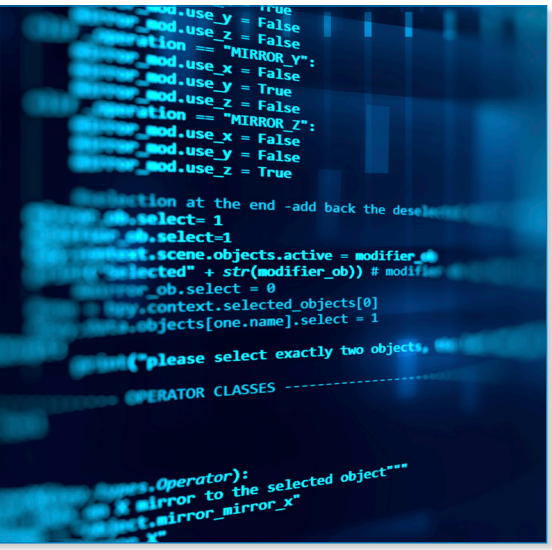
SAS® Cybersecurity

Understand your security posture. Identify current weaknesses. Prioritize remediation. See risk prior to compromise.



Challenges

- **Business initiatives complicate**. Organizational and security changes are constants. Understanding organizational, asset and network security posture is crucial to managing risks and evolving remediation efforts.
- **Security data is messy**. Disconnected, poor quality data in multiple formats requires ongoing data management capabilities for a clear, continuous and comprehensive view.
- **Analytics capabilities are fragmented**. As existing security products inject analytics to boost effectiveness, it's harder to extract consistent, governed insights across technologies.
- **Compliance requirements and fines are growing**. Regulators and cyber insurers are demanding organizations demonstrate more control over data, users and systems. Continuous visibility is required to protect your assets today and tomorrow.
- **The security skills shortage is here to stay**. As the complexity and labor needed for security tools grows, talent is not. Data scientists who can make sense of the results are expensive and hard to come by.

Your security posture evolves with every new business initiative. Data protection regulations are increasing. Your security personnel are perpetual recruiting targets. Worse, they're continually overwhelmed by security events from the products protecting your organization.

You've invested a lot of time and money in point products to solve specific security and compliance challenges. Yet these technologies haven't delivered the value you expected. Each tool has its own data format and analytics capability – multiplying data silos that fragment views of your security risk. Even SIEM and data lake initiatives haven't fulfilled their force multiplier potential.

Security by checklist no longer works. It's time for a new approach.

Security analytics from SAS brings cyber ISR – intelligence, surveillance and reconnaissance – to your network for a complete, continuous and accurate monitoring of your organization's security posture. With this ongoing risk assessment, you can close cyber hygiene gaps, improve security tool effectiveness and better prepare for future threats.

The SAS® Approach

SAS Cybersecurity provides a solid, unifying analytics foundation, enterprise threat detection and risk assessment capabilities. Powered by the SAS Platform, a software foundation engineered specifically to generate insights from any data in any computing environment, our security analytics software addresses the entire analytics life cycle – from data through discovery to deployment.

The result? Effective and trustworthy insights based on current and potential threat scenarios. Allocate your resources more effectively with consistent, managed and governed processes for your security data, investigations and analytics capabilities.

Benefits

- **Reduce MTTD and MTTR**. Get immediate visibility of potential threats within your network and how they've manifested themselves in your organization to better protect your data and infrastructure and reduce remediation costs.
- **Improve security operations productivity**. Scale your ability to cover new areas with existing staff. Make advanced analytics approachable throughout your operations. Eliminate manually intensive processes by allowing your data to trigger detection.
- **Streamline security operations focus**. Eliminate the time spent on false positives and easily prioritize events to focus on the most critical risks. Drive fast action through heightened understanding of security risks. Proactively integrate siloed data from existing investments to improve security ROI.
- **Better understand network operations**. Gain complete visibility into network behavior. Highlight which devices should be reviewed more aggressively. Promote and reward network hygiene now before your network becomes even more complex.
- **Advance security automation efforts**. Exploit the power of analytics to prioritize and automate incident response activities. Develop and retain in-house talent by shifting your staff from routine to important work.

Capabilities

Intelligence

Comprehensive security risk views

SAS Cybersecurity delivers rapid insights into your entire organization's security posture. Make resource prioritization easy with risk-driven intelligence for your network's most critical individual areas. Analysis of structured and semistructured data across multiple dimensions – network, security product and business data, threat feeds and IP reputation information – validates data for an accurate view of your security posture and potential issues. Unstructured text can also yield otherwise-hidden security insights through contextual analysis using machine learning and subject-matter expertise.

Intuitive, role-based workflows support incident triage, investigation and remediation efforts that mitigate risks. Use custom dashboards for threat hunting, deeper investigations or reporting.

Surveillance

Real-time data enrichment

Deployed without an agent, SAS Cybersecurity continuously captures network traffic flow at the source, enriches it with user/identity, endpoint, threat and other network data, then correlates the enriched data before performing analytics. This added context creates an ongoing stream of smarter data that drives a deeper view of risk across your organization. You're already looking at data from individual tools – why not get more collective value across all data?

Self-reinforcing detection

If a record of known compromises exists, you can quickly test and implement predictive analytics models. Otherwise, apply semisupervised machine learning to develop an initial detection model focused on specific statistical anomalies. The model gets refined and improved as investigations confirm or reject it.

Detection model management

SAS provides an environment for creating, managing, validating and monitoring detection models. Test advanced analytics and machine learning algorithms to determine champion models. Performance monitoring and alerting automate the model updating process to address model degradation and ensure that models reflect current conditions.

Rich device-risk profiles

Using unsupervised machine learning, SAS Cybersecurity automatically assigns a risk score to each network device across multiple behavioral attributes with comparisons to peer-group behavior and historical baselines. This analysis of device relationships minimizes false positives and false negatives. Track device risk scores over time to create a rich profile to validate results.

Reconnaissance

Security data management

With our data management capabilities, you can reduce the time required to manage security data and maximize data value. Going beyond simple extract, transform and load (ETL) capabilities, easy-to-deploy workflows target and improve security data quality and reliability. Regardless of where your security data is stored or how it's received – in batch or streaming – it's ready for analytics. And SAS maintains your data lineage for regulatory and organizational compliance.

Device inventory

To understand your organization's security posture, you first need to understand your environment. SAS Cybersecurity has device inventory capabilities (included and also available separately) that monitor your network for you. You get a clear picture of all connected devices, those currently online, those with incomplete system profiles and those never before seen. With this information, you can identify the impact of business initiatives such as IoT, containers and XaaS usage. You can also validate critical, high-value assets to ensure effective resource allocation.

The SAS® Difference

SAS addresses the issues of security data and technology diversity, resource scalability and trust in analytics that usually prevent organizations from gaining an integrated picture of their security posture. With SAS, you can answer critical security questions like:

- How many unknown systems are connecting to my network, and where are they?
- Is this single endpoint compromised, or is there a broader infection in the network?
- Is data being exfiltrated from my network?
- How can we better tune existing point solutions?
- Are there high-value business systems we should monitor more frequently?

Whether your organization is exploring data or expanding established security analytics efforts, SAS can help you ask the right questions, find the right answers, and take the next step toward getting the most value from your analytics.

For more information, vist sas.com/cybersecurity.

To contact your local SAS office, please visit: sas.com/offices