Factsheet

cyber security

Detection is Not Enough: Effective Management of Today's Complex Cyber Threats

Information security has become non-optional to organizations and should be viewed like any other integral business function—one that delivers clear value and benefits. Too often, security is viewed as something of a nuisance, a 'must do'. Atos believes that, in addition to protecting your enterprise, information security should add value and help a business achieve its overall goals.

Security excellence allows you to:

1. Focus on your core competence (which is rarely security itself). Whatever sector your company is in, your chief goals are to increase customer satisfaction and retention, and improve financial performance.
2. Achieve the kinds of returns you expect from other business investments. Many companies have non-integrated point security solutions which cannot provide an integrated view of their security. The total value provided increases as point solutions are combined into one holistic system.
3. Reduce compliance costs. As automation and reporting increases, (for example, via log management), less needs to be spent on auditing and compliance 'by hand'.

These benefits should be viewed in concert with the threat management that security is usually associated with. Today's newest threats (in the form of Advanced Persistent Threats, or APTs) are focused on information theft and on the business itself—on acquiring business secrets, exfiltrating crucial customer data and simply stealing money. More traditional threats remain in place as well, and these can be every bit as damaging—denial of service attacks can cost a company millions in terms of lost revenue and dissatisfied customers.

How Atos Cyber Security works For You

AHPS (Atos High Performance Security) SIEM (Security Information and Event Management) and CSIRT Service (Computer Security and Incident Response Team) work together to detect and remediate security issues, while adding value to your business as a whole.

> 4th quarter profits fell more than 40% for $73 billion retail franchise, Target Corporation, largely because of a security breach.

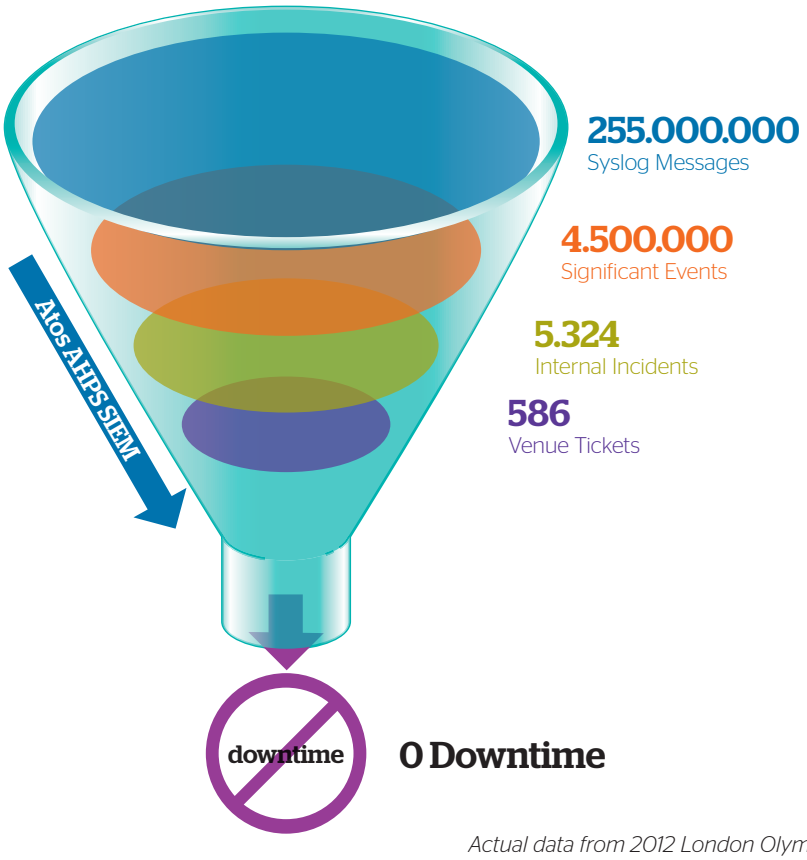
AHPS SIEM detects malware and abnormal activity. Cyber security does not suffer from a lack of information but from having either too much information or a lack of visibility of crucial information. AHPS SIEM and its security engineers gather, combine and analyse log data from a wide variety of sources to detect anomalous activity. By using a correlation engine and rules tailored to your specific enterprise, AHPS SIEM uncovers threats that might be hidden if only a single point solution were analysed.

AHPS SIEM can be considered a security integrator that brings together point solutions and leverages them to provide a detailed picture of your security posture. Trained engineers monitor activities from a wide variety of devices and then raise alerts as needed.

The net result is shown on the next page: millions of potential incidents are filtered down into an actionable few. The noise is removed, leaving behind the abnormal activities that require analysis. The numbers provided are those gathered from our work securing the 2012 Olympics.

But, detection itself is not enough. What is needed is a team that can not only respond to alerts but also manage them effectively through to resolution.

AHPS SIEM resolved millions of potential events down into zero downtime



Actual data from 2012 London Olympics

The CSIRT service analyses potential incidents and determines their severity, priority and the procedures for threat mitigation.

Don't get distracted: Focus on your business, not on hackers.

The CSIRT keeps your company informed of alerts and their progress through to resolution. Not only can the CSIRT perform incident resolution, it can also provide services that complement AHPS SIEM—for example, Threat Management and Forensics.

Threat Management helps companies stay on top of the wide variety and ever-evolving threats in the market through global intelligence feeds of emerging threats, known vulnerabilities, and Microsoft security updates.

The CSIRT can also provide Forensics to help discover the root cause of security breaches, prevent breaches from happening again, and engage with law enforcement if needed.

The net result of AHPS SIEM and CSIRT is that today's sophisticated threats are both detected and remediated by security professionals.

Benefits

The benefits that AHPS SIEM and CSIRT provide are concrete. These include:

1. Facilitation of compliance

AHPS SIEM supports compliance efforts while reducing the total cost of achieving compliance. Companies can spend a great deal of time and on compliance—AHPS SIEM automates many aspects of compliance activities and thereby reduces costs substantially.

2. Focus on your business

The overwhelming majority of enterprises do not have security and risk management as their core competence. Security for a typical company is a distraction from the core business. By using AHPS SIEM and the CSIRT, your company is able to focus on what it does best while improving security readiness.

3. Reduce costs and improve net security value

AHPS SIEM and CSIRT are managed services and as such make expenditures more predictable, and without upfront investment. More subtly perhaps, AHPS SIEM and CSIRT provide a steady stream of security excellence. Instead of hiring expensive, permanent staff your enterprise 'rents' the best security tools and people available. The net value from your security investment increases–you pay less while getting more.

4. Vastly improved security posture

AHPS SIEM and CSIRT improve your company's stance with regard to a wide variety of potential security incidents. Today's sophisticated threats, such as APTs, require sophisticated defense and remediation that AHPS SIEM and CISRT offer.

5. Improved total risk management

Risk management is one of the most fundamental business functions. While most people are aware of financial risk management, many underestimate the damage that could be caused by a severe security breach (perhaps the Target incident will change that, perhaps not). A single security incident may prove catastrophic. In today's 'hacker-rich environment' the risk of a catastrophic attack is high. Security excellence is now mandatory as part of any broad risk management program.

Under the Hood:
How AHPS SIEM and CSIRT Work

The IT estate produces a wide variety of log files from a diverse range of devices, applications and servers. These log files are the fundamental inputs into the AHPS SIEM and can include vulnerability management, intrusion prevention, firewalls, malware scanning, and so forth.

A typical AHPS SIEM deployment uses local log collectors to gather and filter local events. The main AHPS SIEM engine resides in the 'cloud' at a secure Atos data centre.

AHPS SIEM has two main 'components'. First is the SIEM engine which correlates information gathered from the log collectors, using rules and templates designed specifically to your company's security policies and based upon Atos' broad experience in protecting our hundreds of customers across the globe. Second are the trained and experienced analysts who focus on a wide variety of functions, including collector and template design, and analysis of security information. Some AHPS SIEM templates are ready-made (for example, for PCI compliance) and others are created to reflect your particular requirements.

Today's advanced malware may encompass multiple devices and multiple phases—for example, an emailed PDF being opened, followed by atypical network activity, such as callbacks to unfamiliar URL's. These activities need to be correlated (rather than viewed separately) to detect a possible security incident.

AHPS SIEM engineers drill down into alerts to fully understand their context and to determine if they are suspicious or not. Atos analysts produce information-rich reports and communicate with Atos personnel and Atos customers to inform them on a regular basis of their security posture. A customer cockpit is used to facilitate this.

Detection of suspicious activity is mandatory, but problem resolution is obligatory as well. This crucial part of the process is provided by the CSIRT service. When suspicious events are detected by AHPS SIEM, CSIRT personnel are informed and they perform further analysis and problem resolution. The goal is to achieve the zero downtime that we have achieved at the Olympic Games.

The CSIRT service also performs policy design and review, and configuration recommendation, which helps to tune AHPS SIEM to your specific requirements. They also use a knowledge management system to prioritize events. This improves both the operational excellence and transparency of the CSIRT. The CSIRT keeps customers informed of problem status and the progress towards issue resolution.

AHPS SIEM and CSIRT are modular in design so our customers can 'plug' into Atos managed security services at any step in the process. Clients who operate their own security infrastructure can subscribe to our AHPS SIEM service to take advantage of Atos deep expertise in threat detection. Alternatively, customers who already have their own SIEM can opt to have Atos CSIRT service track and resolve problems detected by the customer's own SIEM, and/or take advantage of CSIRT's forensics and global threat management services. AHPS SIEM and CSIRT are flexible services that can be adapted to meet your company's specific business requirements.

Leveraging the Olympic Experience

Atos has provided the entire IT for the Olympics including all key security services since 2002 and will continue to do so until at least 2024. The Olympics has not had a single business interruption due to an IT security incident in the 12 years we have worked with them—this despite the Games being an extremely rich target for hackers.

AHPS SIEM has evolved from that experience. The expertise gained from our work securing the Olympics is used to make AHPS a world-class SIEM service, one that can be relied upon to protect your business.

About Atos

Atos SE (Societas Europaea) is an international information technology services company with 2013 annual revenue of €8.6 billion and over 76,000 employees in 52 countries. Serving a global client base, it delivers IT services in 3 domains, Consulting & Technology Services, Systems Integration and Managed Services & BPO, and transactional services through Worldline. With its deep technology expertise and industry knowledge, it works with clients across the following market sectors: Manufacturing, Retail & Services; Public sector, Healthcare & Transports; Financial Services; Telco, Media & Utilities.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. It is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is quoted on the NYSE Euronext Paris market. Atos operates under the brands Atos, Atos Consulting & Technology Services, Worldline and Atos Worldgrid.

For more information, visit: atos.net

For more information:
Please contact **security@atos.net**