SECURITY AT YOUR SERVICE

Civilian, military and intelligence agencies across the globe rely on ArcSight to protect sensitive data and critical infrastructure.

HP Enterprise Security Solutions Brief

> **"It is not a matter of if we will get hit by an act of cyberterrorism, but when. It's a comfort to have a company like ArcSight standing behind us. Our relationship with ArcSight is not just a financial transaction, it is a true partnership."**
>
> —Program Director for a large U.S. Government Agency

Security Challenges for Governments

Over the last decade, cybersecurity has emerged as an important concern for governments both at the national and local level. The rapid digitization of governmental records and proliferation of e-government initiatives have fueled a rise in cybercrime targeted at the public sector. Consequently, government agencies are investing in more protection for everything from nationally sensitive defense information systems and critical infrastructure to citizens' personally identifiable data.

While private businesses store specific information about consumers such as credit card numbers or medical records, across departments, governments process and store enough information to entirely reconstruct an individual's identity. At the same time, the risk to governments goes well beyond identity theft of citizens. Governments conduct research and development in numerous areas including biotechnology and military advancement. They manage and regulate transportation and utilities infrastructure. All of these functions rely heavily on information systems which, if compromised, would have a widespread impact and tremendous cost.

Protecting the assets that enable governments to serve and defend their citizens requires visibility into a wide range of employee and citizen activity, including application and portal logins, badge swipes, emails sent, and sensitive file and database access. Logs provide a minimally intrusive means of gaining visibility into such activity. However, simply capturing and making sense of this activity is a huge challenge. With millions of events generated daily, security teams need a better way to manage and make sense of log data. There is a dire need for efficient log consolidation, as well as automated, intelligent log analysis.

The ArcSight ETRM Platform

The ArcSight Enterprise Threat and Risk Management (ETRM) platform automates governmental audit requirements and enables early detection and remediation of cybersecurity threats by monitoring all user, application and system-level activity (see Figure 1). The ArcSight ETRM platform is used by governmental agencies across the globe and addresses several imperatives.

Sensitive Data Protection

- Citizens' personal information (e.g., tax, financial, health records)
- Military intelligence, and research and development

Critical Infrastructure Protection

- Networks supporting government operated services (e.g., utilities, transportation, air traffic control)
- National defense networks and systems

User Monitoring

- System admins executing direct queries against citizen record databases
- Any agency service agent accessing citizen records outside their jurisdiction

eGovernment Web Portal Monitoring

- Automated attacks such as botnets and phishing against citizen portals
- Web server vulnerability exploits
- Anomalous access patterns (e.g., international access, same account from multiple locations)

Perimeter Threat Monitoring

- External (especially out of country) access to highly sensitive military, nuclear or other critical networks

Data Capture

ArcSight SmartConnectors provide extensive out-of-the-box support for hosts, databases, security and network devices, and applications. Additionally, the ArcSight Connector framework can easily be extended to collect logs from legacy applications. ArcSight Connectors also enable secure, reliable bandwidth-controlled log collection.

Log Management

ArcSight Logger serves as an audit-quality repository with high speed search capabilities to expedite security breach investigations. Government agencies are subject to a growing number of regulations with distinct log retention requirements, and ArcSight Logger can automate their enforcement. All log data is stored in a highly compressed but easily accessible format for analysis.

Event Correlation

ArcSight ESM delivers scalable real-time analysis of logs across all systems, applications and users for continuous detection of internal and external threats. Through real-time correlation of logs from applications and all supporting infrastructure, ArcSight ESM alerts to the first sign of cybercrime. ArcSight ESM also applies pattern discovery against past user and system activity to detect previously unknown threat vectors. The product offers tracking and escalation of threats, along with inbuilt case management and workflow. Finally, as threats are detected, ArcSight ESM supports a range of automated or approval-based remediation options.

User Monitoring

Effective detection of modern threats requires the ability to track all activity back to specific users. However, legacy systems that are common in the public sector lack unique accounts as well as user context in logs. ArcSight IdentityView is a specialized application that uses a combination of session awareness, IP and asset correlation, and identity mapping to trace each activity back to the specific user who initiated it.

Controls Monitoring

Government agencies are subject to growing regulatory oversight. ArcSight solutions provide pre-built content mapped to best practices such as ISO 27002, and purpose-built content for regulations like PCI and HIPAA that impact segments of the government.

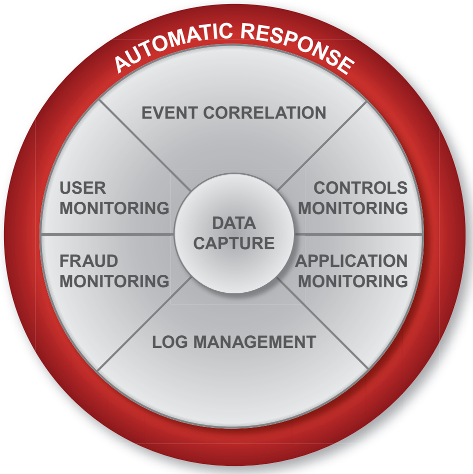
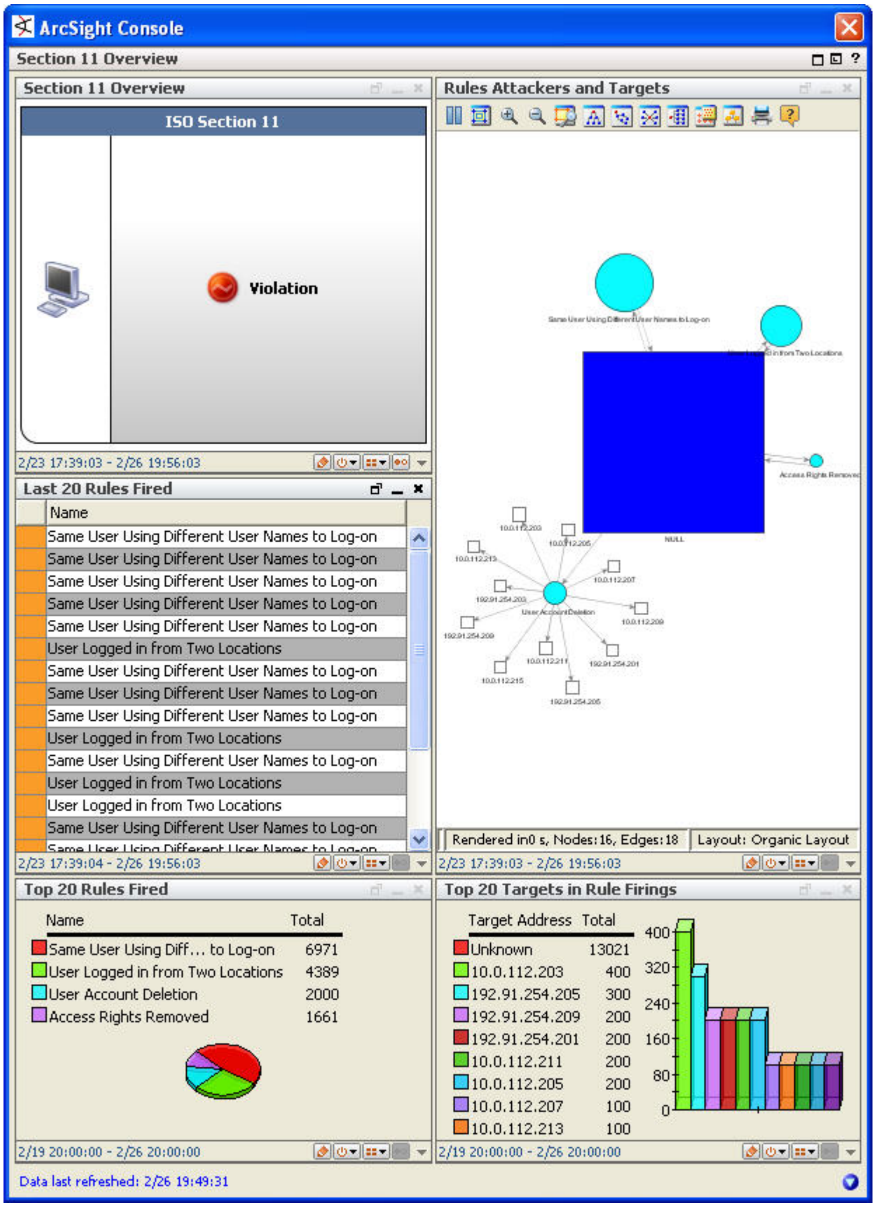


Figure 1: The ArcSight ETRM platform is modular and can be deployed collectively or in phases.

Highlights

- Protect sensitive data
- Secure critical infrastructure
- Combat cybercrime



ArcSight Console

Section 11 Overview

Section 11 Overview

ISO Section 11

Violation

2/23 17:39:03 - 2/26 19:56:03

Last 20 Rules Fired

Name
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
User Logged in from Two Locations
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
User Logged in from Two Locations
Same User Using Different User Names to Log-on
User Logged in from Two Locations
User Logged in from Two Locations
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on

2/23 17:39:04 - 2/26 19:56:03

Rules Attackers and Targets

Rendered in0 s, Nodes:16, Edges:18 | Layout: Organic Layout

2/23 17:39:03 - 2/26 19:56:03

Top 20 Rules Fired

Name	Total
🟥 Same User Using Diff… to Log-on	6971
🟩 User Logged in from Two Locations	4389
🟦 User Account Deletion	2000
🟪 Access Rights Removed	1661

2/19 20:00:00 - 2/26 20:00:00

Top 20 Targets in Rule Firings

Target Address	Total
🟥 Unknown	13021
🟩 10.0.112.203	400
🟦 192.91.254.205	300
🟪 192.91.254.209	200
🟥 192.91.254.201	200
🟩 10.0.112.211	200
🟦 10.0.112.205	200
🟪 10.0.112.207	100
🟧 10.0.112.213	100

2/19 20:00:00 - 2/26 20:00:00

Data last refreshed: 2/26 19:49:31

Figure 2: ArcSight solution packages map directly to best practices and regulations such as ISO 27002, FISMA, PCI and HIPAA to reduce the cost of audits and proactively detect compliance violations.

ESP-SLB015-122310-02, Created August 2011