logpoint

SIEM – or Security Information and Event Management.

Quite a mouthful. So what does it mean?

Metaphorically speaking, SIEM is the Information Technology version of Closed Circuit Television (CCTV). In short: a surveillance system of all data within an entire IT landscape in order to catch intrusions, provide insight into operations and report on functioning.

SIEM. BUT DIFFERENT.

SIEM?! What's that?

CCTV: Preventing crimes before they happen.

Metaphorically, SIEM takes the most modern CCTV system and adds even more dimension.

It is like CCTV with extra crime detection/prevention, weather reports, traffic updates, shipping schedules, flood defenses, rail network and metro infrastructure.

Imagine a system that can alert you when it starts to rain, not only warning to get out your umbrella, but also putting more trains on the Metro to cope with the extra passengers, monitoring the cafes to ensure there is sufficient coffee, or alerting when a vending machine needs restocking.

A tool that gives you a sharp overview of vast and complex infrastructure, combined with the intelligence to review and comprehend what is happening – well, that's not merely SIEM. That's LogPoint.

SIEM?! What's that?

A Brief History of CCTV vs. Log Management

The First CCTV

Originally developed in the 1930's to monitor rocket launches, CCTV began to be used to remotely monitor people and equipment in the 1970's. A very basic instrument at the time, it could not record, replay, keep or store images. Unless you were watching it live, the event would be missed.

Log Files

IT Systems create log files for every activity, be it purely informational, or failures, or even successes. Log Files can also trace who performed the activity, when was it done, etc. However, log files are stored locally on each system, and unless someone can review each and every system, it is almost impossible to find everything. Just like the first CCTV, unless you are watching these logs in real time, the event will be missed.

CCTV Evolves

CCTV evolved throughout the 80's and 90's, gaining the ability to record and replay videos of people and activity – and this could then be used for investigation and criminal prosecution within the courts. Slowly, CCTV cameras began to appear everywhere.

Today, there are 207,431 CCTV cameras covering a large percentage of the city of London – a similar story for most European cities.

Log Management

This is the basis for the Log Management software from which SIEM has evolved – software that enables log collection from an entire infrastructure, storing them centrally, and time-stamping them for analysis. This offers better insight into how "the crime" happened and took place, who was involved, and how can it be prevented in the future.

But this still isn't SIEM as we know it today.

Modern CCTV

CCTV has developed at an amazing speed since the turn of the century. Not only can it now record and store data from hundreds of thousands of cameras, it can also recognize auto registrations and even faces – enabling real-time alerts that can:

- Be sent to emergency operators.
- Dispatch police – e.g., when specific people enters a city or area where they have been banned.
- Track and alert suspicious behavior and movements, such as with crowd control, loitering in street theft hot spots, or troublemakers entering a bar.
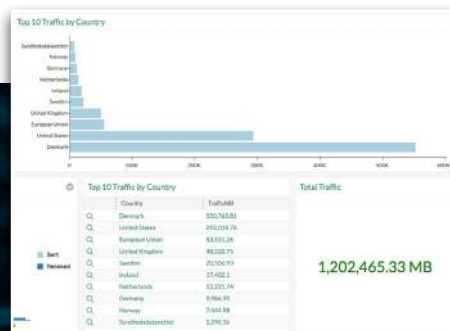
SIEM

Like the modern CCTV, LogPoint is the most advanced form of SIEM – capable of monitoring millions of log files every second, from every device in an infrastructure, detecting log patterns as they evolve.

LogPoint can:

- Regularly report on general activities.
- Identify bottlenecks and monitor the health of your IT infrastructure.
- Replay events to identify when, what and who was involved – providing evidence in criminal prosecution.
- Reveal how to prevent incidents from happening again.
- Alert administrators to security threats and system failures – before they even happen.
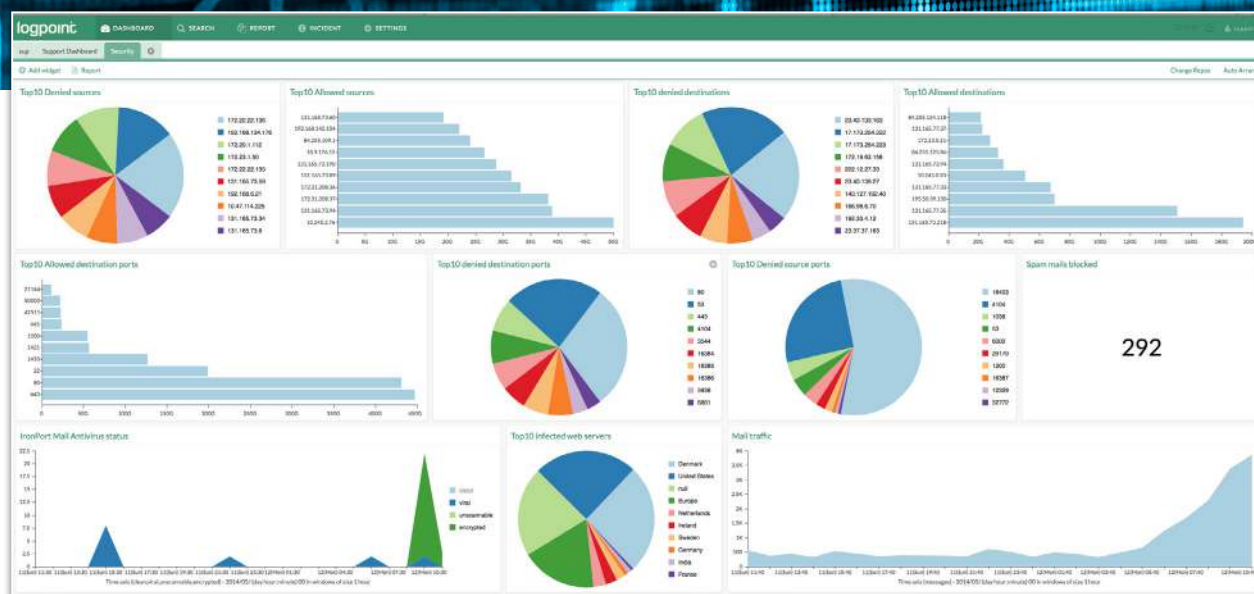
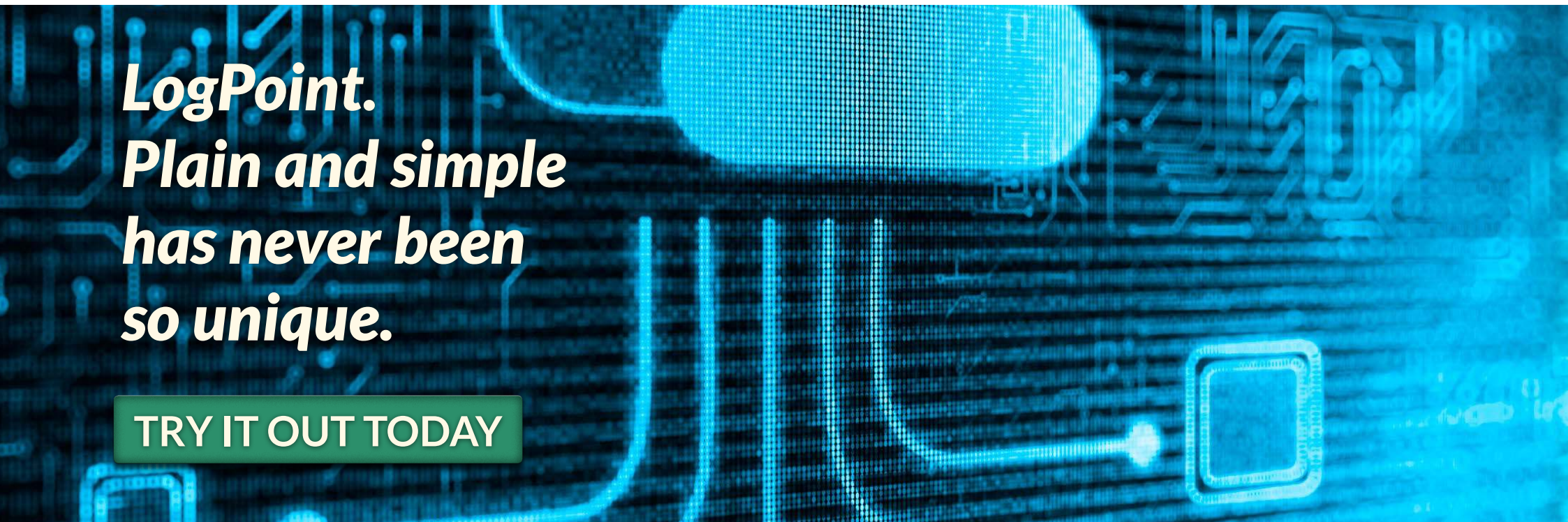*Metaphorically speaking, SIEM is the Information Technology version of Closed Circuit Television (CCTV).*

LOGPOINT.COM

SIEM?!
What's that?

LogPoint:
Real-time
risk alerting.

LogPoint.
Plain and simple
has never been
so unique.

LogPoint.
Plain and simple has never been so unique.

TRY IT OUT TODAY

SIEM. But different.
LogPoint is easy to use, agile by design and intuitive by nature. Find out about more about how your enterprise can benefit from the LogPoint difference.

Contact us for more information:

logpoint

LogPoint A/S
Aldersrogade 6A
2100 Copenhagen O

E-mail: info@logpoint.com
Telephone: +45 7060 6100