

# Information & Asset Protection with SIEM and DLP

“Keeping the Good Stuff in and the Bad Stuff Out”

Professional Services: Doug Crich  
Practice Leader –Infrastructure Protection Solutions



# What's driving the need?

---

## Corporate Governance

*Do employees respect and adhere to internal policies and controls?*

*Are my assets protected against illicit behaviour?*

## Critical Infrastructure

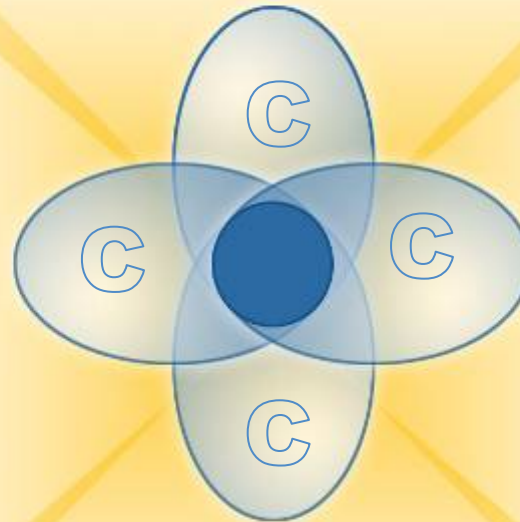
*Are intruders gaining access and removing data?*

*Is my network open to existing and emerging threats?*

## Competitive Advantage

*Are insiders putting the organization at risk?*

*What about my customers' and partners' data?*



## Compliance

*Are there regulatory risks?*

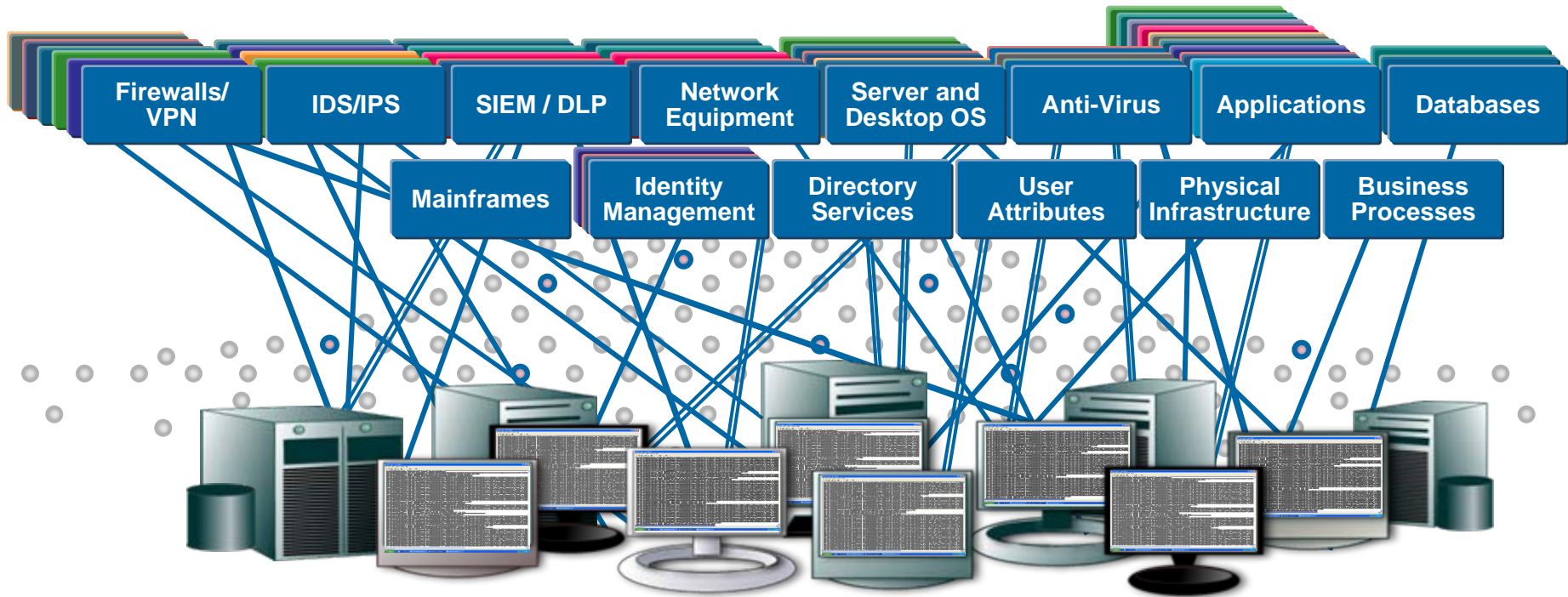
*Are all mandated controls in place?*

# IT security challenges

---

- Gap between Corporate Security Policy and the business use of IT
- Lack of integrated tools to enable situational awareness of security threats
- Thousands of devices & countless applications on Windows, Unix, Linux, etc.
- Spending countless hours investigating “incidents”
- Regulatory retention and reporting requirements are costly
- Decentralized responsibility for managing data and IT assets across the enterprise
- Functional teams require different types of log data for numerous reasons;
- Inventory of assets is not available or not up to date
- No clear view of where critical information and assets reside within the IT infrastructure.

# Making sense of events



**Centralized view provides:**

**Detection...**  
**of sophisticated threats**

**Ability...**  
**to monitor compliance**

**Control of Risk...**  
**to business continuity**

# DLP and SIEM – what are they?

---

**Data Loss Prevention (DLP)** refers to technologies and inspection techniques that detect and prevent the unauthorized use and transmission of confidential information.

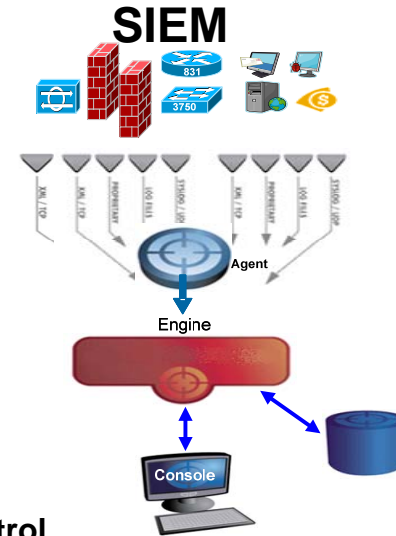
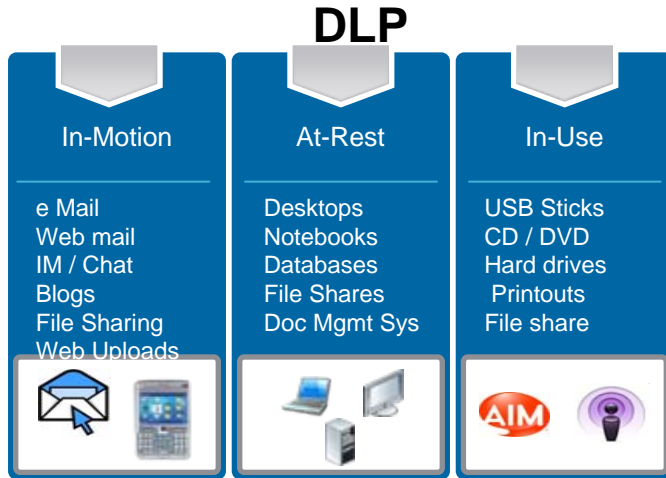
Aka Data leakage protection, Data leak prevention, Information leak prevention



**Security Information and Event Management (SIEM)** consists of managing and reacting to the information and events produced by IT Infrastructure

Aka –SIM and SEM

# What SIEM and DLP have in common



## Preventive Control

- Used to develop, educate and enforce security policies and governance related to handling and transmission of sensitive data
- Mitigates risk through identity aware policy based remediation and enforcement.
- Network, Host /endpoint and discovery (stored)
- Performs some level of remedial action - notification /alerting to active blocking based on policy settings.

## Detective Control

- Provides real-time security alerting and monitoring through log collection
- Filters, aggregates large quantities of data
- Correlates, analyses and scores events to isolate high risk threats
- Primary drivers are regulatory compliance, user activity and resource access monitoring, and;
- Real time event management for network security

*Key Elements of a Multi –Layered Information Security and Risk Management Plan*

# Implementation Considerations

# The vendor's value proposition

---

## The Promise

Out of the Box:

- DLP is ideal for information security and compliance
- SIEM technology provides a holistic view of internal and external threats
- DLP deployment is quick and requires low operational cost
- SIEM solutions improve operational efficiencies and cut administrative costs



## The Reality

*Not Without Considerable Planning , Configuration and Integration*

# The SIEM/DLP objective

---

**To be effective, an organization's SIEM/DLP framework must address and support the business objectives**

## **Strategic**

Protect the confidentiality, integrity and availability of systems and information,  
Improve Service, Legal and Regulatory Compliance;

## **Tactical**

Install Safe Guards and Countermeasures to prevent loss and minimize threats- mitigate risk;

## **Operational**

Implement security policies and workflow that ensures the organization functions in an efficient and predicable manner.



# Common SIEM / DLP deployment mistakes

- Technology implemented without formalized planning .
- Failing to understand what the technology is capable of and how and what to properly integrate it with.
- Lack of understanding of what and where sensitive data reside
- Inappropriate and/or ineffective log generation and capture
- Lack of commitment of project resources
- Little or no integration- systems , ops and workflow.
- Environment is not modelled
- Impacts of outsourcing arrangements are not considered



You Can't Hit A Bulls Eye If You Don't Know Where The Target Is!!

# Implementation best practices

---

- Stakeholder Participation
- Confirm Alignment to Business Goals
- Identify Data that Needs Protection
- Develop Use Cases
- Architect for CIA
- Implement by priority for “Quick Hits”
- Resolve conflicts between security controls
- IT Asset Classification
- Model the Network
- Integrate IDM or AD for more granular “role level” monitoring and reporting
- System Configuration and Tuning
- Technology Is Not A “Silver Bullet”
- Provide mentoring and support following “Go Live”



# Build an Ops framework

---

- Develop an organizational model;
- Create job descriptions and workflows;
- Perform an inventory of existing skills;
- Benchmark existing skills against best practices;
- Recruit and train qualified personnel;
  - Short Term Staff Augmentation
  - Outsourcing
- Align operations processes and procedures with technology workflow
- Provide training on functions, processes and technology to maximize productivity



# Bell's implementation methodology



## Planning & Design

- Requirements Gathering
  - Security Policy Alignment
  - Privacy and Compliance
  - IT Security Objectives
  - Data Classification & Handling
- Use Case Development
- Solution Architecture
- Network and Asset Modeling
- Organizational Model
- Design Sign-off
- Transition to Delivery



## Delivery & Implementation

- Infrastructure Implementation
- Systems Configuration
- Integration of tools and processes
- Content Development
- Training and Knowledge Transfer
- Testing and Tuning
- Sign-off
- Go "Live"



## Operation

- Monitoring and Reporting
- Incident Response and Remediation
- Content Management Updates
- Solution Evolution/Tuning
- Analysis
- Forensics
- Auditing

Continuously Refined to Maintain Alignment with Objectives

# Benefits of “proper” implementation

---

**Benefit**

**Pre-emptive Information Security and Risk Management**

**Benefit**

**Increased Operational Efficiency**

**Benefit**

**Key Elements of a Multi –Layered Information Security and Risk Management Plan**

# Bell is uniquely positioned to address SIEM/DLP requirements

---

- Broad experience developing and deploying information security infrastructure from concept to completion
- “Users” of leadership SIEM/DLP technologies passing best practices to our customers;
- Extensive internal/external ISO17799 compliant security policy development experience ;
- Multiple SOCs providing Security Services to Bell Customers and internally.
- Breadth and depth of ICT Security Solutions offerings provide key building blocks
- Extensive network of labs for solution testing, innovation and execution
- Comprehensive, Professional Services with packaged ‘toolkits’ for planning, deploying and operating SIEM/DLP within Government, Health, Finance, Manufacturing, etc.
- Experience implementing and integrating complex, multi-vendor solutions;
- Leverage our multiple partnerships with leading vendors for comprehensive solutions portfolio



# Bell Security Summit Special Offer

---

## SIEM or DLP Architecture Workshop

**Bell will provide a 2 hour Architecture Planning Workshop  
for either SIEM or DLP**

**Define Client's Requirements and Business Objectives  
Develop a High Level Solution Architecture**

**Limited time offer – valid until November 30.**

# Case Study – Large Canadian Financial Institution

---

## The Need/Challenge

- Financial institution is facing increasing challenges and pressure through legislative, public and internal means to safeguard corporate and operational information by instituting stronger infrastructure safeguards and controls.
- Required to secure and support over 22 different technologies from a multitude of vendors
- Existing vendors included Microsoft Windows Server 2008, Cisco, Symantec, Check Point, IBM, CA

## The Bell Solution

- Understand current log management infrastructure Through Consultation with stakeholders and knowledge Experts
- Analysis of log management ecosystem
- Categorization of the criticality of each network device
- Determine key business and security imperatives
- Provide a Vision with clearly defined measurable goals
- Conduct Survey or Log Mgmt. maturity within Canadian FIs
- Create a strategy and roadmap for

## The Result

- The Strategy and Roadmap provides a structured approach for the FI to evolve towards Log Management/SIEM Best Practices nationally

# Case Study – Large Manufacturer

---

## SUMMARY

### The Need/Challenge

- The organization had separate consoles for four different solutions that was resulting in lost efficiencies, missed security events, extensive manual processes and effort for the organization.
- Client required a all encompassing GRC Security plan including an automated event management process to ensure no critical events were missed.

### The Bell Solution

- Bell engaged the client in creating a GRC Security Roadmap.
- Bell partnered with ArcSight to Provide a "single pane of glass" consolidating event management and monitoring and enabling a Proactive response to events based on threat correlation and triggers.
- Bell partnered with best in class Vendors to enhance their security posture through deployment of SIEM, DLP and Secure Content Solutions.

### The Result

- Faster and more efficient determination of real actionable events that require immediate attention.
- Increase in productivity and Proactive response of the security team.
- Mitigated Corporate Risk Associated by protecting Intellectual Property.
- Preventive response to Data Loss.



## Q&A

For more information on Bell's SIEM, DLP and other Security expertise and offerings, please contact:

**Palma Petrilli**     [palma.petrilli@bell.ca](mailto:palma.petrilli@bell.ca)