BEHAVIOURAL ANALYTICS

ITC Managed Security Services

Making the digital world a safer place to do business

WHAT IS NORMAL ANYWAY?

It's difficult to predict what the next threat to your business will look like.

An effective behavioural analytics platform understands the daily pattern of life for your network.

With this understanding, there's far more chance of spotting changes in behaviours that may be harmful to your business.

THE ISSUES

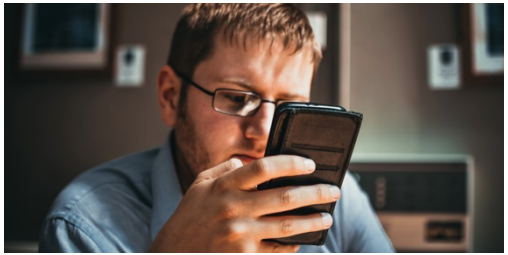
Organisations face ever changing and ever more complex threats.

The amount of sensitive data stored on disparate networks is increasing.

Employees are using Shadow IT, invisible to traditional security tools.

Increasing number of users and devices with access to sensitive data.

Advanced persistent threats and insider threat are difficult to detect.



Traditional rules-based security and cyber skills are at a premium.

THE SNOWDEN EXAMPLE

Insider threats to your cyber security are potentially the most devastating. They are founded on familiarity with your organisation and privileged access to your data.

A recent survey* found that 66% of organisations believe a cyber attack is most likely to come from within.

If Edward Snowden can undermine the NSA, what are the chances an individual could wreak havoc with your business?

* Insider Threat Report, CyberSecurity Insiders, 2018

THE ACCIDENTAL ANARCHISTS

Insiders who threaten an enterprise vary widely in their intentions, awareness and operating privileges.

Collaboration with external threat actors is on the rise, but many of the most destructive insider threats are non-malicious, arising from genuine mistakes, accidental noncompliance and negligence.

Weak passwords and unlocked devices are major factors.

Cyber attacks are forever in the headlines. Week after week we hear of staggering numbers of compromised customer accounts and huge pay outs, as businesses look to put things right.

And this is on top of the even greater cost they'll suffer in damage to their brand, and loss of shareholder and customer confidence.

OUR MANAGED SERVICE AT A GLANCE

ITC-BA is a self-configuring system that reduces the reliance on ‘known bad’ by automatically learning what is ‘normal’ for every device and user on your network.

- From our London-based Security Operations Centre we monitor your entire network (all devices and activity) 24x7x365.
- We provide 100% coverage – cloud, hybrid, on-premise and SAAS.
- Support for, and remediation of, threats and risks is delivered in real time.
- ITC-BA has machine learning and AI which are critical in identifying, and continually adapting to, evolving threats.
- Resources allocation is less critical and your IT teams are freed-up to focus on core business.
- The monitoring of logs, incident reports, anomaly threats and insider risks helps with regulatory compliance.

THE SOLUTION – FOUR ACTIONS

ITC-BA managed security service

1. Identify

Investigate

Optimise

Use threat intelligence

- Global visibility, control and assurance of all assets (known and unknown) 24x7x365.
- Monitoring of all devices accessing your network, including mobile and IoT devices.
- Behaviour models for all devices (managed and unmanaged) to gain insight into rogue actors.
- Prioritised investigations to reduce the threat from malicious insiders and shadow IT.

THE SOLUTION – FOUR ACTIONS

ITC-BA managed security service

1. Identify

2. Investigate

Optimise

Use threat intelligence

- Model breach alerting from experienced analysts who understand your specific security environment.
- Weekly threat intelligence reports with annotations to drive business context and remediation.
- Triage alerts and highlighting of anomalous behaviour to enable rapid investigation and support for incidents.
- Improved stakeholder awareness, providing reassurance that users and systems are acting as expected.

THE SOLUTION – FOUR ACTIONS

ITC-BA managed security service

1. Identify

2. Investigate

3. Optimise

Use threat intelligence

- Deliver against ISO2000-1 a concise actionable service that focuses internal resources, and evolves with your estate and the threat landscape.
- Enable a repeatable consistent approach to threat hunting, and enhance cyber defences with dynamic threat intelligence data.
- Monthly calls to provide ongoing platform tuning and continuous service improvements.

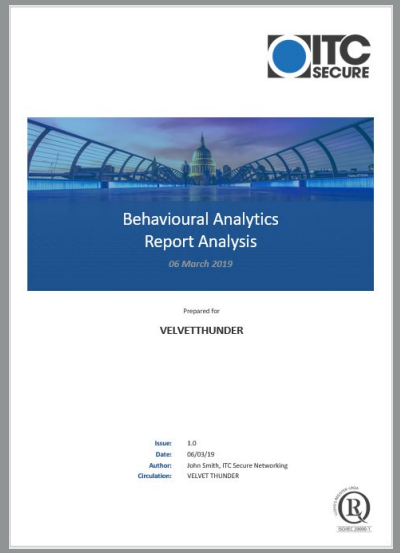
THE SOLUTION – FOUR ACTIONS

ITC-BA managed security service

1. **Identify**
2. **Investigate**
3. **Optimise**
4. **Use threat intelligence**

- Enhance cyber defences with dynamic threat intelligence data, keeping the platform up to date with current threats.
- Take incidents from ‘anomalous’ to ‘known bad’ by the creation of custom models identifying bad URLs, domains, IPs and malicious infrastructure.
- Bespoke intelligence with Threat Horizons leveraging ITC’s expertise to help secure against major malware outbreaks as they happen.

BEHAVIOURAL ANALYTICS SERVICE



- Threat Horizon report model creation
- Proactive threat intelligence
- Indicators of compromise captured
- Model created for all ITC-BA customers

Place internal network security events within the context of emerging external threats

```
import os
import re

#function to build regex for the IDs
def ids_reg():
    name_reg = re.compile('(?<=model name=\").+(?=\" pid)')
    pid_reg = re.compile('(?<=pid=\")\d{2,5}')  #this should
    uuid_reg = re.compile('(?<=uuid\=\")\S{36}')

    return name_reg, pid_reg, uuid_reg

#function to make the strings used for the ids
def ids():
    name = name_reg.search(old_file).group(0)
```

Threat intelligence integration into Darktrace

- Automation script delivers threat model
- 1,000s of malicious IP addresses and malicious websites monitored
- ITC has built the ONLY automated, external threat intelligence integration into Darktrace

WHY CHOOSE ITC-BA

ITC has more than two decades' experience of delivering cyber security for some of the UK's best-known organisations and a number of major global brands.

Our ITC-BA solution is a turnkey service that is painless to deploy, easy to establish and, with no reliance on signatures, able to keep pace with an ever changing threat landscape.

The service is managed from our state-of-the-art Security Operations Centre in London.

Making the digital world a safer place to do business

Boatman's House
2 Selsdon Way
London E14 9GL

itcsecure.com
Tel: +44(0) 20 7517 3900
enquiries@itcsecure.com