



DELEMONT SECURITY SERVICES DIVISION

About Delemont Security Services Division

Delemont Security Services Division, the Laboratory for Information Technology Security, helps customers defend their databases, IT infrastructure, network, computers, applications, Internet offerings and access.

Delemont is also a full service provider of security intelligence to corporations, governments and international organizations.

Delemont relies on a network of research contributors worldwide (security professionals, ethical, hacker groups) and offers intelligence on previously unknown software vulnerabilities. The Delemont team is composed of internationally known information security researchers who often speak at security conferences and events around the globe.

Delemont has security expertise in all areas of known and unknown vulnerabilities, malicious code, and exploits.

Delemont provides its customers with regular reports on new vulnerabilities, network attacks, and IT threats. Delemont also advises on protection, and provides a comprehensive set of potential countermeasures.

DELEMONT SERVICES "ON CALL"

The Delemont research and consulting team can enhance every area of IT, Application and Network system security.

By embedding security measures into overall day to day IT policies organizations can help to ensure that software vulnerabilities and other threats are detected and addressed before they become cause high impact damage.

Delemont can execute customized security services based on client specific infrastructure and application environments.



INFRASTRUCTURE AND APPLICATION SECURITY

Delemont can provide high-end internationally skilled resources in the area of:

– *Network Pen Testing, Web Application Penetration Testing*: Delemont has developed sophisticated methodologies and has considerable expertise in penetration testing and web application security.

Delemont can protect its customers preserving the integrity of their IT infrastructure and the intellectual property it contains.

Delemont will operate infrastructure reviewing, identify weaknesses, and with Actively Penetration Testing will attempt to breach security measures , simulating an experienced attacker or malicious individual inside or outside the organization.

As an example Delemont, upon agreement with the customer, will attempt to: put in place Firewall/IPS/IDS evasion and exploitation, crack wireless keys, compromise remote access systems, retrieve corporate email, instant messages, client account lists, phone calls, passwords, administrative records and intellectual property in general

Delemont can perform an in depth examination of the current state of its client IT infrastructure to identify methods that an attacker might use to access Network, Applications and Databases.

Delemont will also verify the effectiveness of current internal security controls and isolated target areas in its client infrastructures, prioritizing action and remedies to be put in place. As an example, Delemont can inspect: security of mail servers and messaging servers, verify password strength policies, validate wireless networks exposure, check VPN and remote access security standards, test the quality of system events logging.

– *Anti-Data Theft*: Delemont has in house resources and uses the latest techniques to fight Data Theft and helping its client to protect against these attacks.

– *Product Assessment*: Delemont can examine custom application or software vendor's products for security vulnerabilities

– *Advanced Countermeasures against Security Exploits*.



- *Software testing and bugs discovery: Delemont researchers can help customers performing black box audits on software.*

- *Corporate Infrastructure auditing: Delemont can advise its clients on how to setup a secure infrastructure to protect an organization's data, applications, and systems.*

Delemont experienced consultants can work together with its business partners on the end client infrastructure to identify areas of high risk or weakness, and to address security issues with consistent solutions.

Delemont will deliver Infrastructure Audit reports in a format specifically designed to encourage our clients and partners to effectively reduce security exposure at all levels.

INCIDENT REACTION SERVICES

Delemont services are designed to meet the needs of those organizations that have already incurred a security breach and of those who wish to create a plan for incident management if and when it occurs. Using security best practices (processes, policies, guidelines) Delemont supports companies reacting to an identified or suspected system breach, security attack or computer misuse. Delemont can:

- identify the kind and depth of penetration, method of attack, which information is at risk or has been altered, type of compromise
- assess the damage to the network.

Delemont can subsequently advise on improvement of detection systems and incident response best practice.

SECURITY CONSULTING SERVICES

By utilizing and recommending proven practices, educating key personnel of organizations and working with appropriate technologies, Delemont helps mid sized, large corporation, governments and international organizations with:

- IT Security Project Management



- Vendor Due Diligence
- Coaching and Advisories for Executives
- Coaching and Advisories for Technical Executives (CIO, CTO)
- Enhancement of Enterprise Security Programmes
- Alignment of Security and Privacy Practices with enterprise and international regulatory policies
- Alignment of Security and Data Privacy Practices with Business Strategy