Xposure Security Monitor

xposure

Tools for Enhanced Security Management

Automated Security Monitoring

- Real Time Analysis and Correlation
- Rules-Based Prioritization and Notification
- Automated Threat Identification
- Highly summarized views plus drill-down
- Ad-hoc detail queries for forensics / analysis
- Supports the multi-vendor Enterprise
- Security focused
- Distributed Model

6 Areas of Interest:

Threats
Probes
Attacks
Failed Authentications

Misuse
Misconfigured Systems
Trojan Horses
Employee Abuse

Use
Traffic vs. Capacity
Traffic by Type
Misconfigurations / Abuse

System
Device & Network Errors
Misconfigurations
Failovers

Admin
Audit trail

VPN
Tunnel Errors
Tunnel Failures

Managing Xposure

Managing network and system security is challenging — the security components upon which today's Enterprises are built generate huge volumes of event and traffic data. Unfortunately, there is just too much data to make sound security decisions with.

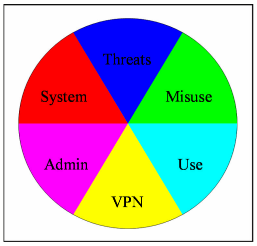
To complicate matters further, point solutions such as firewalls, Intrusion Detection Systems, and servers present their data in obscure and inconsistent formats.

The result of this is that most organizations cannot use this data to be proactive about security. Log information is typically viewed only after-the-fact for forensic purposes.

Xposure is a software tool that collects event information from multiple sources within the Enterprise. It establishes a common ground for interpreting these events by translating them all to a standard security model.

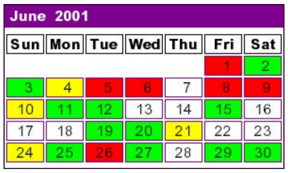
Once in a common format, events from these disparate sources can be correlated, prioritized, and acted upon quickly and automatically.

Xposure sorts events into 4 event categories and 2 traffic categories for clear and consistent alerting, analysis, and reporting, regardless of an event's source.



Enterprise-specific rules are applied to all events to ensure that automated prioritization, alerting, and response reflect the organization's security policies and procedures.

Standard reports are automatically generated. These provide a highly summarized view with rapid drilldown to the event level to speed the analysis and response process.



June 2001

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					🟥 1	🟩 2
🟩 3	🟨 4	🟥 5	🟥 6	7	🟥 8	🟥 9
🟨 10	🟩 11	🟩 12	13	14	🟩 15	16
17	18	🟩 19	🟩 20	🟨 21	22	23
🟨 24	🟩 25	🟥 26	🟩 27	28	🟩 29	🟩 30

The Report Library includes popular reports which may be generated on an ad-hoc basis.

The Report Builder supports detailed custom investigation—new reports can be designed and added to the Report Library as needed..

Real Time and Historical Views

Xposure provides real time management of events to support rapid response to security issues. It also provides historical reporting to support proactive planning and maintenance of the security infrastructure.

Security events are processed in real time as they are logged by security components throughout the Enterprise.

Threats are correlated over time, point of origin, destination, and type of attack to facilitate detection and subsequent investigation.

Enterprise-specific rules are applied to the events to prioritize them and choose what actions should follow—alert, log or discard, identify the source, or run a custom response program. Automation is the key to managing the millions of security events that occur each day.

Historical timeline reports allow trends to be easily identified in event or traffic volumes to support planning. Historical distribution reports allow event and traffic profiles to be easily compared over time to identify emerging problems.

Respond quickly

Minimize Resources

See the Enterprise

Plan Effectively

Event Reporting

Rapid response and analysis of security events is Xposure's main goal. To make this possible, every event received is classified and sub-classified within four "Areas of Interest":

- Threats
- Administration
- System
- VPN

Threats include any events that could represent an attempt to probe or compromise security.

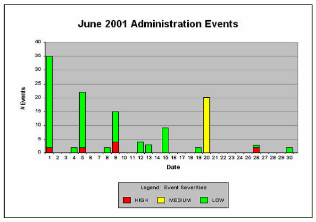
Administration provides an audit trail of administrator actions on security devices.

System events include internal errors or network / system problems that can impact the operation of security devices.

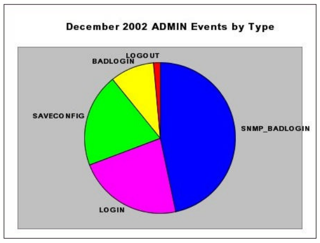
VPN events include establishment and failure of tunnels as well as errors and authentication problems related to VPN tunnels.

Event timelines may be viewed at four levels of detail to support quick identification of issues and drill-down to support analysis and forensics.

- Calendar Summary
- Month
- Day
- Event detail



Distribution views allow a profile to be developed of the baseline security activity in the Enterprise.



Traffic Reporting

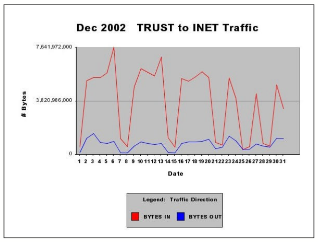
Valuable information about performance, security threats, and configuration errors is buried in the volumes of traffic detail a firewall can generate.

Xposure provides a view into traffic volumes across four dimensions:

- Time
- Location
- Use vs. Misuse
- Traffic Type

Timeline traffic reporting allows changes to traffic profiles to be identified through a monthly or daily view, identifying growth trends or anomalous activity.

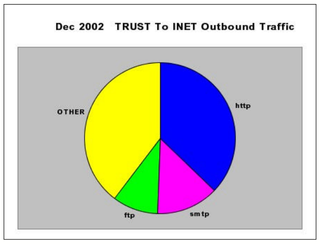
Reporting by location allows the traffic between any pair of security zones to be viewed. Zones can directly match the security boundaries implemented by firewalls, or arbitrary custom zones can be defined (e.g. to segregate traffic by customer in an ASP setting). Zone segregation in reporting allows traffic to be analyzed relative to security objectives and policy.



Traffic in reporting is differentiated between traffic that was permitted or denied passage by firewall policy. Permitted traffic statistics provide a foundation for performance planning and bandwidth provisioning.

They can also expose opportunities to further restrict policies. Denied traffic statistics show intentional or unintentional attempts to violate security policy.

Reporting by traffic type identifies the distribution of network services used, allowing anomalous traffic to be readily identified and quantified. Well-known traffic types as well as Enterprise-specific custom types can be defined to best reflect the business' services



Contact LCM Security Canada:

LCM Security, Inc.
2 Robert Speck Parkway
Mississauga, Ontario
Canada, L4Z 1H8

Phone: (905) 306-3457
FAX: (905) 815-8324

Contact LCM Security USA:

LCM Security, Inc.
9810 Twingate Drive
Alpharetta, GA 30022

Phone: (770) 417-5894
Fax: (770) 417-1430

Email: sales@lcmsecurity.com
Web: www.lcmsecurity.com