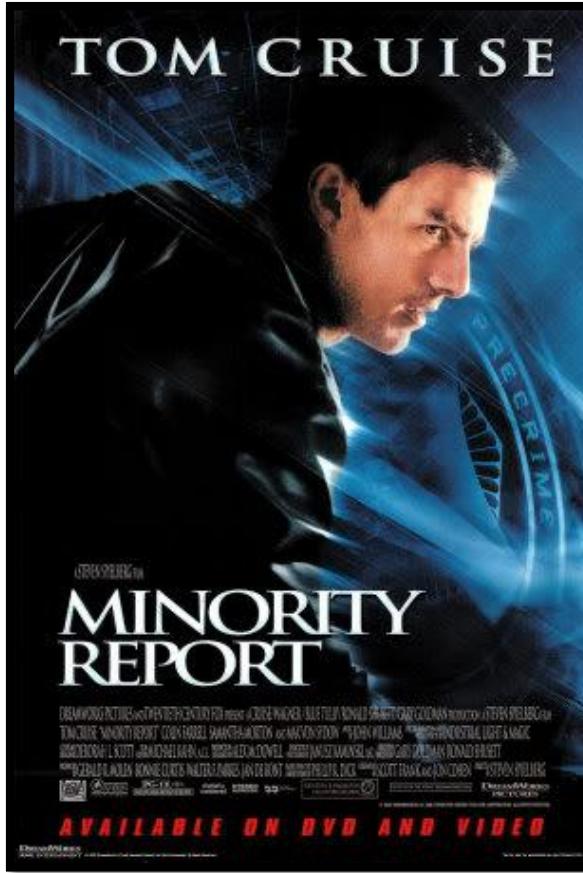


Enterprise Immune System 企業免疫系統

以機械學習智慧應用技術，抵禦各類型先進資安威脅

產品經理 廖本凱 Eason Liao

資安事件是否可以預防?



《關鍵報告-2002 湯姆克魯斯》

知己知彼，掌握到駭客的攻擊手法



《孫子兵法·謀攻篇》

- 能不能在**資安事件發生之前**，就能先預先洞察出威脅的來源？
- 事件發生

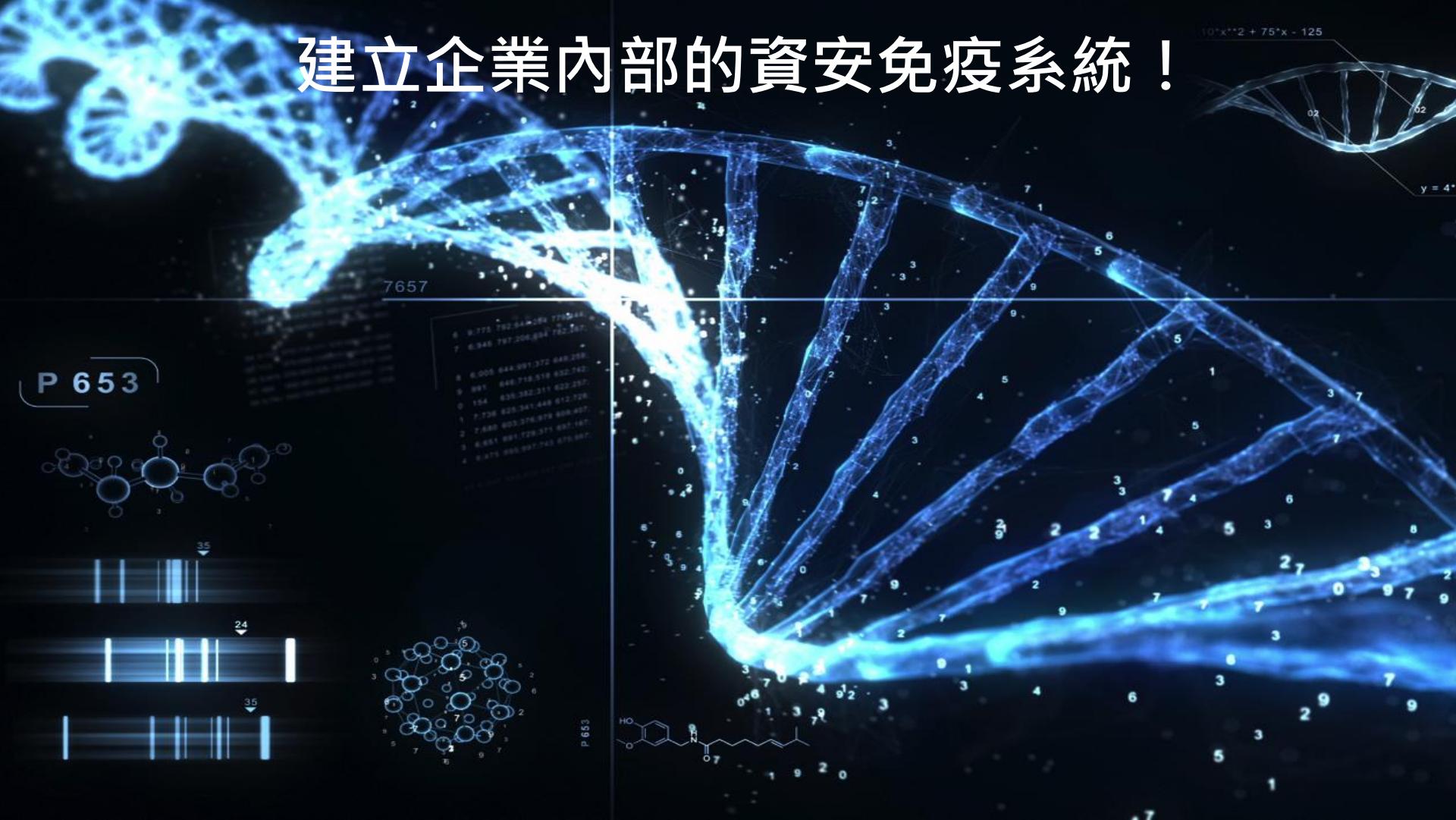
除了被動阻擋，更應該轉為主動預知

The Adaptive Security Architecture

Gartner.



建立企業內部的資安免疫系統！



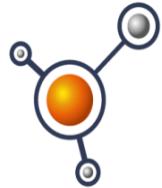
何謂知己？何謂知彼？

最終一役 AlphaGo 再奪勝！人機世紀大戰最終比數 4：1 電腦勝

作者 呂 紹玉 | 發布日期 2016 年 03 月 15 日 17:01 | 分類 Google, 人工智能, 尖端科技



關於 DARKTRACE



DARKTRACE



不需特徵碼



機器學習技術



即時偵測異常

- 2013 年成立於英國劍橋
- 由數學家與政府情報專家組成
- 以機械學習與數學定理為核心
- 總部設於英國劍橋與美國舊金山
- 全球已服務超過 200家重要客戶
- 已於全球17個國家建立營運據點
- 榮獲 2015 Info Security Global Excellence Awards 【年度最佳資訊安全服務企業】獎項
- 榮獲 2015 Network Products Guide IT World 【最佳內部威脅偵測解決方案】獎項
- 榮獲 2015 Gartner 【年度最酷資安廠商】風雲獎項
- 榮獲世界經濟論壇【2015 技術先行者】獎項



DARKTRACE EIS企業行為免疫系統

機械學習結合數學演算，翻轉資安傳統防禦技術，洞悉企業網路威脅情狀

Darktrace Enterprise Immune System

Data Capture & Interpretation Recursive Bayesian Estimation Threat Visualizer

Real-time Total Network Immersion Unsupervised real-time mathematical engines 3D Topological Network Projection

Network Data Log Data User Behavior Data

Raw packet storage for forensics

300+ Intelligent Agents

Human Modeling News Modeling

Intelligent Editor

找出資安設備所找不到的
“潛在異常網路行為”



- ✓ 偵測網路環境內最細微變化，實時更新企業網路生命特徵數據模型
- ✓ 多樣化數據分析比對過往與新興的各式網路數據行為
 - + 全自動建構企業資訊網路行為數學模型
 - + 百分百完整呈現企業資訊網路傳輸行為
 - + 深入個人、主機以及網路設備連線分析
 - + 長期分析企業生命特徵，具備異常行為回放機制
 - + 自動威脅行為分類，支援工作流程以及協作機制

Darktrace EIS 全3D可視化中控台

收集並分析網路封包內164種META DATA屬性並建立出DNA

10.11.160.200

10.11.160.200

Home Menu

Breach Log

Anomalous Connection / 1GB Outbound

Tue Apr 12, 00:00:00 - 16:51:37

10.11.160.200
1.1 GiB External Data Transfer (Client)
Tue Apr 12 09:04:35 Hostname android.clients.google.com
Outgoing traffic
To/from the same IP
To 173.194.72.113

Model Breach Event Log

Tue Apr 12 2016, 09:04:35 All Events

Tue Apr 12, 09:02:34 → A slightly unusual time for a connection externally on port 443
→ 10.11.160.200 was still connected to 173.194.72.113 [443]
A slightly unusual time for a connection externally on port 443

Tue Apr 12, 09:02:28 → 10.11.160.200 was still connected to clients6.google.com [443]
A slightly unusual time for a connection externally on port 443

Tue Apr 12, 09:01:34 → 10.11.160.200 was still connected to 173.194.72.113 [443]
A slightly unusual time for a connection externally on port 443

Tue Apr 12, 09:00:58 → 10.11.160.200 connected to 173.194.72.113 [443]
Tue Apr 12, 09:00:34 → 10.11.160.200 connected to clients6.google.com [443]
Tue Apr 12, 09:00:34 → 10.11.160.200 connected to 173.194.72.113 [443]
A slightly unusual time for a connection and a recent increase in outgoing data volume externally on port 443. A small increase in data being sent to public IPs

Tue Apr 12, 09:00:34 → 10.11.160.200 connected to clients6.google.com [443]

Tue Apr 12, 09:00:25 →

Today Tue Apr 12, 00:00:00 Tue Apr 12, 16:53:17 Models, highest score Include acknowledged breaches 42%

Anomalous File / Uncommon EXE Compliance / Outbound RDP Anomalous Connection / Download and Upload Compromise / Suspicious Request Data Compromise / Beaconing to Rare Destination Device / New User Agent

09:02:06 5 minutes 09:07:06
Tue Apr 12 2016 09:04:36

Views Single device Breach devices

Connection Status Normal Breached

Remote Ports 443 14.8 MiB 11 GiB 52775 0 bytes 31.0 KiB 53 1.0 KiB 355 bytes 138 0 bytes 604 bytes

Local Ports (23) 62567 14.7 MiB 11 GiB 3389 31.0 KiB 50920 13.8 KiB 7.7 KiB 51092 9.5 KiB 4.8 KiB

Devices (12) clients6.google.com 14.8 MiB 11 GiB 1500186JiaoYiHe 31.0 KiB 216.58.217.195 13.8 KiB 7.7 KiB 64.233.189.113 5.3 KiB 2.7 KiB

Subnets 10.40.192.0/24 0 bytes 31.0 KiB

Networks External 14.8 MiB 11 GiB Internal 0 bytes 31.6 KiB

Protocols UDP 14.8 MiB 11 GiB TCP 7.4 KiB 39.7 KiB

Application Protocols Unknown 14.8 MiB 11 GiB SSL 6.6 KiB 39.3 KiB DNS 1.0 KiB 355 bytes

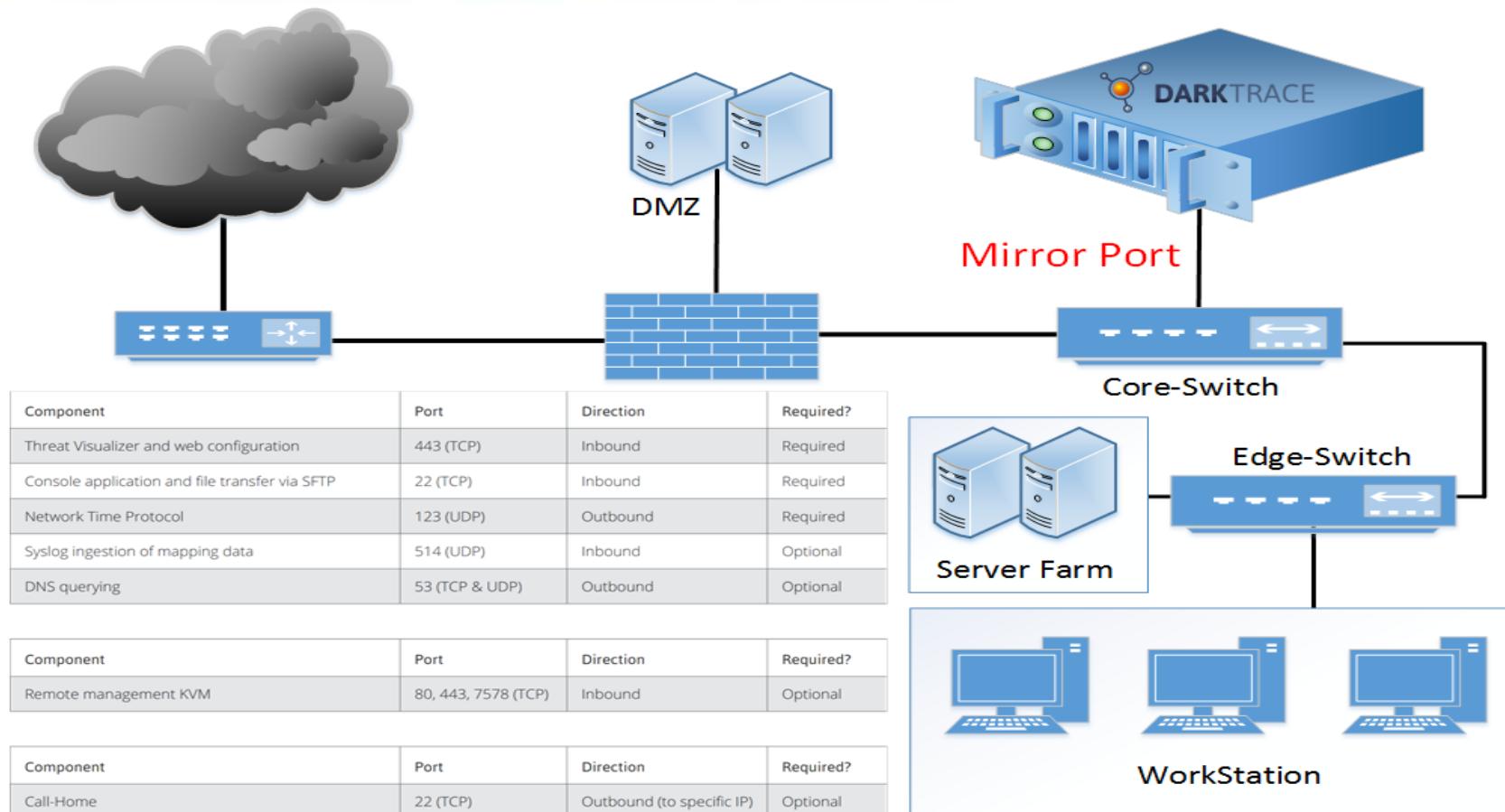
The screenshot displays the Darktrace EIS interface. On the left, a 'Breach Log' window shows an 'Anomalous Connection / 1GB Outbound' event from 10.11.160.200 to clients6.google.com. Below it, a 'Model Breach Event Log' window lists numerous connection events over several hours. In the center, a 3D globe visualization shows network traffic paths between various IP addresses. To the right, a detailed 'Graph' window for 10.11.160.200 on Tuesday, April 12, 2016, at 09:04:36, tracks 'External Data Transfer (Client)' metrics like 'External Connections to Closed Ports' and 'External Data Transfer (Client)' over time. A comprehensive summary table on the far right provides statistics for various network components like ports, devices, subnets, networks, protocols, and application protocols.

DARKTRACE 可以幫助您找到腦人的勒索軟體

The screenshot shows the DARKTRACE user interface. On the left, a sidebar lists 'Similar devices to 10.11.5.253' with various IP addresses. The main area displays a search result titled 'View similar devices' with a red box highlighting it. Below this, there are two donut charts: 'Ports used by 10.11.5.253' and 'Devices used by 10.11.5.253'. To the right, there's a 'Time period' dropdown set to '1 Week', a 'Graph data' dropdown set to 'Connections', and a summary box stating 'Number of similar devices: 3 Devices'. At the bottom, there's a row of ten warning icons with counts: Compliance / SSH To Rare External Destination (1), Anomalous File / Uncommon EXE (1), Compromise / Beaconing to Rare Destination (35), Device / New User Agent (1), Test / Test_0425 (1), Anomalous Server Activity / New or Uncommon External from Server (1), Compliance / File Storage / Dropbox (1), Device / Server Reboot (1), Device / Suspicious Domain (1), System / External Server Detector (1), Compliance / Incoming RDP (1), and Anomalous Server Activity / DC External Activity (5).

快速找出企業內同樣受駭的IT裝置設備

導入架構單純，不影響現有環境



透過模型比對找查異常行為風險

異常行為		說明描述
1.	Remote access attack linked to dangerous malware RAT攻擊潛伏行為	偵測企業內部殭屍網路行為，發掘隱匿於企業環境內高複雜度、高隱匿性與多樣性的殭屍網路通訊
2.	Anomalous data transfer 異常數據傳輸行為	偵測企業可疑數據傳輸行為，尤其是包裝於一般應用程式外表下，卻對外產生異常連結與通訊
3.	Illegitimate access to database server 非法存取資料庫行為	偵測企業非法存取資料庫行為，尤其是額外的、異常的非加密連線，並分析存取來源與目的間相對關係，並研判其風險程度
4.	Unauthorized use of administrator credentials 未經授權卻使用管理員憑證行為	偵測是否有特權用戶，於特殊期間，發生非工作時間多次登入企業網路環境進行存取行為
5.	Fast travel indicating password compromise 單一帳號多點同時登入行為	偵測單一使用者帳號，卻於不同來源，且同一時間登入企業網路進行存取行為
6.	Connections to website linked to Advanced Persistent Threats 瀏覽網路時遭受APT攻擊行為	偵測使用者瀏覽知名社交網站時，經惡意導向至可疑的站台，可能遭遇APT針對性攻擊的行為
7.	Infection with ransomware 遭勒索軟體感染的行為	偵測使用者瀏覽網路後，遭勒索軟體植入後對主機異常使用與連線行為
8.	Domain Generation Algorithm 使用動態網域演算法的惡意行為	偵測企業主機對外連線，其連結對象為使用動態網域演算法，而產生之大量無效網域名稱行為
9.	Malicious web drive-by 惡意偷渡式攻擊行為	偵測使用者遭受的惡意偷渡式攻擊行為，於使用者電腦已遭受惡意程式感染時，它將竄改電腦設定，將您的正常連線導向一個惡意偽冒網站

透過機器學習讓您的安全防護再次提升



Lancope



External threat intelligence



STROZ FRIEDBERG
DIGITAL RISK MANAGEMENT & INVESTIGATIONS



硬體規格符合各客戶的需求

Darktrace appliance	Average sustained throughput	Devices analyzed	Form factor	Data feed interfaces
DCIP-X-11G	5Gbps	36,000	2U rackmount	2 x 10G SFP+ 3 x 1GbE RJ45
DCIP-X-10G	5Gbps	36,000	2U rackmount	2 x 10G SFP+
DCIP-X-1G	3Gbps	25,000	2U rackmount	3 x 1GbE RJ45
DCIP-M-11G	2Gbps	8,000	1U rackmount	2 x 10G SFP+ 3 x 1GbE RJ45
DCIP-S-1G	300Mbps	1,000	1U rackmount	3 x 1GbE RJ45
DCIP-SM-1G	100Mbps	300	Fanless non rackmount	1 x 1GbE RJ45

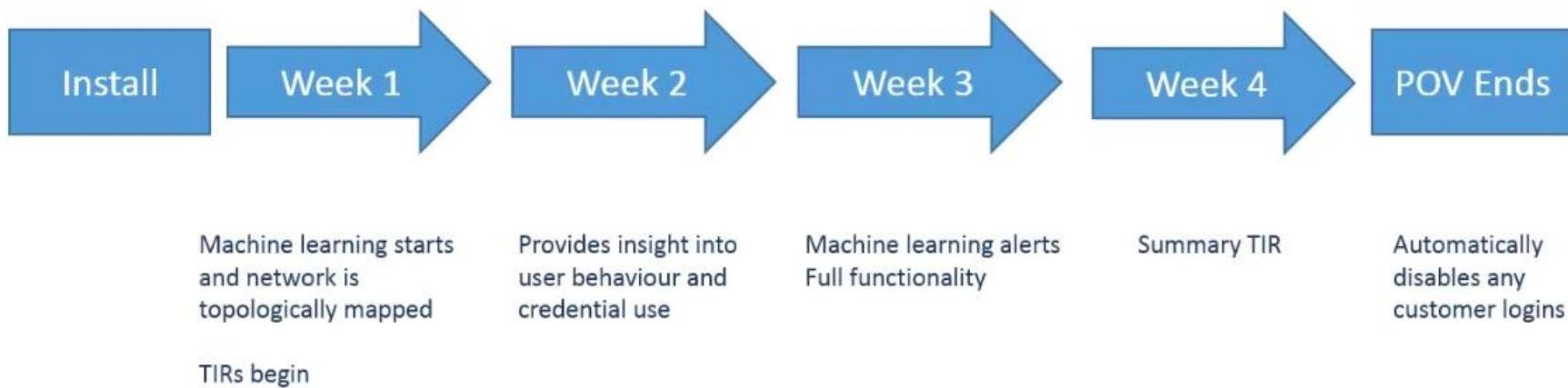
服務項目：

- 每月產出一份異常威脅評估報告
- 原廠現場客戶端教育訓練2天(英文課程)
- 設備提供RMA

DARKTRACE價值驗證 (Proof of Value, POV) 計畫

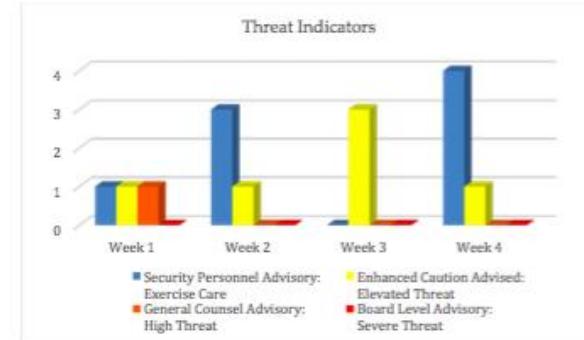
Proof Of Value (POV)

- 檢視企業資訊環境具體情狀
- 標註企業環境高度異常行為
- 專家解析企業網路現有威脅
- 實施資訊環境風險狀態評估
- 提出量身訂製風險改善建議



Threat Intelligence Report (TIR), 企業威脅報告

- 由全球頂尖安全威脅分析師提供網路威脅分析。
- 由全球頂尖安全威脅分析師提供設備諮詢服務。
- 取得基於客戶環境，量身訂製的威脅情報報告。
- 取得對於異常行為，專業並可行的安全性建議。



Week 1

1. Sophisticated malware infection; the device is probably under the attacker's control
2. A user downloaded a suspicious program while attempting to download Google Chrome
3. One device performs trace routes every other day

Week 2

1. Suspicious user behaviours: a user downloads copyrighted TV programmes and transfers files to a home file server
2. A credential is being used on two devices simultaneously
3. Data transferred to Dropbox
4. Use of Telnet between two devices on a Saturday

Week 3

1. One device is regularly Bitcoin mining, possibly due to a malware infection
2. Device downloaded malware while running an out-of-date browser
3. The user reported last week continues to download and then transfer TV programmes to a home file server, now using a different computer

Week 4

1. Large amount of data transferred to Google Drive
2. One device is using the TOR network
3. A device port scanned and attempted access to shared files on another device
4. One device downloaded a third-party VPN client
5. Use of LogMeIn and Disconnect.me services from 8 devices in total

客戶實績



Johnson Matthey

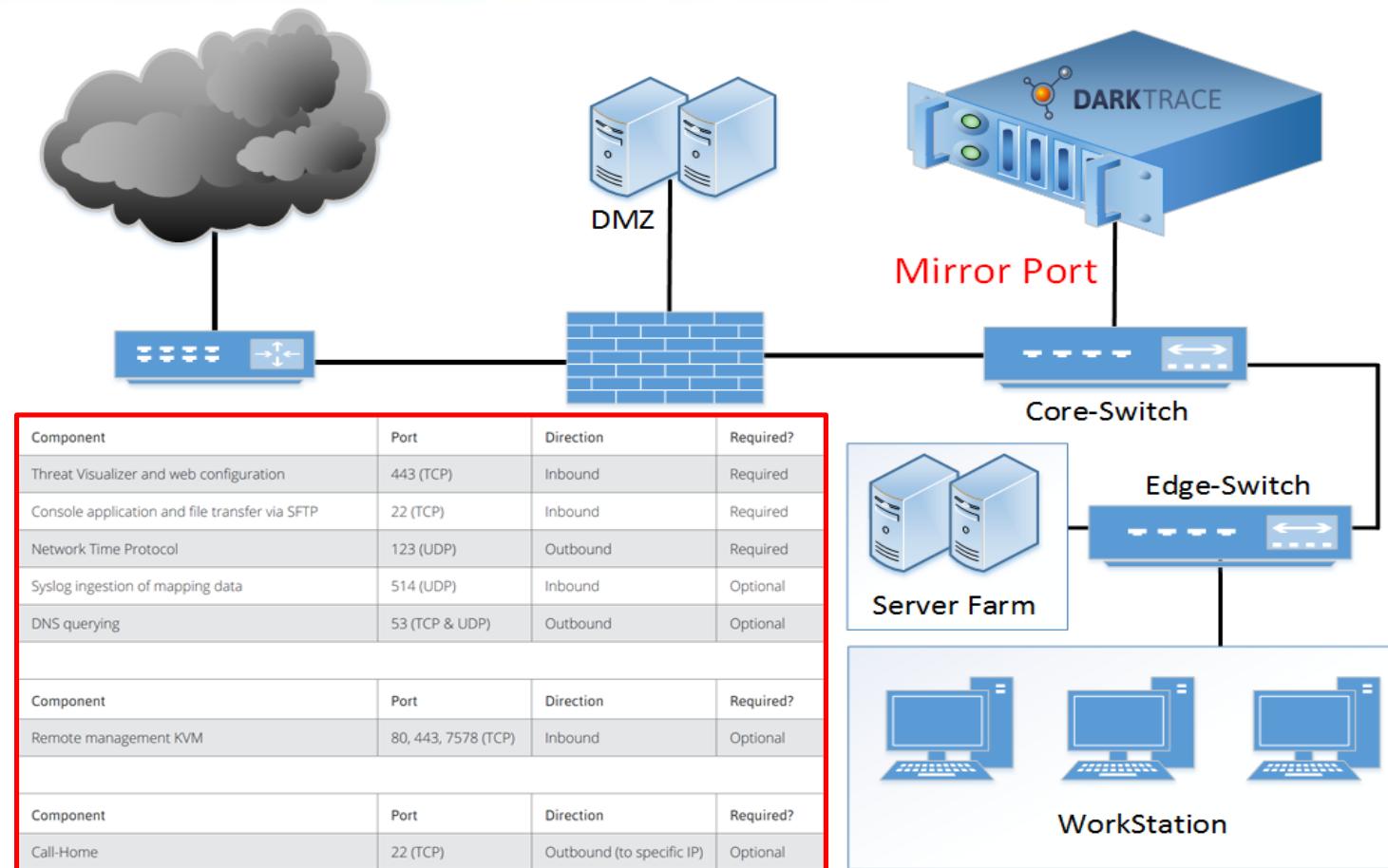


Marathon
Petroleum Corporation



客戶群涵括能源、電信、金融服務、交通運輸、零售服務業等各領域

導入架構單純，不影響現有環境



SYSTEX

Cloud, Mobile, Social, Analytics & Cybersecurity
End to End Ecosystem Enabler



安全政策調適

Folder Compliance /

Policy Name **Bitcoin activity**

Active? **NO**

Type **Weighted**

This policy will breach if there is:

- + Any Bitcoin miner **1**
- Any Bitcoin mining pool server **1**
- Any possible Bitcoin mining **1**

Target score **1**

Target score must be reached within **60** seconds

Wait **60** seconds between policy breaches

Delete

Connections	> 0	in 60 mins
Connections	External Connections	Internal Connections
Active Connections	Active External Connections	Active Internal Connections
Data Transfer	External Data Transfer	Internal Data Transfer
External Packets	Internal Packets	External Data Ratio
External Connection Duration	Internal Connection Duration	
External Connections to Closed Ports	Internal Connections to Closed Ports	
Behavioral Analysis Events	Cases of Malformed Traffic	

(LOG DATA) Proxy Logs | (LOG DATA) VPN Login | 32-Bit Packages Installed | APT Certificates | APT Domain Hits
APT1 Domain Hits | Address Scans | BitTorrent Handshakes | Bitcoin Miners | Bitcoin Mining Pool Servers
Bitcoin Possible Mining Operations | Broadcasts | Clients Not Sending Keep-Alive | Connection Spread
Credential Use Unusual User | DNS Requests | DNS Server Change | Detected Operating System | Detected Sites
Door Entry Swipe HSN2 | Dropped Packet Notices | DynDNS DNS | DynDNS HTTP | DynDNS SSL
Emails from Suspicious Places | Emails with Watched Character Sets | Excessive Capture Loss
Excessive NXDOMAIN Queries | External Connection Spread | External DNS Names | External DNS Servers
External DNS Servers (DT) | External Multicasts | FTP Bruteforces | FTP SITE EXECS | FastTravel Alerts
File Transfers (RAR) | Incorrect File Types | Incorrect HTTP File Type Transfers | Intel APT Hits | Intel Match
Intelligence Notices | Internal Connection Spread | Internal DNS Servers (DT) | Invalid SSL Certificates
Invalid SSLs | Java Malware Downloads | Kerberos Login Failures | Kerberos Logins | Large Data Extractions
Link-Local Connections | Logins Unusual User | Logons | Malformed Traffic | Malware Misspellings | Multicasts
New Devices | New External IP | New Regular Connectivity | New Visited IPs | No DHCP Traffic Events
Outbound TORs | POP3 Login Successes | Port Scans | Processes | Rare OS Useragent Combination | Robots
SMB Directory List | SMB Login | SMB Login Failed | SMB Login Success | SMB Read File



數據模型檢視

← Multiple high risk file types

Folder: Attack /

Model Name: Multiple high risk file types

Active?: YES

Type: Weighted Checklist

Description: Identifying the download of two or more high risk files within a minute: exe, pdf, swf

This model will breach if there is:

- Any external connections (3 filters)
- Any EXE file transfer with a hostname rarity of more than 50% and not to -
- Any external connections (3 filters)

Points:
1
1
1

Target score: 2

Target score must be reached within 60 seconds

Wait 3600 seconds between model breaches

← Exe and Outbound Rare

Folder: Attack /

Model Name: Exe and Outbound Rare

Active?: YES

Type: Checklist

Description: Identifying a download of an executable in combination with a connection to a rare hostname.

This model will breach if there is:

- Any EXE file transfer with a new or uncommon occurrence score of more than 50% or with a hostname rarity of more than 50%
- Any external connections with a hostname rarity of more than 80%

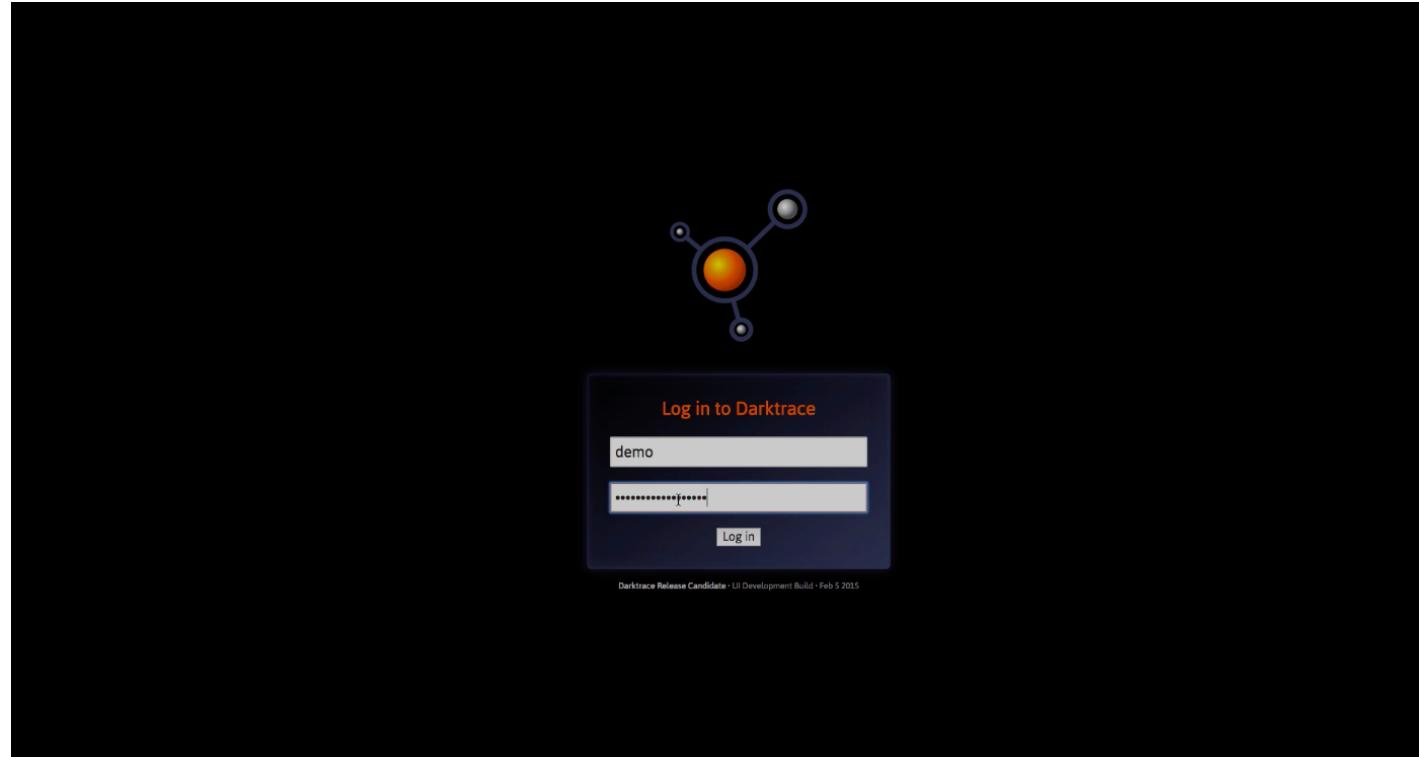
Both components must be breached in the above order YES

Both components must be breached within 180 seconds

Wait 300 seconds between model breaches



威脅視度展示 1/5



感统失调症三七五

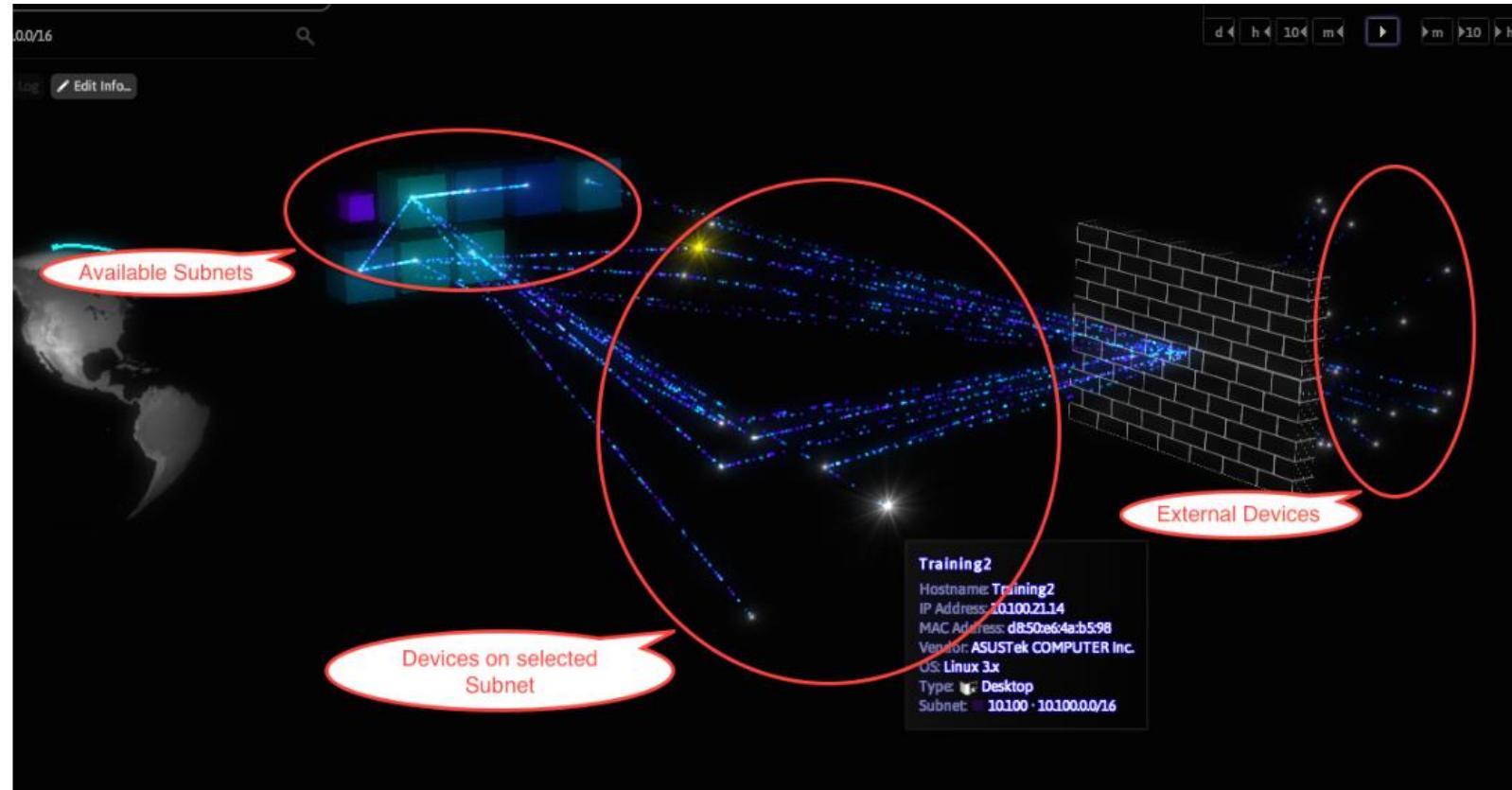
威脅視度展示 2/5



威脅視度展示 3/5



威脅視度展示 4/5





威脅視度展示 5/5

17 subnets, 193 devices, 179 clients, 17 unknown devices, 21 user credentials.

Span Selector, Sort order, Span start, Span end.

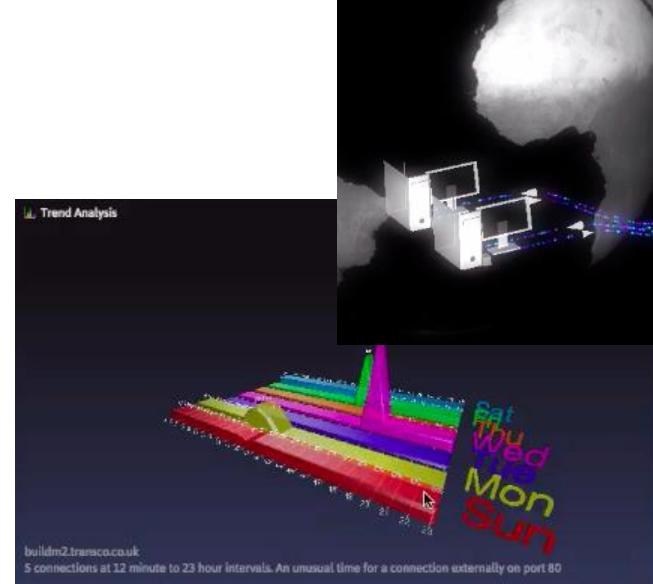
Breach Log: Math / Unusual Connectivity, Wed Jan 28, 14:04:56 – Thu Feb 5, 18:04:56.

Date	Device	Connection	Notes
Wed Feb 4 13:39:03	c1154.transeo.co.uk	Connection	88 % unusual connectivity > 85 %
Wed Feb 4 10:51:22	buildm2.transeo.co.uk	Connection	88 % unusual connectivity > 85 %

Sue Smith, User Information: Name Sue Smith, Department Human Resources.

Device Information: IP Address 10.100.17.11, Subnet 10.100.17.0/24.

Trend Analysis visualization showing a globe with network connections and a 3D heatmap below it.



Darkflow

350 – 1,000+ measurements

Extracted from raw network traffic feeding
into
Unsupervised Machine Learning Approaches

PACKET META DATA • PACKET FLOW DATA
• DPI • O/S & APP FINGERPRINTING •
USER ACTIONS

2 Appendices

2.1 List of metrics

Connections	The number of connections created involving the device over a period of time. The IP address, port and protocol define a connection.
External Connections	Every connection has an originator (source) that creates the connection, and an endpoint (destination). Generally speaking, a connection can be between two internal machines, between a machine and a public IP address, between a public IP address and an internal machine, or between a public IP address and another public IP address. In this context <i>device</i> refers to only an internal device. (DCIP does not consider www.google.com to be a device.)
Internal Connections	The number of connections between the device and other devices on the internal network over a period of time.
Connected Devices	The number of distinct IPs (machines) the device connects to over a period of time.
External Connected Devices	The number of distinct external IPs (machines) connected to in the outside world over a period of time. Analogous to 'Connected Devices' but for external IPs.
Internal Connected Devices	The number of distinct IPs (machines) connected to within the internal network over a period of time. Analogous to 'Connected Devices' but for internal IPs.
Active Connections	The number of ongoing connections at any one time involving the device over a period of time.
Active External Connections	The number of ongoing connections at any one time between the device and the outside world over a period of time.
Active Internal Connections	The number of ongoing connections at any one time between the device and other devices on the internal network.
Data Transfer	The volume of data transferred by the device over a period of time.
External Data Transfer	The volume of data transferred between the device and the outside world over a period of time.
Internal Data Transfer	The volume of data transferred between the device and the internal network over a period of time.

Where do We fit

端末設備 (防毒、紀錄、更新)	網路設備 (防火牆、沙箱、威脅分析)
Rules & Signatures	Rules, Signatures, Data-mining/ science
安全事件分析 (安全事件管理、大數據)	整體網路環境 
Data-mining/ science	Machine Learning

Rules and Signatures : 發掘【已知】的惡意程式以及異常行為

Data-mining/science : 提供管理同仁異常事件的關連【紀錄】

Machine learning : 實時顯示資訊網路潛藏之【異常】行為



Customer Perspectives

“Darktrace has the unique capability to detect things that happen over time.”

“We have found that other products claiming to offer behavioral learning are in fact rules based, with little or no true machine learning.”

“While most companies are claiming to do some correlation analysis and behavioral analysis, I have looked into their offerings and nothing comes close to Darktrace.”

“We like the way that Darktrace continues to
“No existing products on the market can do what Darktrace does.”

learn over time and avoids the noise.”

“It’s the best security technology on the market.”

“I think the math algorithm is brilliant – it sold the product to me.”

“I got unprecedented visibility of my network.”

Case Study: Drax

Industry

- Energy & utilities

Challenge

- Drax is part of critical national infrastructure
- Defense for corporate & production environments required
- Concerned about insider threat
- Needed protection about advanced threats

Benefits

- Detected threats that had bypassed other security tools
- Added Industrial Immune System to monitor Industrial Control Systems
- Continual monitoring of networks & anomalies
- Ability to investigate and mitigate threats in real time

“Darktrace’s technology has identified threats with the potential to disrupt our systems”

Drax



Case Study: Virgin Trains

Industry

- Transportation

Challenge

- Cyber security named priority by Virgin Group
- Large partner base connected to network
- Increasingly wireless on trains
- Maintain customer experience while managing risk

Benefits

- Baseline of how users, devices and network operate
- Unlike SIEM tools, provides total, real-time visibility
- Able to pinpoint security spend and maximize resources
- Improved customer confidence

“Darktrace’s cyber intelligence platform provide us with total visibility into what is happening in real time”

Louis Kangurs
IT Network Director, Virgin Trains



Case Study: DNK

Industry

- Insurance

Challenge

- Lead cyber security efforts in shipping industry
- Potential threats & cyber warfare against DNK's members
- Proactive defense required to anticipate problems

Benefits

- Constant monitoring of corporate network
- Ability to address security issues in real time
- Greater confidence in ability to defend against sophisticated threats and protect members
- Boost to DNK as leader in security and risk mitigation

“Darktrace detects potential issues without us having to define what we’re looking for in advance or make assumptions”

Svein Ringbakken
Managing Director, DNK



Case Study: Sega Games

Industry

- Games

Challenge

- Protection against APTs
- Widespread use of social media and other data-sharing sites
- Defense of core intellectual property (games), customer data and corporate reputation

Benefits

- Adaptive monitoring
- Better understanding of dynamic digital environment
- Surfaces anomalies that would otherwise hide in Sega's busy networks
- Significant reduction in cyber risk
- More stable environment for customers, customer and digital assets

“Darktrace gives us a higher degree of confidence in our security, and that translates into a more stable environment for our staff, customers and data.”

Sega



Case Study: BT

Industry

- Telecommunications

Challenge

- Large, widely dispersed network
- Fast-evolving sophisticated threats
- Wanted a solution that could parse complex network data and detect previously unknown threats

Benefits

- Real-time, dynamically updated visibility of entire network
- Confidence that previously unknown threats can be detected within network before they do serious damage
- Enhanced their own security offerings with Darktrace's expertise in unsupervised machine learning and Bayesian mathematics
- Defended against potential insider threat

“Darktrace’s machine learning and mathematics are extremely powerful in detecting activity that is abnormal and will be critical to our future cyber security offerings.”

Mark Hughes, President
BT Security

