MSSP GIANT ACHIEVES SCALE IN SIEM REPORTING

The MSSP provides multi-layered, full-service cybersecurity offerings to multiple enterprises across India. The Information Security Operations Center (ISOC)/Security Incident and Event Management (SIEM) team monitors their clients' network for vulnerability towards cybersecurity breaches, third party injections and other security attacks. Their task is to safeguard enterprises against threats of various kinds and origins as their clients' data moves between employees, offices, data centers and cloud applications.

It's 10 PM on Friday night and the team of IT security professionals are in the middle of their workday at the Secure Intelligence Center. Their task is to produce reports on all the security threats detected and managed till Friday evening for their clients. Each client's report is over 20 pages long and the data must be extracted and compiled manually. Each report takes between four to six person hours to compile, check and disseminate. The group must publish reports for about 30 clients today.

The team's work begins at the end of the business week, on Friday evening, and goes on late into the night and through the weekend. This week has been especially challenging since one of the team members has called in sick. The team fears that it will be Monday by the time the last of the clients will be alerted to the threats that could be a serious breach in security.

CHALLENGES

The ISOC/SIEM team analyzes and monitors events, applications and private as well as external hosts for their clients. The team identifies threats to client networks, takes action to combat them and reports them to stakeholders. The success of the team's efforts is key for ensuring the effectiveness of the countermeasures and to trigger timely corrective actions.

The SIEM team manually compiled their analysis into a weekly cybersecurity report pack. Pulling data and screenshots from multiple sources, these weekly reports included data from flat files, spreadsheets, web services as well as reports and screenshots from multiple tools. The weekly reports were also consolidated into monthly and quarterly reports, which were also prepared manually and were far more effort intensive.

THE MSSP WANTED TO AUGMENT CAPABILITIES WITH SIEM REPORT AUTOMATION

The MSSP quickly realized that capturing growth opportunities required introducing efficiencies in their reporting function. They set out to engage a partner who could accelerate their growth and partner with them for current as well as future transformative initiatives. Their goals were:

1. **INCREASED EFFICIENCY AND ACCURACY**
   Reduce error and improve efficiency in obtaining data from multiple sources, which is then collated into a single report.
2. **ACHIEVE SCALE**
   The capability to serve a larger number of customers without a corresponding increase in response time or breaching the SLAs.
3. **GAIN INSIGHTS**
   Explore correlations between currently siloed data, moving away from reporting towards analytics.
4. **STANDARDIZED, INTERACTIVE REPORTS**
   Rich user experience consistent across customers and the ability to create and reuse templates.

THE MSSP WORKED WITH INTELLICUS TO REALIZE ITS DIGITAL TRANSFORMATION PLAN

The MSSP decided to onboard Intellicus since they offered both a full suite platform as well as the capability to complement data engineering expertise with professional services. With Intellicus, the MSSP knew the solution would be tailor-made to their needs and Intellicus' expert guidance would ensure successful implementation.

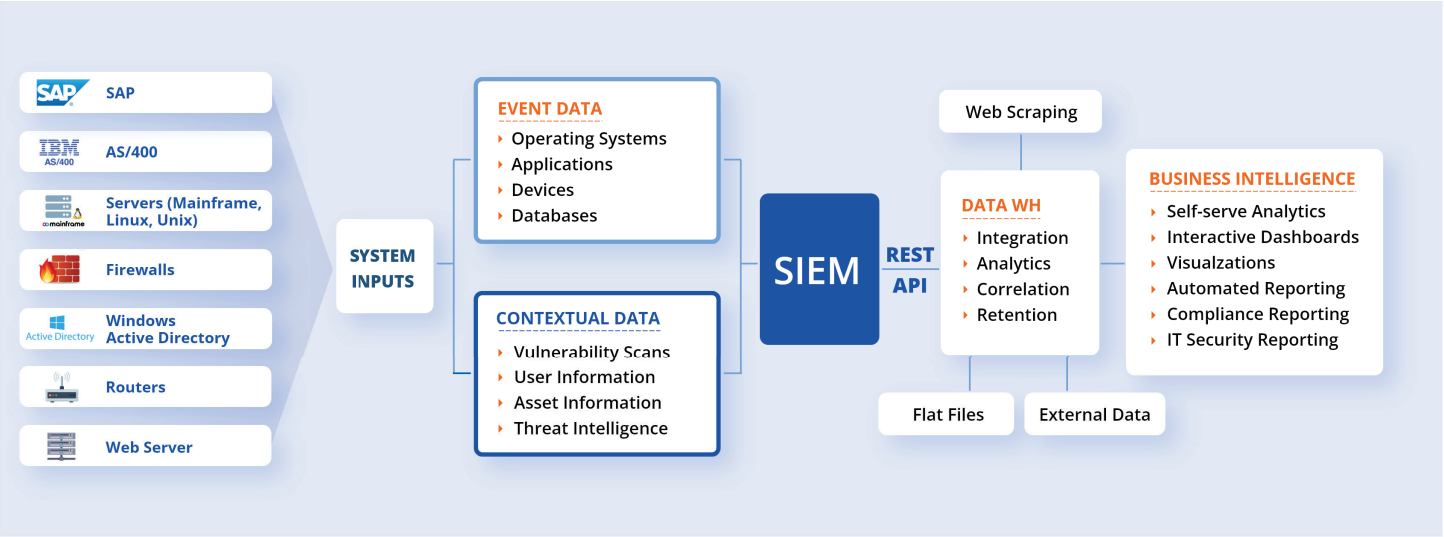
The key to solving the challenge of scale was automating not just the reporting, but also the data pipeline. However, Intellicus' team believed that the existing architecture would not support the speed and efficiency required for achieving scale. Pulling data directly from the current SIEM ERP and the other sources was not optimal for speed to analytics.

Intellicus' recommendation was supported by evidence gained from a test run on the existing architecture. Generating one client's report took an hour and a half, less than half the time needed for the earlier manual process. While the very significant improvement in efficiency was already a great win, Intellicus advocated changes in the fundamental architecture. Their analysis revealed that the main culprit was the time taken to fetch data from the SIEM raw storage using its REST APIs. Intellicus recommended adding a dashboard-friendly staging database into the architecture and creating a data warehouse (DWH).

DESIGNING AN ARCHITECTURE THAT ENSURES LONG-TERM SUCCESS

The proposed architecture would not only allow the possibility of correlating data, it'd do so without increasing the load on the SIEM ERP database. Additionally, some of the existing storage systems lacked a good query system, which is an absolute must for business intelligence and analytics readiness. The DWH allows joining internal as well as external data sources along with data transformation, correlation and aggregation—something not possible if data for analytics is pulled straight from the transactional database. The robust architecture was geared to meet the digital transformation needs not just for today, but to sustain growth through the next decade. It provided the power as well as the flexibility to serve the MSSP's purpose through any change of technology they would want to adopt for their growing enterprise.

> *At the test run, generating a report took a few minutes, down from the 4-6 hours needed for the manual process.*



CONTRIBUTING DATA ENGINEERING & BI SKILL

While the MSSP had a strong team with expertise in the SIEM domain, data warehousing required a special skill set not available within the organization. Facing this unprecedented need, the SIEM giant was faced with the challenge of addressing the gap in the expertise required for a successful BI implementation.

Intellicus helps companies in adding complementing skills sets

- BI architecture design
- Data modelling
- Implementing Machine Learning for Predictions
- Designing Interactive Dashboards
- ETL, OLAP, Multidimensional DWH
- Self-Service Reporting & Analytics Implementation

A scheduled ETL process was designed to automate data integration of the SIEM raw data, Excel spreadsheets, flat files, APIs and web scraping for both data and images into the centralized DWH. To reduce the load on the SIEM ERP, data was integrated every day in the DWH and was pulled from it whenever reports were needed.

Next, a mechanism was designed for analyzing the data using ML algorithms to find the security anomalies. Automating and scheduling data extraction and routine tasks ensured improved efficiency for the team and accuracy of the process. Bringing data to a common platform created an infinite opportunity for the MSSP to analyze this data in multiple ways.

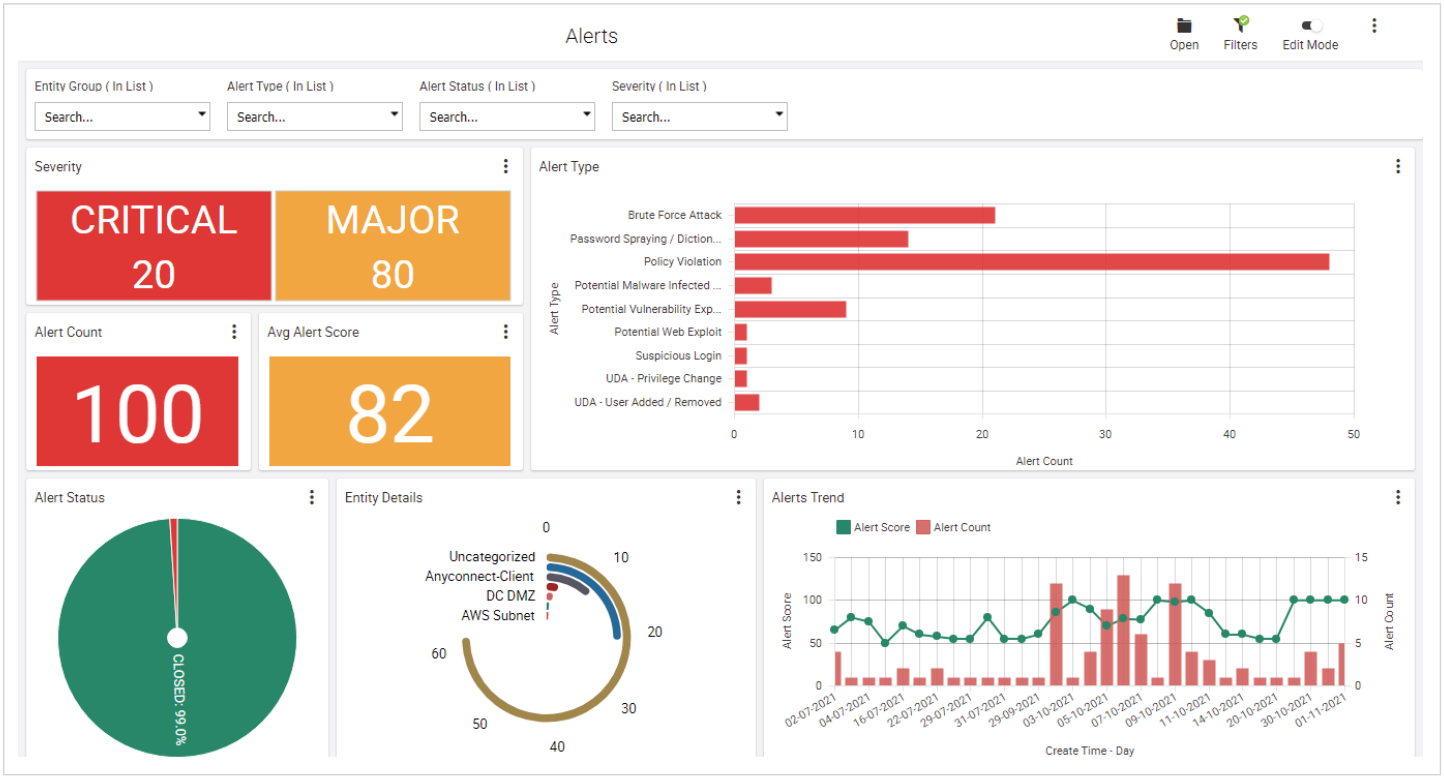
Lastly, the manual distribution process was automated through the event-based multiset feature of Intellicus. This allowed the scheduling to move from a purely time-based method to automatically running reports for multiple clients concurrently. The engineers scheduled the generation of the first weekly report after the data had matured, but the process was optimized by triggering subsequent reports soon after the completion of the previous report. Pulling data from the DWH, generating reports as HTML as well as PPTs, attaching to an outgoing email, disseminating to the right distribution list and alerting the right team members about any failures—the complete process was now automated.

The SIEM team, now free from heavy burden of manual routine operations, could shift focus to risk assessment and analysis to create value.

MOVING FROM REPORTS TO INSIGHTS

With the automation of reports, the SIEM team could focus on strategic analysis that led to better insights. The reduced operational burden meant that the team could devote time and human resources to performing the task that people do best—engage customers and deliver value.

Before adopting Intellicus, when the MSSP or their customers needed to tailor a dashboard, they would have to raise a request and wait for several weeks before the new dashboard could be deployed by their service providers. Intellicus BI and analytics platform includes dashboards with customizable widgets which gives business users the power of self-serve, custom-designed analytics instead of one-size-fit-all reports. Business users of the MSSP can now not only tailor dashboards and generate ad-hoc reports for their unique needs in a few clicks, they can share the gained insights with their end users instantaneously. The universal semantic layer (USL) built over the SIEM data lets business users add or alter data sources through a no-code user interface. The USL also lets them cut and dice data according to their requirements, with no dependence on an IT team.



Further, correlation of data allowed the SIEM team to create dashboards with multi-dimensional analysis. When creating incident summaries, they had the ability to not only split each report by severity, but also choose to reflect other details, such as the status of each open, closed or remediated incident. Existing visualizations were also refined to add not just more information but to also enhance their intuitiveness. For instance, geographic visualizations were enhanced with the optimizations of scale or the addition of gradients color-codes. Within the visualizations, the SIEM team could also take control of the granularity of the data, choosing to depict as much or as little detail as was pertinent for the stakeholders. For instance, when reporting the volume of data between points in their network, the team could reduce the number of nodes on a chard diagram to only the critical nodes.

CREATING RICH, REPLICABLE EXPERIENCES

The teams could now also prioritize enriching the customer experience. Rich report templates were created using advanced visualizations. The templates supported formatting and dynamic white-labeling for each customer. In addition, Intellicus' pixel-perfect Studio reports gave the SIEM team reports that were generated to exact specifications, often meant for printing rather than manipulating data. Further, each template was parameterized to make it reusable for multiple customers. The templates were flexible enough to be rendered across any date range, adapting to fit the full spectrum from daily reports to annual summaries.

> *Standardized templates ensured a consistently rich, tailor-made experience and deep insights that enabled data-driven decisions for every business user.*

ACHIEVING TRUE SCALE

The SIEM team at the MSSP is witnessing incredible progress in scaling up their ability to meet the requirements of the expanding enterprise. Freed from the bottleneck of manually processing each report, the team is now ready to expand from serving 30 to 300 or even 3,000 customers. In fact, the organization as well as one of their service providers are exploring other aspects of Intellicus to drive improvements for multiple engagements. With Intellicus, every organization in the value chain experiences smarter ways of working.

Intellicus enables SMEs as well as large enterprises to take the next step in their digital transformation journeys.

To understand how we can assist in yours, visit https://intellicus.com/contact-us/

intellicus