/18 10:33:21.878787  114.979248   tcp      147.32.85.30         50369      ->  195.113.232.82    80        FSPA
2011/08/18 10:33:21.952945  0.000649     udp      41.218.252.75        18263     <->  147.32.84.229     13363     CON
2011/08/18 10:33:21.958227  3513.208984  udp      147.32.84.229        13363     <->  95.180.133.174    51739     CON
2011/08/18 10:33:21.980044  0.000667     udp      91.122.175.91        8649      <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.201924  0.002006     udp      78.184.195.192       40263     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.210098  0.004124     udp      213.222.191.183      50577     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.218803  0.000464     udp      147.32.86.20         52769     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.219555  0.206327     tcp      147.32.86.20         4136       ->  188.138.84.239    80        FSPA
2011/08/18 10:33:22.236229  1.286484     tcp      59.99.239.16         1516       ->  147.32.84.118     6881      S_RA
2011/08/18 10:33:22.247562  0.216236     udp      147.32.84.229        13363     <->  98.230.215.189    59387     CON
2011/08/18 10:33:22.277813  0.000416     udp      147.32.85.76         58454     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.318572  1.170866     tcp      80.185.151.16        51223      ->  147.32.84.118     6881      S_RA
2011/08/18 10:33:22.419106  0.000885     udp      49.201.117.152       58155     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.439736  0.002084     udp      147.32.85.76         62378     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.442573  0.002001     udp      147.32.85.76         52044     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.446514  0.002295     udp      147.32.85.76         50082     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.502187  0.000340     udp      147.32.84.59         57573     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.503362  0.000234     udp      147.32.84.59         62260     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.542577  3233.600643  udp      95.133.129.59        64143     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.563972  71.532562    tcp      147.32.85.76         1767       ->  92.123.64.154     80        FSPA
2011/08/18 10:33:22.593418  4.433805     udp      88.212.37.9          9662      <->  147.32.87.7       427       CON
2011/08/18 10:33:22.599189  140.182770   tcp      147.32.85.76         1770       ->  195.113.232.82    80        FSPA
2011/08/18 10:33:22.599900  119.181908   tcp      147.32.85.76         1771       ->  195.113.232.74    80        FSPA
2011/08/18 10:33:22.637985  0.582104     udp      83.163.181.154       49197     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.640440  0.000597     udp      201.92.64.136        45731     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.706683  2634.993164  udp      95.79.186.82         44126     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.757035  0.000639     udp      24.140.87.29         3192      <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.774717  0.000232     icmp     213.138.70.54        0x0008    <->  147.32.84.225     0x0002    ECO
2011/08/18 10:33:22.781172  1709.450806  udp      60.46.72.55          55487     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.788734  0.718300     udp      68.81.208.159        64481     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.799083  3190.135986  udp      80.78.69.18          30489     <->  147.32.84.229     13363     CON
2011/08/18 10:33:22.834157  0.000123     udp      147.32.84.138        56748     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.834171  0.000212     udp      147.32.84.138        36666     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.834453  9.047104     tcp      213.138.70.54        3920       ->  147.32.84.225     4899      S_
2011/08/18 10:33:22.843044  0.000268     udp      147.32.84.138        54667     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.843051  0.000274     udp      147.32.84.138        40809     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.848745  0.000301     udp      147.32.84.138        40113     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.848752  0.000300     udp      147.32.84.138        32961     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.852122  5.646749     tcp      147.32.86.179        49532      ->  94.100.187.195    80        SRPA
2011/08/18 10:33:22.854022  0.000313     udp      147.32.84.138        42325     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.854026  0.000320     udp      147.32.84.138        53209     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.858775  0.000216     udp      147.32.84.138        39159     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.858782  0.000259     udp      147.32.84.138        56882     <->  147.32.80.9       53        CON
2011/08/18 10:33:22.864354  0.000015     udp      147.32.84.138        42643     <->  147.32.80.9       53        CON
```

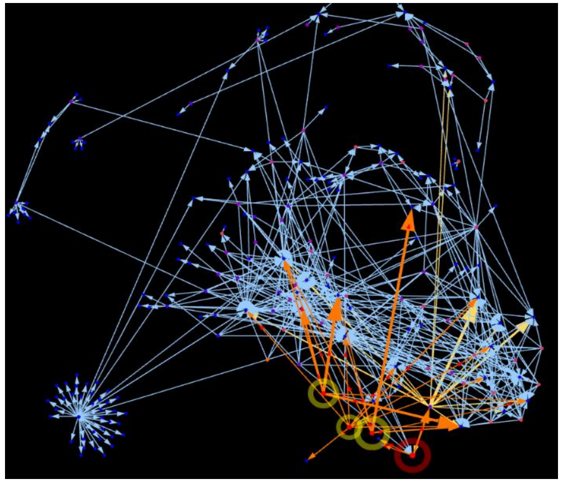
Feature layer



Model layer



Threat layer



“Computers are incredibly fast, accurate, and stupid; humans are incredibly slow, inaccurate, and brilliant; together they are powerful beyond imagination”

- attributed to Albert Einstein

BT