The first SIEM products were introduced 10 years ago to solve a big data perimeter problem. Routers, firewalls and IDS tools were all generating a multitude of events that needed to be combined, filtered and turned into information. This made it possible for security operations staff to identify threats and then be able to respond to attacks.

Over time many products (including HP ArcSight SIEM) have expanded their capabilities to look across an ever expanding IT landscape. This landscape encompasses servers, databases, applications, vulnerability information and virus scan results, SCADA infrastructure, etc. Significantly, this also includes the people behind the actions. This process utilizes real-time collection; normalization and aggregation of log data from, potentially, thousands of sources. Advanced correlation processes are applied to identify suspicious patterns that could be specific to each individual business.

This is good news for the hard-pressed CISO or CIO whose world is getting more complex every day. It is obviously hard to maintain a reliable record of what is happening on networks and architecture – and it’s getting harder all the time.

New ways of working in the enterprise – outsourcing, consumerization, virtualization, mobile and cloud – have resulted in a huge uplift in data calls and data transfers, driving additional log entries across the enterprise.

“SIEM is about consolidating and analyzing millions of security-related events coming from the logs generated by network devices and other security products to find and highlight actionable security incidents” Jay Huff, EMEA Director, HP Enterprise Security Products

Key challenges that SIEM can help with

It defends the organization against aggressive external threats including APTs: HP has been dealing with threats for profit (organized crime/nation state), but now also has to deal with threats that are more political or social in nature. Attacks are also targeted, persistent, well organized and happen over a period of time and below the radar.

- Defend against malicious or compromised insiders, creating a bigger risk in increasingly tough financial climates
- Ensure that IT policies are adhered to and that supported products are functioning within normal parameters
- Assist in significantly automating compliance; reducing time and effort in preparing for audits
- Monitor and audit file downloads and data transfers
- Effectively identify and manage false positives
- Understand and effectively police configuration changes across the network

Security Information and Event Management (SIEM) is fast becoming an essential tool for security professionals faced with an increasingly complex mixture of cyber threats, rapidly changing work patterns and increasing legislation.
The SIEM advantage
The new generation SIEM systems offer a unified state-of-the-network overview in an easy to understand dashboard display.

The best SIEM solutions can display a comprehensive, real-time overview of data flows and event logs recorded across the enterprise right out to the managed endpoints.

The i in SIEM
Some argue that it would be more accurate to attribute the "i" in SIEM to "intelligence", because the very best solutions offer a set of data that gives a valuable insight into the workings of the enterprise in terms of data flows and data efficiencies. It can be a valuable business as well as operational tool. Some ways in which SIEM offers more than just security are:

- Organize data for long term storage and meet compliance demands e.g. PCI-DSS
- Monitor employee server and data requests and flag suspicious or unusual activity
- Alert unauthorized configuration changes to servers and virtual machines
- Track specific application usage and bandwidth consumption levels for devices across the enterprise right out to the endpoint
- Determine real network breaches against false positives and deliver administrative efficiencies
- Ensure anti-virus and patches are up to date and functioning
- Generate error and breach reports and identify cause and system vulnerabilities
- Identify best efficiencies for third party security tools and improve ROI

Calculating ROI for SIEM
Making a business justification for investing in SIEM technology is often the hardest part of the security project. The value of security investments can be realized in the form of “soft benefits,” such as increased situational awareness, reduced organizational risk, broader security visibility and better brand awareness – benefits that are hard to compute.

However, hard figures can often be calculated up front and verified over time. The business justification of a SIEM investment can be quantified by looking at cost break-even points, and the costs (or fines) avoided with the SIEM solution.

Choosing the right SIEM for your business
While there are obvious business benefits to installing SIEM, it is not a magic box of tricks, nor a silver bullet to all business problems. “Often one of the main challenges in implementing a successful SIEM solution is that of scope management. The capabilities of any SIEM solution are, ultimately, only limited by the inputs available, tied in with the business logic that drives the reporting and alerts created by the system. Thus the participation of Project Management in addition to the business is fundamental to any SIEM project and its importance should not be underestimated.” Chris Roberts, SIEM Practice Lead, HP Enterprise Security Services.

There are some additional caveats that you must bear in mind when considering SIEM:

- Think about your key objectives when implementing SIEM
- Compliance, data management, application management, security efficiency
- Ensure you have some basic analysis built into your solution
- A pile of logs on its own is worthless
- Train the right people to interpret the reporting output
- Meaningful actions based on log information
- Deploy scalable solutions
- Flexibility to change as your business needs develop

SIEM is much more than security. Think outside the “SIEM box” – work with your trusted security partner to tweak the SIEM to deliver real business intelligence to your enterprise.

In an age of data overload, a SIEM should make your life easier, not harder.

Videos:
What’s new in ArcSight Logger with Hugh Njemanze, ArcSight CTO
http://bit.ly/LSVmLb

How HP ArcSight assisted Vodafone

Case studies:
Real-life examples on how SIEM delivered ROI and other efficiencies:

How SIEM can deal with modern day threats:
http://bit.ly/L4wVx6