



Business Impact

“Threats in cyberspace move at the speed of light, and we are literally under attack every day as our networks are constantly probed and our adversaries seek to exploit vulnerabilities.”

– Lt. Gen. William Shelton
Chief Information Officer
US Air Force

Challenges

- **Sophistication of criminal tactics.** Attempts by foreigners to steal information are advanced, persistent, constantly changing and well-resourced.
- **“Low and slow” attacks.** Attacks that cause the most damage penetrate “under the radar” and span longer time periods, leaving little to no pattern or signature, which makes them extremely hard for current network security devices to detect.
- **Siloed data.** Different agencies implement numerous technologies to combat cyber network attack, defense and exploitation activities, and the data generated by these systems is scattered among disconnected silos in inconsistent storage formats, making data consolidation and integration a challenge.
- **Disjointed network views.** Disconnected systems make it practically impossible to gain a holistic view of networks and associated devices, which in turn makes network domain awareness and complete situational awareness elusive.

How can we prevent government networks from falling victim to cyber attacks?

YOUR GOAL: Evolve systems and processes to overcome growing cyber threats

The rapid growth of Internet technology has enabled friend and foe alike to occupy a common virtual space. As a result, the velocity, veracity and volume of cyber attacks and exploitations have increased exponentially. The Department of Defense detected 300 million network penetration attempts last year, up from 6 million in 2000. The Pentagon recently disclosed that it had spent \$100 million in the past six months to repair damage from cyber attacks. And the US Government Accountability Office found that in 2008, 23 of the 24 major agencies surveyed did not have adequate computer security protections in place.

Computer networks are constantly bombarded with probes, worms, viruses, bots, malware and host-system root access attempts that originate both inside network boundaries and outside the network from sources around the world. Most organizations attempt to counter such threats with point products like firewalls, routers and intrusion detection sensors. Others employ event correlation engines to manage point-product collection information and provide a single view of potential network intrusions at one point of control. Even so, our nation’s cyber defenses are being challenged like never before by sophisticated, well-organized intrusion efforts aimed at disrupting critical systems and stealing classified information.

OUR APPROACH

With information systems now considered weapon systems, the cyber domain has become one of our most important national security challenges – and it must be treated accordingly. In recognition of this, Congress has established directives to allow for full-spectrum engagement across law enforcement, intelligence, diplomatic and homeland security mission areas. But while we can identify more vulnerabilities and intruders than in the past, the number of cyber terrorists lurking in the shadows continues to increase. SAS approaches the problem by delivering software and services to help you:

- **Become wiser than the attacker by exposing activities indicative of hard-to-detect, low and slow attacks** by uncovering hidden relationships and detecting subtle patterns of behavior that may otherwise go unnoticed.
- **Provide information-rich data sets that facilitate multiple analyses of the nature, occurrence and impact of network attacks** by aggregating and consolidating the volumes of data from network monitoring devices, policy compliance and event logs, asset tracking or virtually any other source – regardless of system or format.
- **Go beyond forensic actions** by using sophisticated data mining, text mining and forecasting technologies to proactively predict the possibility of future attacks far enough in advance to take preemptive actions.

SAS offers proven solutions for creating the “smart storage” necessary for cyber analysis, statistical algorithms for combating cyber intrusions and situational awareness to enhance warfighter preparedness. And you can use these same cyber-related solutions to combat sophisticated attackers who go undetected and cause the most damage.



THE SAS® DIFFERENCE: In-depth analytics that turn possibilities into reality

SAS provides a framework that can integrate with your existing infrastructure to aggregate, manipulate, fuse, visualize, process and analyze enormous amounts of network traffic data into problem-specific, applicable information to provide complete situational awareness of your entire network. With SAS, you get:

- **Scalability.** SAS can store and process continually growing volumes of captured cyber data – which can mean up to several gigabytes of data each day.
- **Speed.** Multithreading, optimized routines and smart storage for extremely fast retrieval enable SAS to process even the largest volumes of data that sensors create each day.
- **Flexibility.** SAS provides a flexible cyber network solution framework that will allow you to expand, grow, modify or adapt as the cyber environment changes.
- **Data refresh capability.** SAS refreshes data to underlying systems and analyses in 15-minute increments to ensure that your data is always up-to-date.

No other solution available provides the same level of detection, automation and power that you get with SAS.

CASE STUDY: Navy Cyber Defense Operations Command (NCDOC)

Situation

With a staff of about 200, the NCDOC coordinates and monitors the defense of the Navy's vast global networks. An overwhelming amount of data crosses the network each day, and every alert must be investigated. Since about 90 percent of the alerts are of a probing nature that do not require immediate action, a lot of valuable time is wasted on unnecessary investigations. In addition, the Navy's many network monitors produce huge volumes of data in different formats, and the NCDOC needed a way to aggregate and store the data necessary for performing historical analysis, trending, data visualization or in-depth analyses.

Solution

Implemented within a real-time network computer defense solution that used event correlation data and several other data sources, the SAS solution provided:

- Robust support for a single point of control for handling hostile activity.
- Smart and fast technologies, including 15-minute-increment updates to the integration and storage of large volumes of computer network defense data.
- Customized information-delivery and event investigation interfaces for Navy personnel in the best format for their job requirements and functions.
- R&D related to multimodal layered analysis of network architectures for threat detection of low and slow activity.

Result

- Potential threats are recognized sooner than ever before.
- Analysts can investigate incidents on a network view of the data with greater speed.
- Prioritization capabilities ensure that NCDOC staff spend time on the right things.

The Vision

Monitor

What if you had a real-time network defense system that automatically generated attack alerts when threat response actions were required, while also dramatically reducing the number of false positives?

Uncover

What if you could pinpoint anomalous properties of network traffic, which would normally go undetected, as well as uncover hidden relationships and behavior patterns that might be indicative of damaging low and slow attacks?

Integrate

What if you could aggregate, correlate and merge data from all your network monitoring devices and any other data sources so you could achieve complete network domain awareness?

Predict

What if you had a way to detect and score the severity of a possible attack well before it happened, so you could provide intervention measures?

SAS FACTS

- SAS has more than 30 years' experience working with government agencies, including all 15 federal departments, all military departments and the joint commands.
- Approximately 85 percent of independent US government agencies and commissions use SAS.
- SAS solutions are used at more than 45,000 sites in over 100 countries – including 91 of the top 100 FORTUNE Global 500® companies.

Learn more about SAS software and services for government at:
www.sas.com/govedu/



SAS Institute Inc. World Headquarters +1 919 677 8000

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

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. © indicates USA registration. Other brand and product names are trademarks of their respective companies. Copyright © 2009, SAS Institute Inc. All rights reserved. 104061_546026.0809