flexeye

Security Metrics Platform

Bridge the information security performance gap and protect your organization by releasing your information security team to respond to the present and shape the future, rather than try to react to the past.

There’s a gap between the needed and actual performance of big organizations’ information security systems. And it’s growing.

Threats have grown in speed and complexity – Stuxnet may have been political, but it scared large organizations with what was possible.

Device and data usage have exploded. As consumers, employees use a wide variety of cloud applications, a habit which they’re bringing into the office. They have multiple devices connected to the internet. And organisations’ appetite for agility and merger is causing existing security systems to have to adapt quickly.

The traditional method of managing information security has been to establish key controls. To increase speed of detection these controls are simply measured more frequently.

The control data sits in databases and spreadsheets and is often pulled out manually by a variety of tools: SQL tools, data quality tools, business intelligence tools, and data mining then presented in a variety of formats.

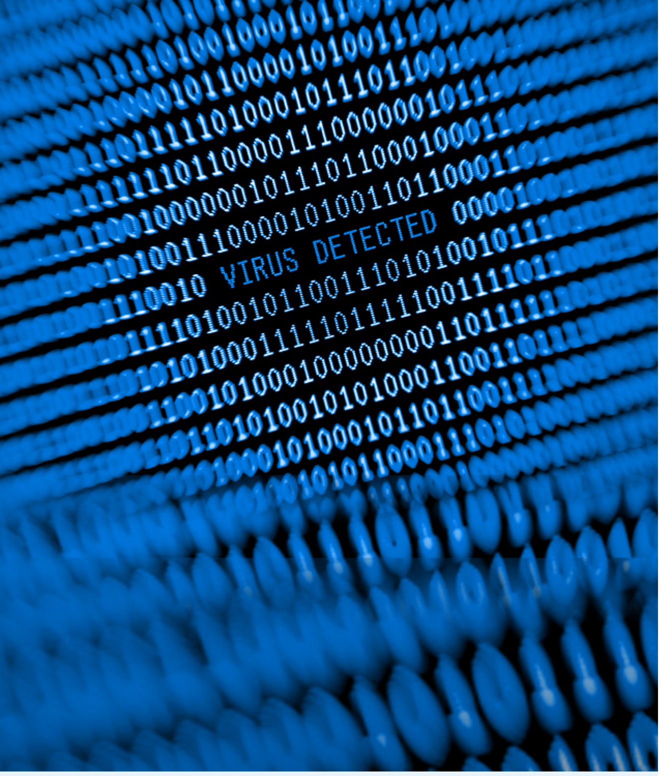
This delay between measurement and presentation and the fragmentation of data sources makes it very difficult to know what’s happening right now, or how it compares with last month. It’s hard to see the whole picture.

Which can help explain the very public information security breaches in verticals such as Government agencies in the US and UK, an electronics giant, one of the worlds leading social networks, a global news agency and a global payment transaction provider, to name but a recent sample.

These organizations are not small, and neither are the consequences. They’ve all been hacked. It’s the stuff that keeps senior information security staff awake at night.

If only there were a better way.

The good news is, there is.



Hunting down the Zero Day attack

Currently, your best defence against a Zero-Day Threat may be to hope that it happens to someone else first. As Stuxnet has shown these threats can affect process control networks and other critical assets, and can bleed away ultra-valuable IP.

Many organizations have increased the number of security controls they use to pre-empt these threats, and the frequency with which they measure. This feels safer but information security departments are bending under the weight of administering them.

Flexeye's advanced big data integrator has the capacity to easily absorb both the number of measurements and increased frequency. It's parallel computation and in memory architecture enables it to throughput massive amounts of data easily, and it's scheduling of collection gives you foreknowledge of your network load.

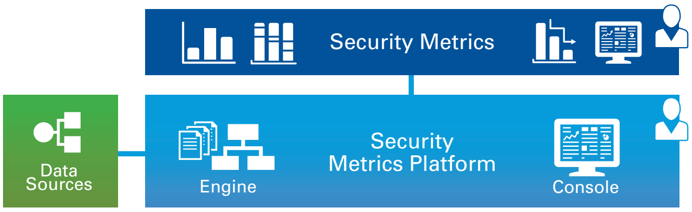
All of which means you can confidently take an increased level of action to detect malicious zero-day threats.

How does it work?

Flexeye works by building an outer data layer around its 'Engine.' This data layer is subject to an inner definition layer configured, maintained and reconfigured at the Engine's user console. From these layers the Engine builds its smart virtual asset model of the network which it uses as a basis for its powerful analytics.

The Engine's Universal Collector gathers the required data

Flexeye's engine can retrieve information automatically from a wide variety of sources including any SQL database for which there is a valid JDBC driver, excel spreadsheets, XML files, RSS feeds, Lotus Notes databases, any HTTP, HTTPS or FTP served files and others. For policy information data can be input via manual forms. Data can be collected on demand or on a scheduled basis, so your measurements are as current as you specify them.



End-to-end Platform

Flexible infrastructure modelling

The Engine's smart virtual asset modeller builds a complete, evolving and bespoke model of your organization, your networks and your assets. Measurement data can then be mapped onto this control to provide you with rich contextualized information. Data can be enriched further by using Flexeye's advanced analytics to provide derived metrics.

Techniques like asymmetrical modelling and linear regression enable a clear picture of historical, current and projected future data to be presented together, and solves problems like recognising single assets with multiple names in different sections of the business.

The Engine operates at a highly granular level of detail. This enables you greater control over roll ups and modelling.

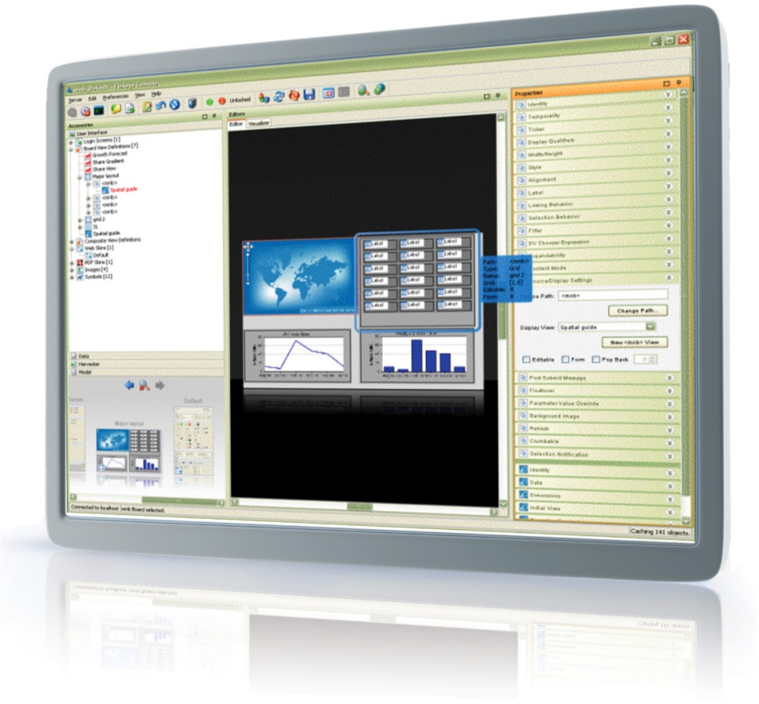
Personalised metrics visualization

The core engine is directed by a user friendly console which a single user with training can configure. From the console they can create security bound applications which present key performance indicators to a targeted audience.

If an exception presents itself, your employees won't just get a notification of an aberrant pattern, they'll know what business process measurement has been effected. And Flexeye's granularity allows them to drill down from this aggregated pictorial presentation to the individual exception to enable fast remediation.

Adaptable to existing architecture

The Flexeye Information Security Metrics Platform can be deployed in minutes. Its web-based and requires no special coding to integrate into your existing systems. There's no lengthy integration project, and there's no requirement to retain a specific high-value skillset in order to support it. It'll stay light on its feet.



Flexeye console: User experience design interface

Global top 10 Bank selects Flexeye

What do you do when your existing information security control measurement systems won't scale and are underperforming? This Global top 10 bank faced three key problems with it's legacy system:

- Struggling performance due to the increasing importance of security, and regulatory pressure
- Original systems engineers were unavailable to maintain and develop the system further
- Struggling to scale across the group.

Flexeye was selected for its powerful capabilities to collect, analyse, compute and distribute the information, and its flexible framework that allowed the system to be continually evolved.

Across the bank Flexeye now covers 50 security controls across 500 services and 250,000 PCs and servers. The system enables users from the CIO to service owners to determine their compliance globally by looking at personalized data visualisations, resolve non-conformities by drilling down to granular detail, and the systems modelling features supports the GIS business area in making risk and strategy decisions.

The Security Metrics Platform: A better way to bridge the performance gap.

There's a new model for bridging the gap between information security systems' actual performance and what's needed. It's called the Security Metrics Platform.

You won't need to worry about the delay between the time when a control makes a measurement and the time you're aware of it, you can specify it. You won't need to worry about the fragmentation of your controls across systems or geography as Flexeye pulls information from just about anywhere.

It brings all your control data together, compares it against an evolving smart model of your network assets and provides rich timely view of performance against expectation to users who are authorized to see it, on any device. And it'll do all of this on a massive scale.

Information security teams love it because it gets rid of the mundane grunt work of data harvest, processing and formatting. Information security management love it because it allows the team to spend their time on more value added activities like continually evolving the organizational model to provide greater nuance of response, or modelling proposed organizational or technical changes from an information security point of view.

What else would you expect from a technology built to solve the problem of how to correctly measure information security on a massive and evolving scale.

Global top 10 Oil and Gas multinational selects Flexeye

A global top 10 Oil and Gas multinational needed to give key security control and compliance indicators to the relevant stakeholders more quickly and effectively. The assets they wished to report on included approximately 160 sites each of which had one or more process control networks hosting an average of 400 servers. The challenge was to find a system which could collect data from multiple centres at maximum speed and precision.

Flexeye was selected over their existing GRC supplier for its *"powerful data collection capabilities, flexible infrastructure modelling capabilities and personalized metrics visualisation,"* said their project manager.

Through close collaboration the Flexeye team was able to able to review the datasets to add extra value.

"The system is so easy to use. It allows our security team to very quickly identify non-conformities with our internal policies and record and share strategies to reach compliance," reported a Senior Architect within the company.

Flexeye Security Metrics Platform

Is easily deployable, You can host it securely in the Cloud or it will sit on your own server.

Has a lower total cost of ownership built in. You don't need to make any changes to your existing architecture and there's no expensive time consuming programming integration project up front.

Can get going fast. You can download the software in about 20 minutes. It will be a few weeks before the system has enough data in it to provide meaningful feedback.

Has a powerful data collection capability. Flexeye's advanced big data integrator in the core engine can pull data from a wide variety of sources. It can do it when asked or to a user defined timetable, and if it can't get the data then it'll SMS you to let you know.

Keeps you informed of what's going on right now. Automatic Data Collection ensures your performance against KPI is as current as you have specified it.

Is continually evolving. The core engines scenarios fold back into the model enriching it, and its powerful asset on-boarding facility enable it to stay up to date in even the most agile environment.

Frees your information security teams time to concentrate on more value added activities than data aggregation. The core engine is configurable through a single, easy to navigate web-based console.

Flexible infrastructure modelling. The core engine's smart virtual asset modelling allow you to get in front of potential security threats by modelling different scenarios of usage, policy or asset change. This can provide an input into where you need to invest in your information security or the likely information security consequences of a business decision. Forewarned is forearmed.

Personalized metrics visualization. Flexeye displays key data in easy to read form, so authorised personnel can see at a glance what's happening in your information systems. These applications are easy to construct from a console onto the core engine.

Facilitates compliance. As Flexeye's architecture is based on the ISO 27000 standard it can help you align with the series and automate the documentation and reporting needed to prove and maintain it.

Has the power to be massively scaled. Parallel computation architecture and easy asset introduction in the core engine enable easy scaling.

Has collaboration built in to the core engine. The core engine is designed with social collaboration around control metrics in mind. Solve problems quickly by discussing them together as soon as they emerge.

Just what's so clever about Flexeye's Security Metrics Platform?

Hot deployment for a start.

This is Flexeye's ability to adapt and change without an operator having to stop the program and recompile it. It's a bit like buying a tailor made suit which adjusts itself when you ask it to 'tighten the waist', or 'loosen under the arms would you?'. Rather than a suit which has to be sent back to the tailor for a six month resizing project when you need it adjusted.

This is essential to maintaining an ongoing, accurate picture of your organization's information security. Why? Because your total information security is a sum of the security of all your individual assets. Flexeye's core engine manages this by creating a model of each asset in it's own right. This gives it an unrivalled level of detail or granularity.

We call these individual asset models Smart Objects. Smart Objects are encapsulated: they contain all the rules they need to operate. And each granular Smart Object can grab data, store data, compute data, ensuring it's own accuracy, signal to other smart objects, speak to other machines, they're able to present themselves on a screen, and they can hold business rules, like who gets the right to access them. They're very resilient, so if the power's cut, all of this data is retained.

So when the core engine builds a model of your organization's infrastructure, it's not building a database; it's building a computing machine: a community of living objects which interact with each other, and the assets they mirror in your infrastructure.

Each smart object is extensible: it knows the rules that govern its behaviour. It has 'ears' to hear a human operator asking it to modify a rule, or add a new one. Combined with it's ability to communicate with other smart objects, this creates a reflectivity within the community of Smart Objects: the ability to change and spread rules and parameters systematically, a process called directed evolution.

Security metrics need this ability for hot deployment and continuous adjustment to stay relevant to agile and cloud based infrastructures. And the granularity of the smart objects make getting to the root cause of an exception fast and easy.

The alternative is to commission an (often significant and costly) project to add functionality, then stop the program and recompile it to incorporate the changes. And when it comes to taking down your security monitoring and management, that's no alternative at all.

Yet, this is more than a technical or performance benefit, its an organizational one. Flexeye breaks organizations out of a vicious buying cycle. It's easy to get into a pattern whereby a system which fits well upon purchase, becomes less and less so over time, constantly decreasing until a new system is required. Flexeye establishes best fit upon purchase and adjusts incrementally to maintain best fit over the lifetime of the system.

Now that's clever stuff.

Why so clever?

- Hot deployment means your security monitoring and management is always on and always in a state of 'best fit'.
- Fine granularity, assets modelled at an individual level make viewing the root cause of an exception super-fast and easy.
- Directed Evolution within the system breaks your organization out of a vicious buying cycle caused by constantly decreasing fit as organisational, environmental, regulatory and other variables change.

How big an issue is cyber security really?

Both the US and UK governments take cyber security very seriously.

Iain Lobban, Director at the British Intelligence Agency GCHQ, puts the imperative well when he says 'Don't let cyber security become the agenda – put it on the agenda.'[1] Having monitored cyber attacks on British organizations CESG (GCHQs information arm) knows that the effect of a cyber attack on UK based corporations can be significant enough to have a negative effect on the whole economy. Like the leading UK Biotech company whose product was beaten to market by cheap foreign imitators because the firm's Research Director opened an infected PDF he believed was from a trusted source, which then bled away the fruit of over £1 billion of R&D.

The US is no less forthright in its treatment of cyber security issues: *"Securing the United States against cyber attacks has become one of the nations highest priorities."* [2]

How important is monitoring in Cyber Security?

Whilst the challenges are not just technical, the US advice adds in its introduction, that a *"critical component of such a defense system is continuous monitoring – that is, the ability to automatically test and validate whether current security measures are working and proactively remediate vulnerabilities in a timely manner."*

Monitoring is a key theme picked up in the advice to UK Executives: *"The board should seek assurance that key information risks are both assessed and prioritised, and that there is regular monitoring where threats and vulnerabilities are constantly changing".*

Sources:

1.10 steps to cyber security: Executive Compnaion. Available at http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive.pdf p.2 CESG 2012

2. SANS 20 Security Controls. Available for download at http://www.sans.org/critical-security-controls/ p.3

What are the CSIS 20 Critical Security Controls?

In 2008, facing a myriad of possible cyber security controls, the US Secretary of State for Defense asked for help to prioritize them. How should the US government best use its resources to fight cyber infiltration? The National Security Agency (NSA) picked up the request and developed a list of controls which worked it's way out through US defense, government and business, and became accepted by the UK in 2011.

The strength of the 20 is in the principle, that was a mantra amongst the White House cyber security team, that 'offense must inform defense'. This meant that for inclusion in the list controls must be matched to known threats. There's no room on the Critical List for controls against theoretical vectors.

Surveys since have shown that around 80% of breaches could have been prevented if the list of 20 had been implemented and active at the time of infiltration.

The 20 are:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defences
6. Application Software Security
7. Wireless Device Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defence
14. Maintenance, Monitoring, and Analysis of Security Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Loss Prevention
18. Incident Response Capability
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

Links: http://www.sans.org/critical-security-controls/

Summary and conclusion

Organizations' information security systems have been put under enormous pressure by a convergence of complex threats, organizations aspirations for agility organization, and employees non-compliant by nature. Doing more of the same to reduce risk has become proportionally more cumbersome and less effective.

Flexeye protects your organization by:

- Automating massive data gathering and analysis tasks
- Making KPIs ultra accessible, current and individually tailored
- Allowing users to drill down to a granular exception immediately
- Predicting the future with very smart modelling techniques
- Freeing your information security team to proactively fight threats
- Adapting fluidly all the time

So join some of the world's leading corporations, close the gap between the actual and needed performance of your organization's information security systems.

We're excited about the possibilities that Flexeye offers for securing organizations like yours against current and future threats. To get us listening to exactly what you need, email sales@flexeytech.com or call +44 1483 306060.

Flexeye, the company

Flexeye's reputation has been built by the people behind it. We are a mid-sized, tight-knit technology company of high calibre individuals, well used to dealing with big issues on behalf of big organizations.

We employ the brightest business, system and data analysts, along with the smartest software developers. Thanks to them we can present our clients with precise, cost effective and easy-to-operate systems. Many of our team have backgrounds in vertical sectors including finance, healthcare, telecommunications with expertise in audit, risk, security & compliance. They also have extensive experience working with large, multi-national corporations and governments. Many of our managers came to us from major consulting companies including IBM, SAP and TATA.

Flexeye combines its skill and experience with its technology platforms to give our clients systems theyneed, rapidly. That many international enterprises including leading banks, telcos, pharmaceuticals, media and technology companies use our systems is a reflection of the high level skills of our software developers, and the power of our technology.

Sales:	sales@flexeyetech.com
Support:	support@flexeyetech.com
Head Office:	Hays House, Millmead, Guildford, Surrey GU2 4HJ
Phone:	+44 1483 306060
Website:	www.flexeyetech.com