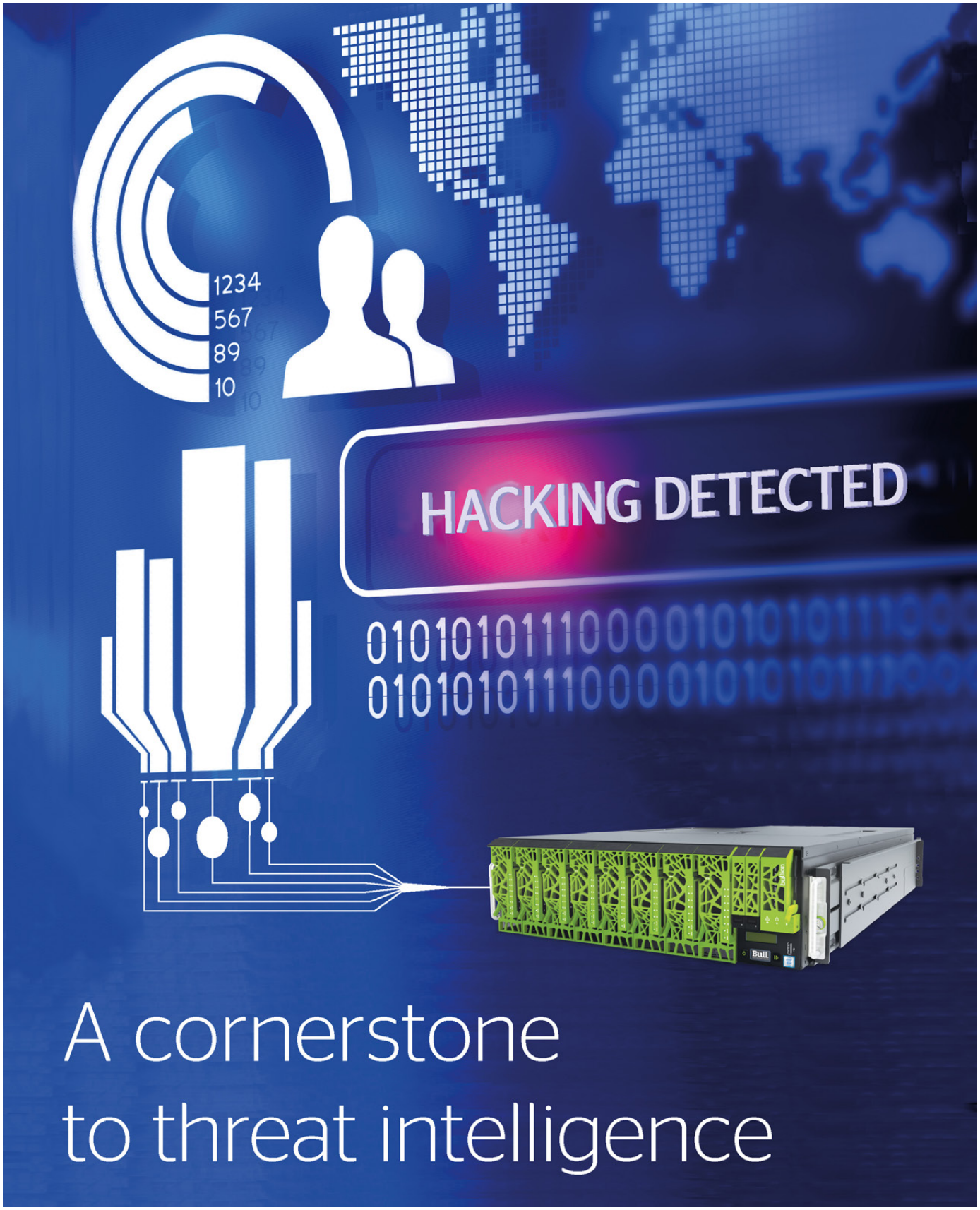
SIEM by bullion ™



A cornerstone
to threat intelligence

intel XEON inside™

Bull
atos technologies

Security information and event management (SIEM) systems are a cornerstone of threat intelligence. By bringing all data from various sources – hosts, servers, networks elements – to a central point and making cross source correlation, it enables a centralized reporting and analysis.

Today, most SIEM appliances on the market are relying on many different commodity servers each with a piece of specialized software, on a one server – one function basis. This leads to limited scalability and efficiency.

SIEM by bullion, consolidates inside in a single high-end enterprise server (2 in HA mode) many virtual machines (VMs) each one delivering a specific function. It enables a smooth data center integration and easy connection to other security services. The main benefits are simplified architecture and operations, extended scalability, improved security and TCO reduction.

SIEM by bullion may be teamed-up with value-added services from Atos to form an end-to-end solution helping organizations to anticipate, detect and manage their digital security risks.

SIEM: a cornerstone to threat intelligence

The SIEM adoption is driven by the customer's need to apply security analytics to event data in real time for the early detection of targeted attacks and data breaches. It collects, stores, analyzes and reports on log data for incident response, forensics and regulatory compliance.

SIEM technology aggregates event data produced by security devices, network infrastructures, systems and applications. The primary data source is log data, but other sources such as network data, may also be processed. Event data is combined to provide a context about assets, threats and vulnerabilities.

SIEM simplifies regulatory compliance

Many organizations deploy SIEMs only to streamline their compliance reporting efforts with a single tool, as standardized report are embedded. Without a SIEM collected and centralized data, it may be necessary to generate individual reports for each host, manually retrieve data periodically and reassemble it to generate a single report. This can be incredibly difficult and costly because different operating systems, applications and other pieces of software are likely to log their security events in various proprietary ways. Converting all of this information requires extensive efforts/code/customization.

By leveraging a SIEM, an organization can save considerable time and achieve its security compliance reporting.

SIEM infrastructure challenge

The SIEM market is driven by software vendors who bundle different pieces of software on a collection of servers and deliver a whole package. In most cases, the market appliances rely on the following components:

- log receiver, manager and archiver (most of each are doubled for HA reasons)
- application and system data monitor
- role based correlation engine and other real time analytics
- central console for management.

The underlying commodity servers are sized for a range of events per second (EPS – main SIEM metric), according to the hardware limits and software scalability. If software often scales pretty well, hardware scaling is another issue. This leads to unused processing power or capped operations capabilities. This results in either limiting the spectrum of analyzed data and thus risks not detecting threats or "rip and replace" the selected appliance component thus impacting the solution TCO (Total Cost of Ownership).

SIEM infrastructure specifications

According to those architecture constraints, and to enhance a customer experience, an optimal SIEM architecture should be:

Simple: fully engineered with one stop shop and support and smoothly integrating in the IT landscape

Scalable: scaling alongside the needs enables to ensure optimal threat protection and quick delivery of compliance reports

Flexible: being available as an appliance or a tailor-made solution enhance the value proposition

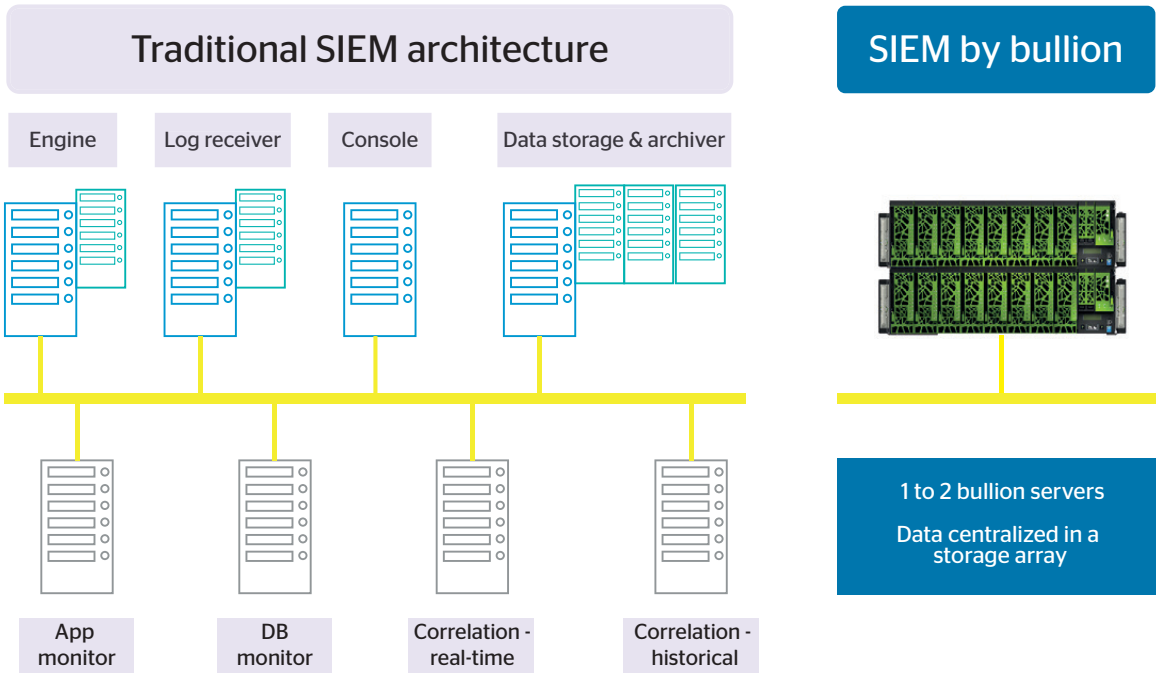
Efficient: limit the data center footprint, optimize the TCO and protect the investments is a must

SIEM by bullion: the optimized SIEM infrastructure

Bullion high levels of performance, scalability and flexibility to virtualize the SIEM

SIEM by bullion is the Atos appliance based on it's unique x86 Enterprise server bullion, a virtualization technology (from VMware ®), an enterprise storage array (Unity® from EMC®) and a SIEM solution (from Mc Afee®). Designed to meet the need for Data Center optimization, bullion is based on Intel® Xeon® E7v4 processors. Bullion – which is positioned among the best servers in the SPECint benchmark and SPECvirt tests– scales from 2 CPU/48GB RAM up to 16 CPU/24TB RAM, thus is the x86 server capable of delivering a reliable, flexible and cost-effective response to all types of data processing. Adding more computing power is just a formality; thanks to the latest generation of the Bull Coherence Switch (BCS) – for simple interconnection of up to 16 processors.

Atos engineered and validated SIEM solutions - with software partners like Mc Afee® and RSA® - on a virtualization layer. This means that all single function servers found in a classical SIEM architecture are consolidated within a single scalable server. A storage array centralizes all data and provides the required high-availability storage wise. This enables to optimize data center resources (rack space, network ports, addresses, cooling, power ...) like in every consolidation project through virtualization. Moreover it reduces the infrastructure cost of the global solution and thanks to virtualization smoothly integrates it in the datacenter.



An open appliance or Tailor-made Integration

SIEM by bullion solution is declined in 2 different modes for more flexibility; an appliance (turnkey to optimize time to market) and a Tailored Datacenter Integeration (TDI – to reuse some data center components).

The appliance will be most suitable for critical productions, as it is a fully engineered solution with one stop shop and support and optimized time to market. It is fully scalable, moreover with the virtualized layer, it is very easy to integrate in the IT landscape and connect to the other security components.

Tailored Datacenter Integration is a way to architecture and implement a SIEM environment to utilise existing components. For example, a SAN storage array can be reused in a client Data Center, with some dedicated SIEM disks. It is also possible – for reasons of hardware consistency and skills – to opt for a particular storage technology provider and still taking full advantage of bullion benefits and a validated virtualized architecture. So TDI addresses different needs from the appliance, with on-site integration and increased flexibility.

SIEM by bullion: the most advanced SIEM architecture

In the SIEM context bullion virtualized solution will specifically provide:

Improved security: SIEM by bullion enables more correlations at the same time, faster analysis and deeper analytics due to the high performance architecture. This improves security by reducing false positives and shortening dwell time. Moreover it's very simple to expand capacities to analyze new sources of data containing additional information.

Efficiency: with its huge processing power and RAM footprint and extreme scalability, the very same material can host all functional VMs in a single server - or be shared among 2 to provide High availability. This enables performance improvements (as network communications are done inside the same very powerful server, reducing latency), simplified operations (less efforts to manage a single server with VM, easy resource provisioning and reallocation) and cost savings.

Those benefits are delivered thanks to bullion **modularity** and **scalability** - the same bullion technology can be used for any SIEM deployment from 2 000 to 100 000's of EPS very simply. Indeed a bullion module is able to deploy an environment larger than 50 000 EPS, and 8 modules can be easily interconnected as a single server.

Reduce your costs

The SIEM by bullion aims at maximum efficiency and thus save costs through different domains:

- Optimized infrastructure costs: compared to the appliance competition, the SIEM by bullion may achieve 30 to 35% infrastructure cost savings thanks to virtualization technology, reduced hardware and software investments and limited network footprint.
- Reduced operations costs: SIEM by bullion relies on a highly efficient infrastructure which reduces significantly the cooling, saves up to 50% power consumption and simplifies human operations and maintenance.

Towards a successful SIEM / SOC project

A successful SIEM project relies also on professional and expert services. Atos is strongly committed to deliver a full range of services from consulting (security, infrastructure ...) to integration expertise to ensure successful SIEM implementations.

Atos proposes a dedicated or mutualized turnkey security solution: the Security Operations Center (SOC). The SOC enables to anticipate, detect and manage digital security risks embarking also a SIEM (should it be on premise or managed). The SOC solution integrates seamlessly with security policy. It strengthens the protection and governance of IT systems, for effective and sustainable cybersecurity.

The SIEM by bullion is paving the way to prescritive security. Different tools will side the SIEM like 'Big data/data lake' platform crunching data to ascertain trends and "Big data/ machine learning" to automate the detection of anomalous activities. All of them can rely on bullion to provide the benefits of consolidation, scalability and TCO optimization.

www.bull.com/SIEMbybullion

CT_17021O_LPM_F-SIEM_by_bullion-en1