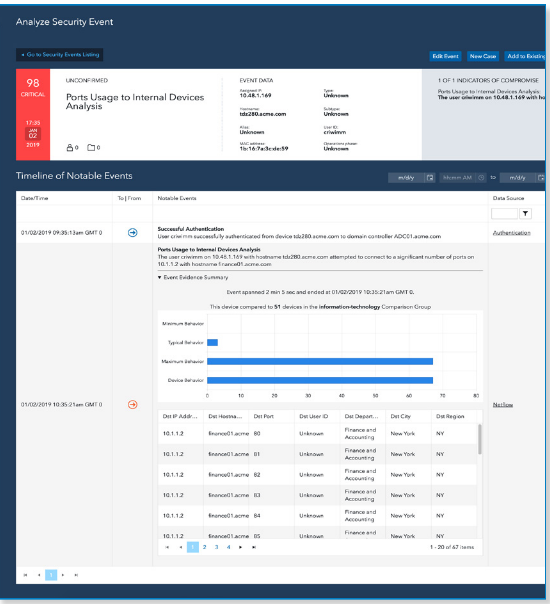
SAS® Cybersecurity

Understand your security posture, identify vulnerabilities, prioritize remediation, see risk before compromise



Analyze Security Event

98 CRITICAL

17:35 JAN 02 2019

UNCONFIRMED

Ports Usage to Internal Devices Analysis

EVENT DATA

Assigned IP: 10.48.1.169

Type: Unknown

Hostname: tdz280.acme.com

Subtype: Unknown

Alias: Unknown

User ID: criwimm

MAC address: 1b:16:7a:3c:de:59

Operations phase: Unknown

1 OF 1 INDICATORS OF COMPROMISE

Ports Usage to Internal Devices Analysis: **The user criwimm on 10.48.1.169 with ho**

Timeline of Notable Events

Date/Time	To | From	Notable Events	Data Source
01/02/2019 09:35:13am GMT 0	➜	**Successful Authentication** User criwimm successfully authenticated from device tdz280.acme.com to domain controller ADC01.acme.com	Authentication
01/02/2019 10:35:21am GMT 0	➜	**Ports Usage to Internal Devices Analysis** The user criwimm on 10.48.1.169 with hostname tdz280.acme.com attempted to connect to a significant number of ports on 10.1.1.2 with hostname finance01.acme.com	Netflow

▾ Event Evidence Summary

Event spanned 2 min 5 sec and ended at 01/02/2019 10:35:21am GMT 0.

This device compared to **51** devices in the **information-technology** Comparison Group

Dst IP Addr...	Dst Hostna...	Dst Port	Dst User ID	Dst Depart...	Dst City	Dst Region
10.1.1.2	finance01.acme	80	Unknown	Finance and Accounting	New York	NY
10.1.1.2	finance01.acme	81	Unknown	Finance and Accounting	New York	NY
10.1.1.2	finance01.acme	82	Unknown	Finance and Accounting	New York	NY
10.1.1.2	finance01.acme	83	Unknown	Finance and Accounting	New York	NY
10.1.1.2	finance01.acme	84	Unknown	Finance and Accounting	New York	NY
10.1.1.2	finance01.acme	85	Unknown	Finance and	New York	NY

1 - 20 of 67 items

What is SAS® Cybersecurity?

SAS Cybersecurity provides a solid, unifying foundation for enterprise risk assessment, threat detection and alert management. Powered by SAS® Viya®, our security analytics software addresses the end-to-end analytics life cycle, from data through discovery to deployment.

Why is SAS® Cybersecurity important?

The traditional patchwork of point products creates data silos and a fragmented view of risk. Even SIEM and data lake initiatives have fallen short of the promise. It's time to fortify your cybersecurity defense with advances such as high-performance computing, applied machine learning and artificial intelligence.

For whom is SAS® Cybersecurity designed?

Security investigators and analysts use it for earlier detection, analytics-driven risk indicators, custom event detection models, and smart alert prioritization and management. Security executives use it to gain valuable insight into overall security posture, staff effectiveness and performance.

The greater our dependence on data networks, the greater the opportunity for criminals or unwitting intermediaries to disrupt essential functions of government and society. Today's cyber threats come in countless forms – ransomware, DDoS attacks, Trojans, malware variants, insider attacks and more. As soon as one threat is quelled, new ones emerge somewhere else.

How do you keep pace with fast-changing risks? In many cases, short-staffed cybersecurity teams have to overlook a significant number of alerts because they can't manage the volume. Lacking good context around alerts, it's hard to know where to spend valuable investigative effort.

All too often, more time is spent managing security data than analyzing it. And with analytics scattered across point security products, it's a challenge to extract insights in a consistent, accurate and well-governed way. False positives are endemic. Emerging threats are missed or discovered too late.

A volatile risk environment calls for a more effective and proactive line of attack – a risk-based approach instead of just closing gaps after incidents have occurred. SAS Cybersecurity security analytics software delivers essential visibility and broad context, continuously informed by analytics insights from all your data sources.

Key Benefits

Elevate your security outcomes: More routine days, fewer fires

- Reduce the time to detect and respond to security incidents.
- Gain visibility into overall organizational risk and specific devices at risk.
- Reduce false positives without limiting results to "Top X" events.

Elevate your security resources: Better use of time, lower staffing costs

- Provide analytics-driven guidance for security investigations.
- Augment human expertise through machine learning and AI.
- Reduce the time and effort required to prepare and manage data.
- Bridge the gap between cybersecurity and data science with easily interpreted analytics.

Elevate your data/analytics environment: Less complexity, more value from existing investments

- Consolidate data and analytics capabilities, including open source initiatives, into a single hub.
- Implement smart data quality workflows for more accurate results.
- Gain new event context from existing network, endpoint, authentication and threat data.
- Achieve a complete view of individual network pain points and overall organizational security.

Overview

SAS Cybersecurity is flexible security analytics software that delivers greater network visibility and better security outcomes through a unique combination of data, analytics and collaboration. SAS Cybersecurity:

- Inventories all your network devices, so you always know what's connected and what's happening.

- Captures all your network flow data in real time and enriches it with other data for broad context.
- Intelligently prioritizes alerts so it's clear where to focus for the best outcomes.
- Uses analytics-informed workflows to target and improve the quality of security data.

SAS Cybersecurity can be deployed on-site (distributed across servers to grow as needed), in a private cloud hosted by your organization or an external service provider (such as SAS), in a public cloud infrastructure – or a hybrid of deployment approaches.

Capabilities

Network device analytics powered by machine learning and AI

SAS Cybersecurity continuously analyzes network activity, using the high-performance, in-memory analytic engine of SAS Viya technology. More than 70 device analytics capabilities are available out of the box and can be customized and extended to answer your most pressing security questions.

What is normal activity for a device compared to its peer group or to the organization as a whole, now and over time? Is a device's behavior unusual compared to past behavior? Atypical patterns may indicate a recent compromise or involvement in malicious behavior, such as a DDoS attack.

Is a rare or unlikely activity taking place on a host, port or other value for a device? That might indicate botnet command and control activity, data exfiltration or high-risk user behavior. Is an overall pattern of behavior unusual when examined by unsupervised machine learning? Are any of these behaviors associated with discrete security events, such as multiple failed authentication attempts?

With SAS Cybersecurity, you get real-time insights generated by statistical time series models, deep learning neural networks, anomaly detection analytics and more – sophisticated quantitative science to spot cyber threats.

Multidimensional detection and composite device risk scoring

Out of the box, SAS Cybersecurity builds context around security events by bringing together NetFlow, web proxy, DNS, DHCP, endpoint and authentication data across multiple measures. Customize with adapters to bring in additional data sources. SAS Cybersecurity correlates results with internal and external threat intelligence.

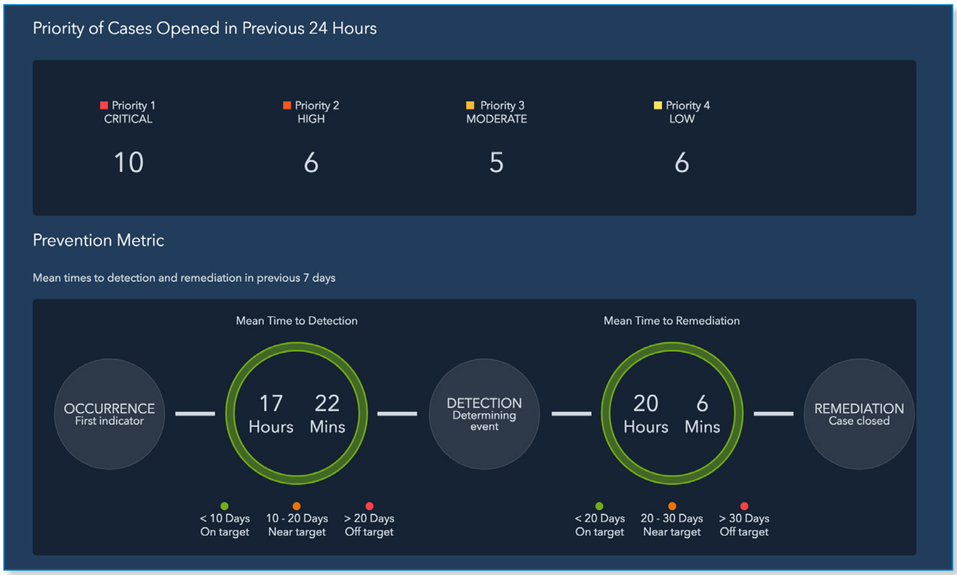
Guidance and context for investigators

Once a potential security threat is identified, SAS Cybersecurity empowers investigators to get results with less time and effort. For example, security investigators can:

- Quickly locate security events by date or assumed risk.
- Review analytical, graphical and unprocessed (raw) event data.
- Create cases to manage and track event remediation.
- Search cases for historical reference.

Prebuilt, intuitive performance dashboards and reports

Security managers can monitor the efficiency and performance of the security team and the system with easy-to-understand KPI and audit reports. Track critical metrics such



Priority of Cases Opened in Previous 24 Hours

Priority 1 CRITICAL	Priority 2 HIGH	Priority 3 MODERATE	Priority 4 LOW
10	6	5	6

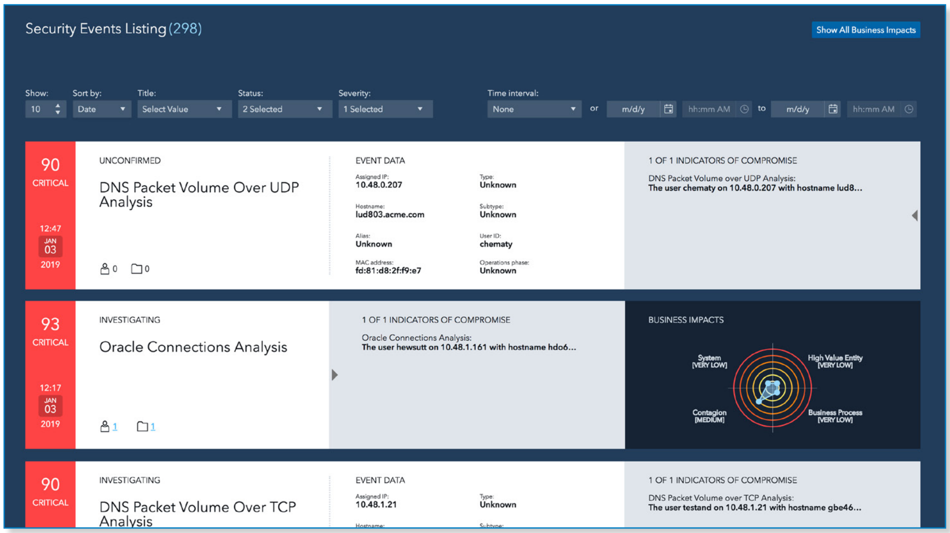
Prevention Metric

Mean times to detection and remediation in previous 7 days

Mean Time to Detection: 17 Hours 22 Mins

Mean Time to Remediation: 20 Hours 6 Mins

Figure 1: Use SAS Cybersecurity performance reports to measure the actual time to action of your security team against preferred or goal time to action.



Security Events Listing (298)

Show All Business Impacts

Show: 10 Sort by: Date Title: Select Value Status: 2 Selected Severity: 1 Selected Time interval: None or m/d/y hh:mm AM to m/d/y hh:mm AM

90 CRITICAL 12:47 JAN 03 2019

UNCONFIRMED

DNS Packet Volume Over UDP Analysis

0 0

EVENT DATA

Assigned IP: 10.48.0.207
Type: Unknown
Hostname: lud803.acme.com
Subtype: Unknown
Alias: Unknown
User ID: chematy
MAC address: fd:81:d8:2f:f9:e7
Operations phase: Unknown

1 OF 1 INDICATORS OF COMPROMISE

DNS Packet Volume over UDP Analysis:
The user chematy on 10.48.0.207 with hostname lud8...

93 CRITICAL 12:17 JAN 03 2019

INVESTIGATING

Oracle Connections Analysis

1 1

1 OF 1 INDICATORS OF COMPROMISE

Oracle Connections Analysis:
The user hewsutt on 10.48.1.161 with hostname hdo6...

BUSINESS IMPACTS

90 CRITICAL

INVESTIGATING

DNS Packet Volume Over TCP Analysis

EVENT DATA

Assigned IP: 10.48.1.21
Type: Unknown
Hostname:
Subtype:

1 OF 1 INDICATORS OF COMPROMISE

DNS Packet Volume over TCP Analysis:
The user testand on 10.48.1.21 with hostname gbe46...

Figure 2: View a full list of security events or filter by specific criteria to pinpoint the most critical risks in your network.

as event detection to case creation or remediation, summaries of security events, volume and disposition of open and closed cases, case priorities and threats thwarted. Audit system activity related to entities and access.

With an included (or standalone) module, you get an up-to-the-minute network device inventory:

- See list of all connected devices within the network.
- Identify devices currently online on your network.
- Pinpoint devices with incomplete profiles in SAS Cybersecurity.
- Find devices never before seen on your network.

High-performance, applied machine learning and artificial intelligence through SAS® Viya®

As a SAS Viya product, SAS Cybersecurity benefits from enhanced artificial intelligence (AI) capabilities. For example, built-in intelligence supports smart automation of data and analytics processes. Embedded machine learning makes predictions more explainable, transparent and accountable. Distributed, in-memory processing delivers answers fast.

Self-healing mechanisms ensure always-on protection, whether SAS Cybersecurity is deployed on-site, in the cloud or in hybrid cloud configurations. For maximum flexibility in a hosted deployment, SAS Cybersecurity can securely support separate organizations (tenants) on a shared software stack.

Self-service data management

Advanced data management capabilities are available in an interactive, self-service manner. Security analysts and cyber data scientists can consolidate data from internal and external sources for analysis and investigation. Built-in, automated data quality tools resolve data inconsistencies and redundancies. The result? Less time spent accessing, cleansing and preparing the data for analysis, and more time turning data into insight.

Key Features

Network device analytics powered by machine learning and AI

- More than 70 device behavior analytics calculated continuously to analyze network activity.
- Out of the box, extensible analytics based on NetFlow, authentication, web proxy, DNS, DHCP and endpoint data.
- Open, Jupyter Notebook and Python-based analytics processing architecture for custom model development.
- Analytics processing using the SAS Viya in-memory analytic engine.
- Full suite of comparison analytics to compare device values to peer devices or all devices in the organization.
- Deep learning neural networks to identify domain generation algorithm (DGA) activity and specific variants.
- Statistical time series models to analyze device behavior over time and spot possible compromise or malicious activity.
- Device interactions – ports, hosts and other variables – analyzed for rarity with respect to peer groups or overall.
- Anomaly detection analytics using deep learning neural networks, principal components analysis, and SAS Cybersecurity-specific algorithms.
- Capture of discrete events, such as unsuccessful authentication attempts, to mark key activity.

Integration with McAfee Data Exchange Layer (DXL)

- Incorporates McAfee DXL data into the device risk scoring process.
- Makes the results and underlying enriched data available to McAfee ePolicy Orchestrator, McAfee Enterprise Security Manager, McAfee Active Response and third-party DXL-compatible solutions for further analysis.

Investigation/guidance

- Rapid location of security events by date or perceived risk.
- Ability to review analytical, graphical and unprocessed (raw) event data.
- Case creation to manage and track event remediation.
- Searchable case records for historical reference.
- Security events shown in full context with diverse network data.

Prebuilt, intuitive performance dashboards

- KPI reporting such as event detection to case creation or remediation, event summary, open and closed cases, case priority and prevention.
- Audit reports of system activity relative to entities or network access.

Illuminating device inventory

- Up-to-the-minute list of all connected devices in the network and those that are currently online.
- Quick identification of devices with incomplete SAS Cybersecurity profiles.
- Identification of previously unknown devices on the network.

High-performance, applied machine learning and artificial intelligence through SAS® Viya®

- AI capabilities such as smart analytics automation and embedded machine learning.
- Distributed, in-memory processing for low latency in delivering results.
- Self-healing mechanisms to sustain premium 24/7 uptime in cloud, on-site and hybrid deployments.
- Support for multi-tenancy, shared software stack to securely support isolated tenants.

Self-service data visualization

Business and technical users can discover relationships, trends and outliers via box plots, heat maps, network diagrams, geographical map views, decision trees and more. Add data visualizations and web content to reports. Distribute reports as PDFs or secure emails, on your schedule.

Custom detection model development with modern machine learning algorithms

Security analysts can tap into a broad set of modern statistical, machine learning, deep learning and text analytics algorithms in a single environment. Improve models by testing different approaches in a single run. Compare results of multiple supervised learning algorithms with standardized tests to reduce false positives. Automatically find and understand sentiment from text sources, such as social media and Google Analytics. Combine or layer analytic techniques to answer new questions or old questions with new accuracy.

Rule and analytic model management

On SAS Viya, you can continuously refine SAS Cybersecurity models. Logically manage rules, models and alerts for security investigators. Automatically track how and when models were developed and published, to maintain tight governance even as you deploy more and more models.

TO LEARN MORE »

Whether your organization is exploring new approaches or expanding established security analytics efforts, SAS can help you take the next step.

For more information, visit sas.com/cybersecurity.

Key Features (continued)

Data management

- Consolidation of historical data from internal and external sources for analysis and investigation.
- Automated, built-in data quality tools to reduce or eliminate data issues.
- Seamless integration with third-party applications.
- Interactive, self-service data access, blending, shaping, cleansing and report preparation.
- Interfaces designed for technical and nontechnical users.

Custom detection model development with modern machine learning algorithms

- Broad set of modern statistical, machine learning, deep learning and text analytics algorithms in a single environment.
- Clustering, regressions, decision forests, gradient boosting models, support vector machines, neural networks, Bayesian networks and more.
- Ability to test multiple modeling approaches in a single run.
- Comparison of multiple supervised learning algorithms with standardized tests to reduce false positives.
- Automatic location and analysis of sentiment from text sources, such as social media and Google Analytics.

Rule and analytic model management

- Logical management of rules, models and alerts for security investigators.
- Robust model tracking and governance as more models are developed, published and deployed.

Self-service data visualization

- Self-service capability for business and technical users to visually explore data.
- Box plots, heat maps, network diagrams, geographical map views, decision trees and more.
- Ability to add content from data visualizations and the web to reports.
- Reports distributed as PDFs or secure emails – as one-time reports or at recurring, scheduled intervals.

Diverse deployment options

- On-site across distributed servers for scalability.
- On enterprise, private or public cloud infrastructure or hybrid cloud infrastructure.
- Available as a SAS managed software as a service (SaaS).
- Cloud Foundry platform as a service (PaaS) to support multiple cloud providers.

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

sas THE POWER TO KNOW.