Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. We help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 15,000 people worldwide.

DIGITAL Trust. Mastering business security

Computacenter

Computacenter (UK) Ltd
Hatfield Avenue, Hatfield, Hertfordshire AL10 9TW, United Kingdom

computacenter.com
+44 (0)1707 631000

MAXIMIZE SECURITY VISIBILITY WITH MINIMUM EFFORT

SIEM Excellence Center enhances the value of Splunk deployments

Security Monitoring and Analytics is an essential capability deployed by most organisations to help protect against cyber-attacks. Many deploy SIEM (Security Incident & Event Management) tooling as a key component of this monitoring and analytics capability. However, SIEM tooling such as that based on Splunk's data analytics platform, will only provide the valuable insights required by a company's security function if it is designed, implemented and configured in the most effective way.

Splunk in particular is an analytical tool that is so flexible and adaptable, that it can offer almost limitless analytical insight. Therefore, making sure that it gives the insight needed requires significant design and continuous configuration effort – something that requires comprehensive expertise and knowledge in both security and Splunk. There is a current market skills shortage in both these areas which is a major contribution to ineffective deployments.

OUR EXPERTISE, HELPING TO MAKE YOUR ORGANISATION SECURE

This is exactly where the SIEM Excellence Center can help. With years of experience setting up, configuring and operating Cyber Defence Centers, we know exactly what an efficient SIEM looks like. We have collected all of the experience and specialist knowledge we have in this area and combined it with our knowledge of Splunk to create a comprehensive and effective remote consultancy offering.

This covers all aspects of SIEM from use case development, dashboarding & reporting, analytics, machine learning, automation, testing, roll-out, orchestration, quality assurance, standardisation and best practice to design for SIEM tools like Splunk.

As a result, we can help with the selection of appropriate technologies as well as the design, implementation and configuration of your analytic platform, be it Splunk or an alternative vendor. Giving you a SIEM solution to meet the highest level of expectations, all without needing to build in house technical expertise.

OUR SIEM SERVICES

- SIEM STRATEGY AND CONSULTANCY

If you do not yet have a SIEM solution in place, or you are planning a change to your current SIEM platform, we can help you to develop a SIEM strategy and advise you on the selection of the best technology outcome for your business. Once your strategy is clear we can help you to develop a SIEM concept and roadmap your deployment, showing you how to best implement it.

- INFRASTRUCTURE AUTOMATION

Should you select Splunk as your analytical tool of choice then we can automate the deployment rollout, regardless of whether it's a large scale global deployment or a smaller local implementation. Our extensive experience will ensure that any deployment is not only more cost effective but will also provide support for updates and upgrades, SIEM migration and automation activities. By automating much of the deployment approach, we can help to reduce cost and timescales and create more predictability in the outcome.

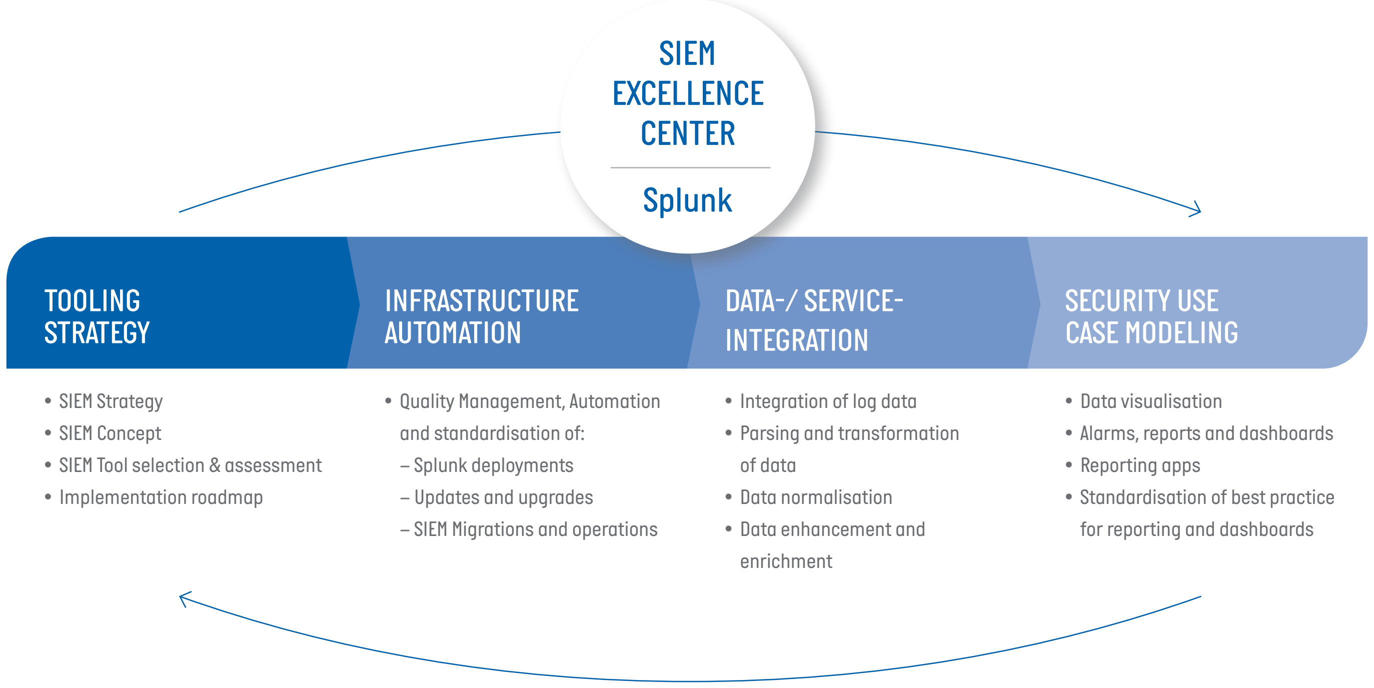
- DATA-/SERVICE-INTEGRATION

This is a key service when working with Splunk data because it ensures that the data of different log sources are available as normalised information. This is achieved by parsing or transformation to meaningful data. Typically the data must also be enriched with information from the CMDB, data from vulnerability management, and from other systems to achieve meaningful results. This is a complex and extensive undertaking that requires real expertise, however the outcome is essential for successful SIEM deployments. Our experience, our toolbox of parsers and proven methodology will quickly help you achieve the results you need.

- SECURITY USE CASE MODELING

To ensure that collected data is utilised in the most effective way it is essential that the right analytical assessments and visualizations are undertaken. With our Security Use Case modelling service we will ensure that the correlation rules for security information are modelled, implemented and tested using SPL, Machine learning and AI. We also design dashboards, alarms, reports, and other ways to visualise the data for the benefit of key business stakeholders. This includes the development of bespoke Splunk apps if required.

No matter how complex the requirement is, or how challenging the expectations are, we have the experience and defined processes to be successful. Whether it is deploying SIEM rules from our library of standards, developing bespoke SIEM rules for machine learning use cases (e.g. active hunting, fraud detection or UEBA), or undertaking cross analytics with data from VM systems, CMDB's and ticket systems, we can help.


SIEM
EXCELLENCE
CENTER
Splunk
TOOLING STRATEGY
INFRASTRUCTURE AUTOMATION
DATA-/ SERVICE-INTEGRATION
SECURITY USE CASE MODELING

TOOLING STRATEGY

- SIEM Strategy
- SIEM Concept
- SIEM Tool selection & assessment
- Implementation roadmap

INFRASTRUCTURE AUTOMATION

- Quality Management, Automation and standardisation of:
  - – Splunk deployments
  - – Updates and upgrades
  - – SIEM Migrations and operations

DATA-/ SERVICE-INTEGRATION

- Integration of log data
- Parsing and transformation of data
- Data normalisation
- Data enhancement and enrichment

SECURITY USE CASE MODELING

- Data visualisation
- Alarms, reports and dashboards
- Reporting apps
- Standardisation of best practice for reporting and dashboards

RELIABLE INFORMATION AT A GLANCE

Our SIEM Center of Excellence can ensure that your business is never again under informed about the current state of your security. With extensive use of automation, consequent standardization, implementing best practice process, knowledge sharing, automated testing and quality management we can ensure that your Security operations team is equipped with the best analytics platform. Our services ensure that analytics are operated in a more efficient manner and to a higher quality standard resulting in better data, better assessment and better visualisation. With individual reports and dashboards, each relevant to specific target stakeholder groups, you will never have to worry about a lack of relevant and reliable information about your security state, allowing you to make business decisions with confidence.

OUR SPLUNK KNOW-HOW

Benefit from our extensive Splunk expertise and knowledge and our many years of experience in analytics and SIEM projects. With Splunk alone, we have implemented more than 100 projects, we are Splunk Elite Partners and have over 60 employees with Splunk certificates and accreditations.

In our Global Solution Center in Munich we operate a dedicated splunk development and test laboratory, where development from source to application (from data connection to analytics based on Mitre ATT&CK) is part of our daily business. Our security team continually analyses security incidents and attacks and design, develop and integrate appropriate security rules for Splunk, adding them to our library of standards.