

## Security Information and Event Management - SIEM

The modern organization has multiple IT components that produce thousands, and in some instances, millions of events in any given day. Finding those events that pose serious security risks is sometimes a tedious and manual exercise. This means that under a security attack, the IT and security teams cannot do their most basic job: identifying, prioritizing and defending against the highest priority threat.



So from a response standpoint, the strategy is to minimize the amount of time your organization is vulnerable to a security incident. This is where Cistel Security Solutions can help. We have partnered with the world leader on SIEM technology, ArcSight Inc., to provide you a reliable, repeatable and auditable capability to rapidly and automatically respond to different incidents in your infrastructure at multiple enforcement points.

### Most Common Threats

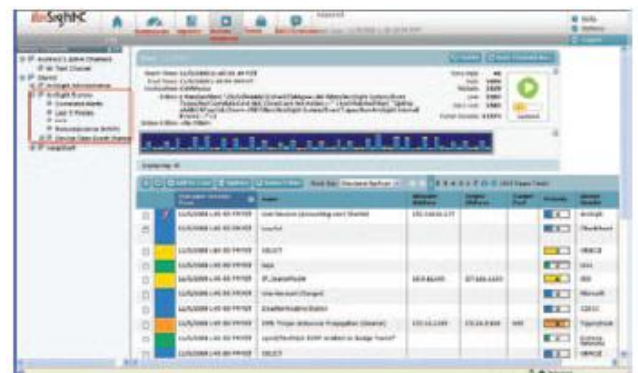
SIEM identifies the most significant problems:

- Bot, worm and virus attacks
- Hacker detection
- Unauthorized application access
- VPN sneak attacks
- Bandwidth hogs and policy violations
- System and user impacts
- Failed audits, fines and penalties

### The Benefits

A SIEM implementation will allow you to:

- Reduce risk and cost to your operations
- Monitor real-time events
- Comply with industry regulations
- Correlate events to pinpoint threats
- Deploy rapidly for fastest time to value



Correlation Alerts dashboard

## SIEM with Cistel Security Solutions

### ArcSight Family of Products

The ArcSight SIEM platforms have been designed to accommodate large, medium and small IT organizations:

- ArcSight ESM and ArcSight Logger provide complete visibility to monitor enterprise-wide business risk
- ArcSight Express is the security expert in a box, providing correlation, log management and automated compliance for the mid-size organization
- Specialized modules include ArcSight IdentityView, ArcSight Connectors, and ArcSight Compliance

### Value Proposition

Cistel Security Solutions takes the cost and complexity out of your SIEM program. We have designed an implementation plan **to enable your success in days, not weeks or months** and allow you to get optimal value from your investment immediately, while laying the foundation as your security needs and policies evolve:

- Effective integration of disparate, heterogeneous data sources
- Assess the timeframes involved and the resources required
- Ensure that the SIEM implementation ultimately maps to your organization's security objectives

Whether you are doing an initial implementation or addressing a new challenge, we can help.

### Cistel is Your Trusted Partner

Our customers have come to rely on our deep expertise on IT and consulting services. We can plan and deploy ArcSight appliances that will let you manage the security incidents to which your organization may be exposed. Our team has the product expertise, technical skills, and the commitment to understand your organization's capability and business processes:

- Work with your team to prioritize your requirements
- Assess your environment and objectives to fine tune the time and resources required
- Implement a tailored plan that will achieve desired results



Cistel is a reseller and partner with ArcSight Inc., ISO 9001:2000 certified by the Canadian General Standards Board and is a qualified supplier to the Government of Canada through CPSA, TBIPS, SBIPS, PS-Online and others.

For more information, please contact your Cistel Account Manager or email us at: [security@cistel.com](mailto:security@cistel.com)