NTT Security

Technical Insight

Can Security Information and Event Management tools deliver security benefits and business value?

In today's landscape, security information and event management (SIEM) is an important piece of any organisation's security strategy. It helps organisations to protect business operations and intellectual property, meet compliance obligations and ensure availability of key online services by providing valuable insights into threats and attacks, which in turn enable better detection and faster response to security incidents.

There are many excellent SIEM technologies on the market, but organisations are increasingly recognising that such technologies do not deliver the expected benefits unless there is a corresponding and continual investment in staff and operational processes – challenges which are complex, difficult to deliver in practice and often prohibitively expensive.

Specifically, organisations wishing to operate their own SIEM tool typically have to overcome problems such as:

- **Making the business case for significant capital expenditure** – to fund SIEM technology purchases, together with the associated professional services resource needed to ensure the tool is correctly implemented and configured as well as supporting the ongoing development of new reports, addition of new log sources, and response to continual changes in the estate such as firewall upgrades or re-architectures
- **Ensuring sufficient skilled and dedicated internal resources available to provide effective 24x7 monitoring and analysis** – provision of a core business hours operation only is increasingly seen as insufficient, as it is unable to respond sufficiently quickly or consistently to incidents such as loss of customer data or intellectual property, service downtime, brand damage, or loss of income/revenue
- **Lack of threat intelligence to detect more advanced threats** – attackers are now highly sophisticated and agile, and can therefore evade traditional, commercially available threat data sources which are limited in their breadth and relevance to organisations
- **Difficulties in attracting, training and retaining in-house skills to accurately interpret the alerts raised by the SIEM tool** – without the expertise to filter out or prioritise the alerts effectively, organisations risk drowning in information or else missing true incidents, which become lost amongst the noise of false positives
- **No economies of scale** – working independently to defend your organisation means operating without the ability to reuse or benefit from what other organisations are seeing in the wider threat environment and how they are responding to attacks. With the scale of the challenge which we all face today, it is often simply impractical for the vast majority of organisations to defend themselves effectively within their available budgets.

The result of these challenges is that many SIEM deployments do not deliver the envisaged benefits and are therefore classified as failed projects, leaving the organisation no better protected than before.

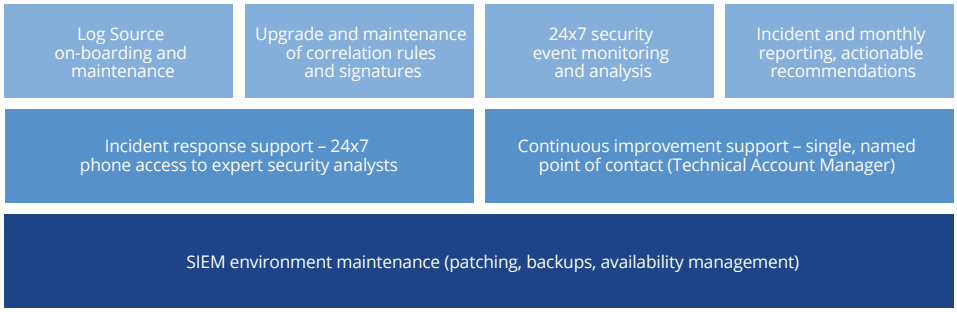
Security Information and Event Management – the Service-led approach

NTT Security SIEM-as-a-Service (SIEMaaS) addresses these challenges by delivering a comprehensive security monitoring and analysis service based on:

- Global threat intelligence network, backed by the NTT Group, and unmatched in the industry
- Large team of expert, highly qualified security analysts, with a passion for security and battle-hardened through decades of exposure at the front line of security defence
- Rapid alerting and 24x7 incident response support
- Clear, pragmatic, actionable incident reports
- 24x7 telephone and email support and advice
- Monthly reporting and engagement with customers to help build a culture of continual improvement and risk reduction
- Constant tuning of the service, based on experience of attacks across our client base, to ensure continued alignment to your changing business needs and risk appetite
- 'Pay as you grow' OpEx model, offering flexibility and controllable costs
- Dedicated Technical Account Manager to help place recommendations in the context of your business and act as your trusted partner in meeting the security challenges of your organisation

NTT Security SIEM-as-a-Service is a flexible service with R&D outputs, threat feeds and analysis techniques being added on a constant basis. Backed by the power of the NTT Group, based on a fourth generation platform and coupled with over 20 years' experience of protecting organisations across sectors as diverse as Financial Services, Government and Defence, Retail, Manufacturing, Pharmaceuticals and Gaming and Leisure, our SIEM-as-a-Service will ensure we keep you ahead of the threat.

Figure 1: SIEM-as-a-Service – Service Model Overview



Service architecture – our philosophy

Unlike many SIEM-based services on the market, NTT Security SIEMaaS has been built specifically to enable the large scale capture and correlation of both security and non-security device log source feeds. It also has the flexibility to evolve at the pace of the rapidly changing threat environment. Key attributes of the underpinning architecture include:

- Building the solution on one of the best log indexing tools on the market, enabling rapid, highly flexible search and categorisation of logs, and allowing the ongoing development of additional in-house functionality
- Recognition of the value and importance of humans-in-the-loop to provide context and judgement which systems are unable to deliver
- Ability to accept the widest possible range of threat intelligence feeds
- Automated filtering of false positives and prioritisation of alerts
- Analyst-centred user interface, together with the removal of all unnecessary operational tasks, to maximise the time analysts can spend on identifying attacks
- The ability to develop and incorporate additional features quickly and easily
- Rapid access to historical data such as previous attacks and incidents, enabling security analysts to apply lessons learned to the whole customer base
- Easy and cost-effective scalability

NTT Group Security threat intelligence – keeping ahead of the threats

The threat landscape is becoming ever more hostile, and threat intelligence needs to draw upon the widest possible range of sources and evolve continually to stay ahead of the game. NTT Group Security threat intelligence, a core component of NTT Security SIEMaaS, enables clients to benefit from:

- Over 30,000 websites scanned across the world each day to identify global threat trends
- A widespread network of global, automatically dispersed and configured honeypots
- Unpublished blacklists internal to the NTT Group – harder for attackers to detect
- A large team of research and development staff dedicated exclusively to identifying new threats and continually improving detection logic
- Continual enhancement of the threat intelligence picture by security analysts identifying threats and attacks in other customer environments
- Constantly updated internal incident databases
- Ability to contribute to and consume vendor-sourced threat intelligence
- Range of global CERT partnerships enabling sharing of newly discovered vulnerabilities and threats

Knowledge, not data – automated security analysis and the value of human enrichment

The SIEM platform uses a combination of highly-advanced automated security analysis and human enrichment, to convert the huge volumes of data, enabling in-depth understanding of the nature and severity of the attack on an organisation and practical, actionable recommendations as to how best to address the incident.

The automated analysis stage contains hundreds of custom-developed correlation rules and signatures which are continually maintained and updated to help filter out noise and retain only those alerts of potential interest and importance. Twin analysis engines – a real-time engine for detection of those attacks for which speed is of critical importance, and a batch engine for the low and slow attacks which seek to avoid the traditional detection mechanisms – are employed, with the resulting alerts being automatically classified and prioritised for further review by security analysts.

Armed with this information, the analysts will draw upon a range of other tools and information sources to further qualify the incident and ensure that the remediation advice is tailored to the client's specific environment. These include: access to global threat intelligence feeds, wikis, reference to client-specific action cards containing details of the client's assets, networks and applications and further queries of the raw log data. The resulting incident reports and associated technical/analyst support provide clients with all they need to know in order to address the risk to their business.

Figure 2: SIEMaaS – Illustrative deployment architecture

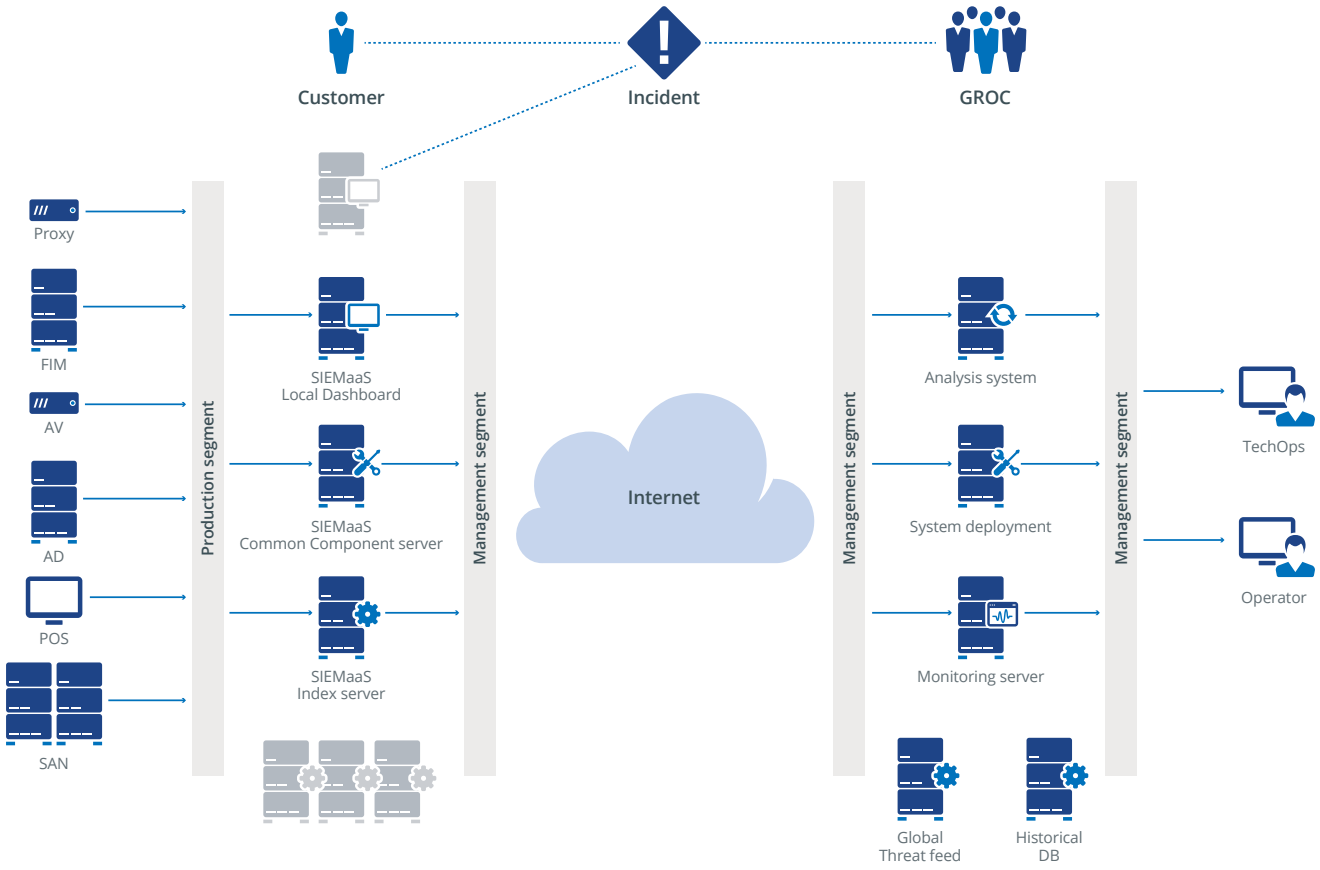
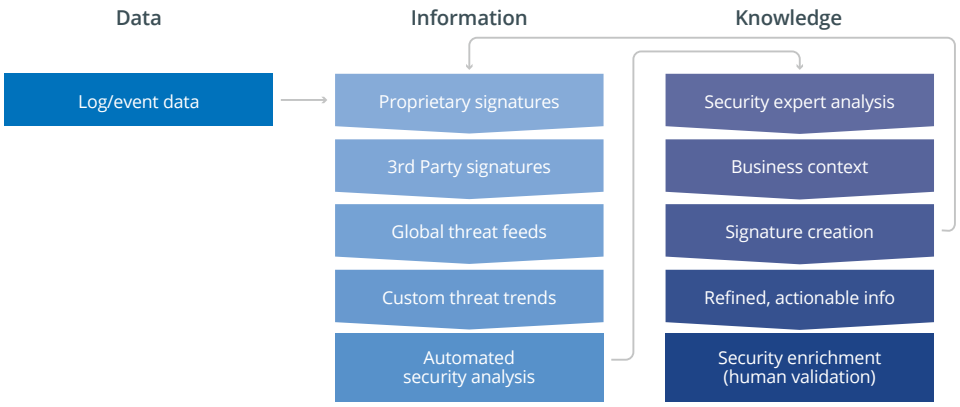


Figure 3.1: Process Overview – converting data into knowledge

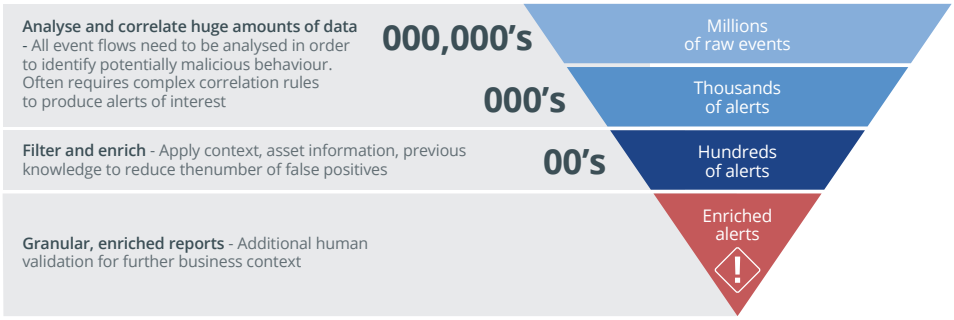


The benefits – greater visibility, faster incident response and more effective defence

With NTT Security SIEMaaS, operational security monitoring and analysis of your environment is in safe hands. The service delivers new levels of visibility and insight into the security posture of your organisation, and enables you to respond to incidents more quickly, and with greater confidence. Moreover, it enables you to move your organisation towards a more strategic, proactive approach to information security and risk management.

SIEMaaS is not a silver bullet for all security challenges of course. Nor does it replace the need to address the basics of security management such as well configured firewalls, mature patching policies and processes or strong intrusion prevention systems and management. Nevertheless, it has helped numerous customers looking for cost-effective ways to reduce risk exposure, support compliance obligations and free up resources to focus on helping their organisations succeed in the market.

Figure 3.2: Process Overview – converting data into knowledge



To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organisations to build high-performing and effective security and risk management programmes, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com**