CSP Security.com
SOLUTIONS FOR HP NONSTOP SERVERS

Prevention and Detection

A Risk Based Approach to implementing Security

Thomas Leeb / Peter Grainger

WWW.CSPSECURITY.COM

GTUG Hotspot 2012, Dresden Sep 27th

About CSP

- Based in Toronto, Canada.
- NonStop® DSPP Partner since 1987.
- Develop, Support and Distribute Security and Audit Solutions for the HP NonStop® Market.

- Customers include:
  - Largest Banks
  - Major Stock Exchanges
  - Defense and Healthcare organizations
  - Telecommunications
  - Manufacturers

Business Partner

hp®

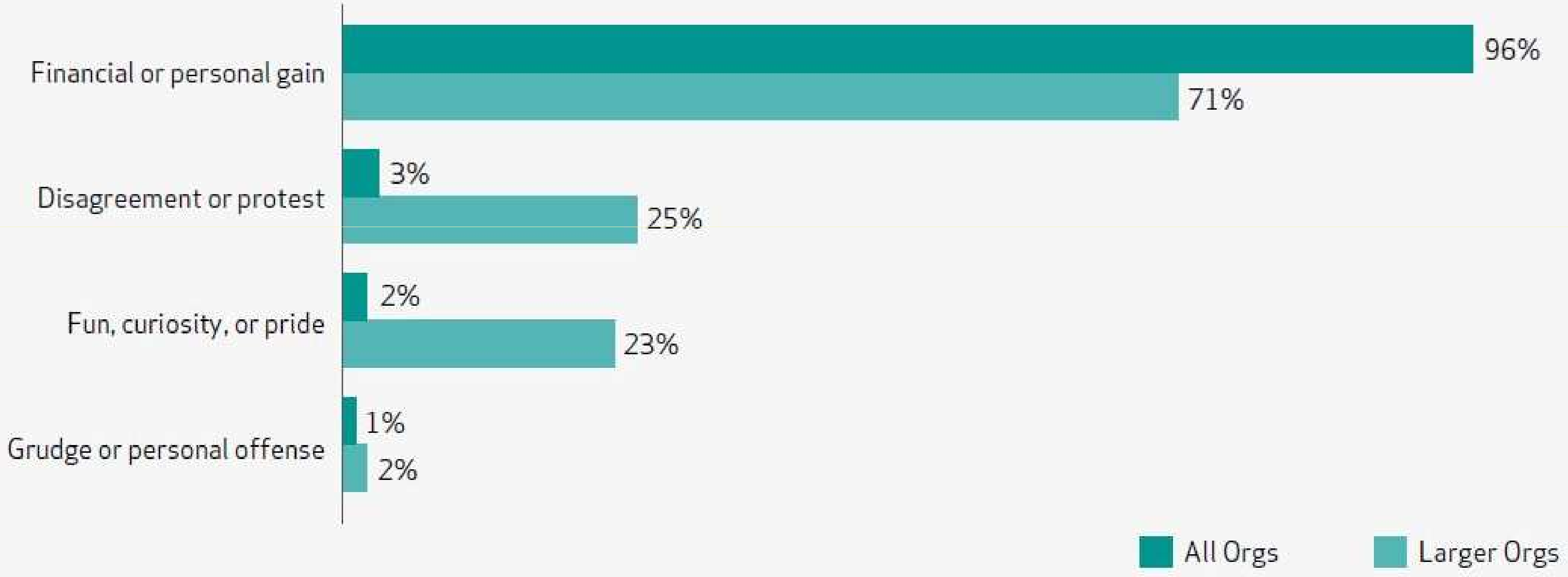
invent

Why should you care ?

- There are 2 data breaches / day (datalossdb.org)
- Significant consequences
  - Financial damage, lost business
  - Lost reputation, lost customers
  - Fraudulent activity with direct financial impact
  - Fines for non-compliance, license withdrawals
- „Compliance“ is mandatory but not the ultimate answer to security requirements / reducing risk

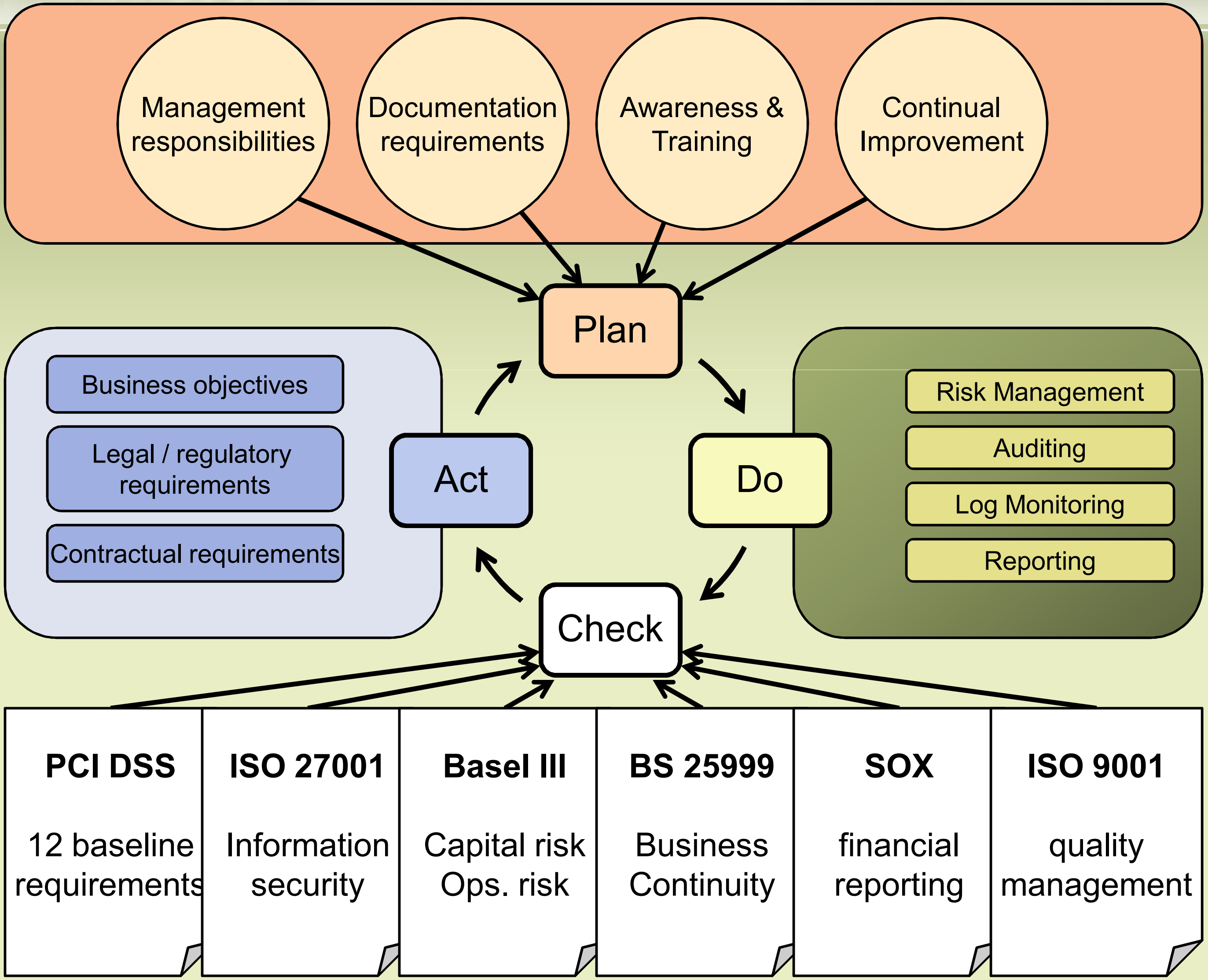
The motivation for cyber crime

Figure 15. Motive of external agents by percent of breaches within external



Source : Verizon 2012

ISMS using UCF



Risk based approach / questions to ask

- What could go wrong ?
- What‘s the probability of it happening ?
- What would be the consequences ?
- How can we reduce the probability of it happening ?
- How can we reduce the impact if it did occur ?
- How will we know that it is occuring or about to occur ?
- What is our contingency plan if it does occur ?

Measuring and Quantifying Risk

- **ALE – Annualised Loss Expectancy**

ALE = SLE * ARO

Sample case : risk of potential data breach
SLE = 6 M$
likelyhood of occurence : Once in 12 years

ALE = 6 * 1/12 = $500,000

Investment in intrusion detection and data encryption :
SLE(target) = 2 M$
likelyhood of occurence = once in 25 years

ALE = 2 * 1/25 = $80,000

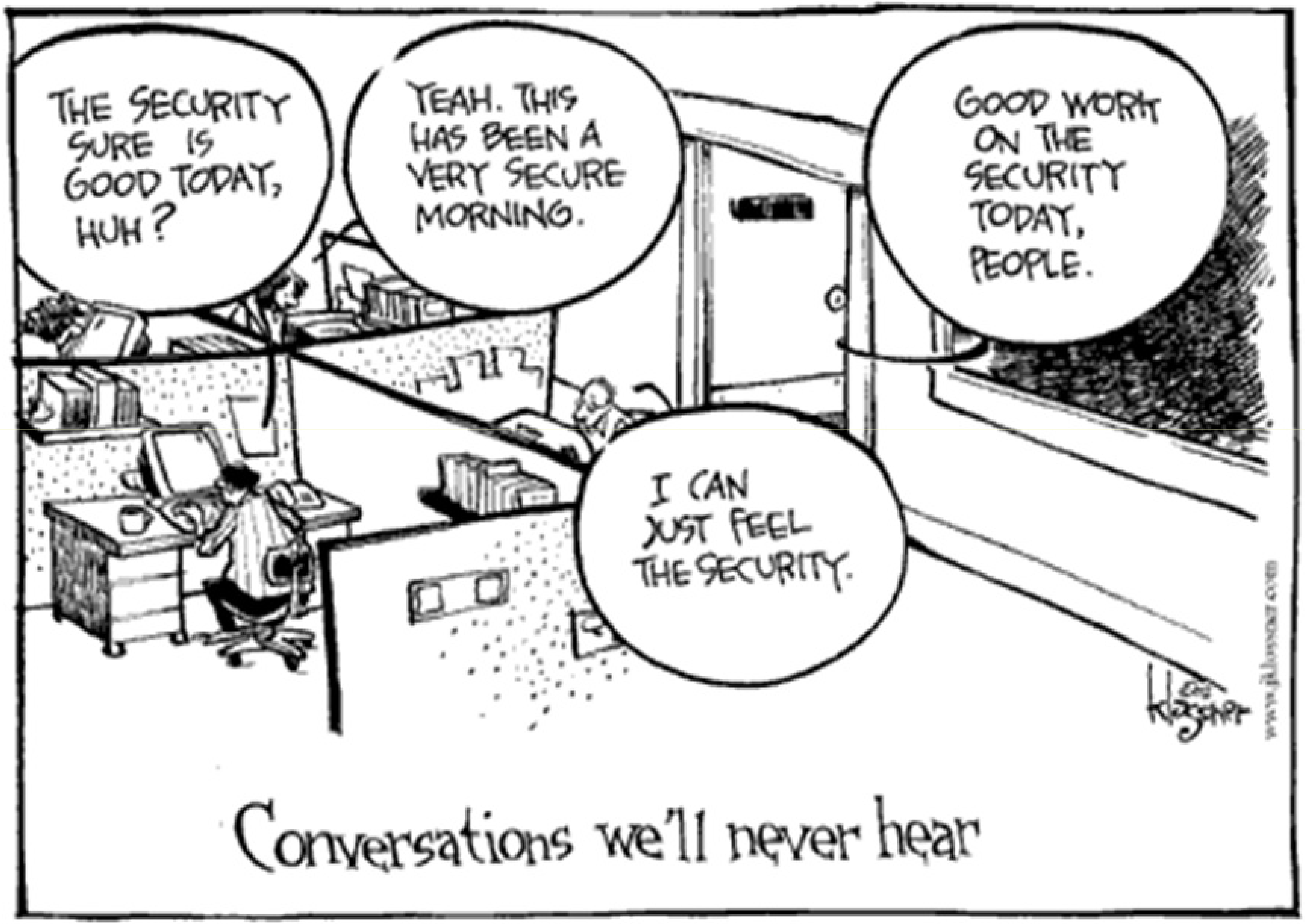
The 2 Dimensions of Reducing Risk

Reduce Probability of Incident

- Authentication control
- Access restriction policies
- Password mangement
- Encryption
- Usage restricition of administrative tools
- Time based access control
- Change control procedures
- Software updates
- Vulnerability management
- Policies for reporting weaknesses
- …

Reduce Impact of Incident

- Real time event Monitoring of user activities
- Detection of unauthorized actions
- Filtering, Alerting and Escalation
- Monitoring and reporting of security Events
- Log Management
- File Integrity Monitoring
- Network intrusion detection
- O/S level intrusion detection
- …


THE SECURITY SURE IS GOOD TODAY, HUH?
YEAH. THIS HAS BEEN A VERY SECURE MORNING.
GOOD WORK ON THE SECURITY TODAY, PEOPLE.
I CAN JUST FEEL THE SECURITY.
Klossner
www.jklossner.com

Conversations we'll never hear

You’re compliant

So you’re secure

CSP Compliance products

Compliance Reporting Module

PCI DSS
SOX
NSK Best Practices

File Integrity Checker

PCI DSS 11.5
Critical files given unique fingerprint

But are you really secure ?

- Compliance is generic
- How many people really understand Tandem security ?

Tandem Security issues

Little outside knowledge

Security through obscurity?

Few “High School” virus attacks

Almost all external attacks aimed at Microsoft and Unix

Limited targets

Other platforms offer far larger number of targets

Code and data segment architecture

Difficult to corrupt programs, pass on worms, etc.

So – The NSS is quite secure from the outside world

BUT

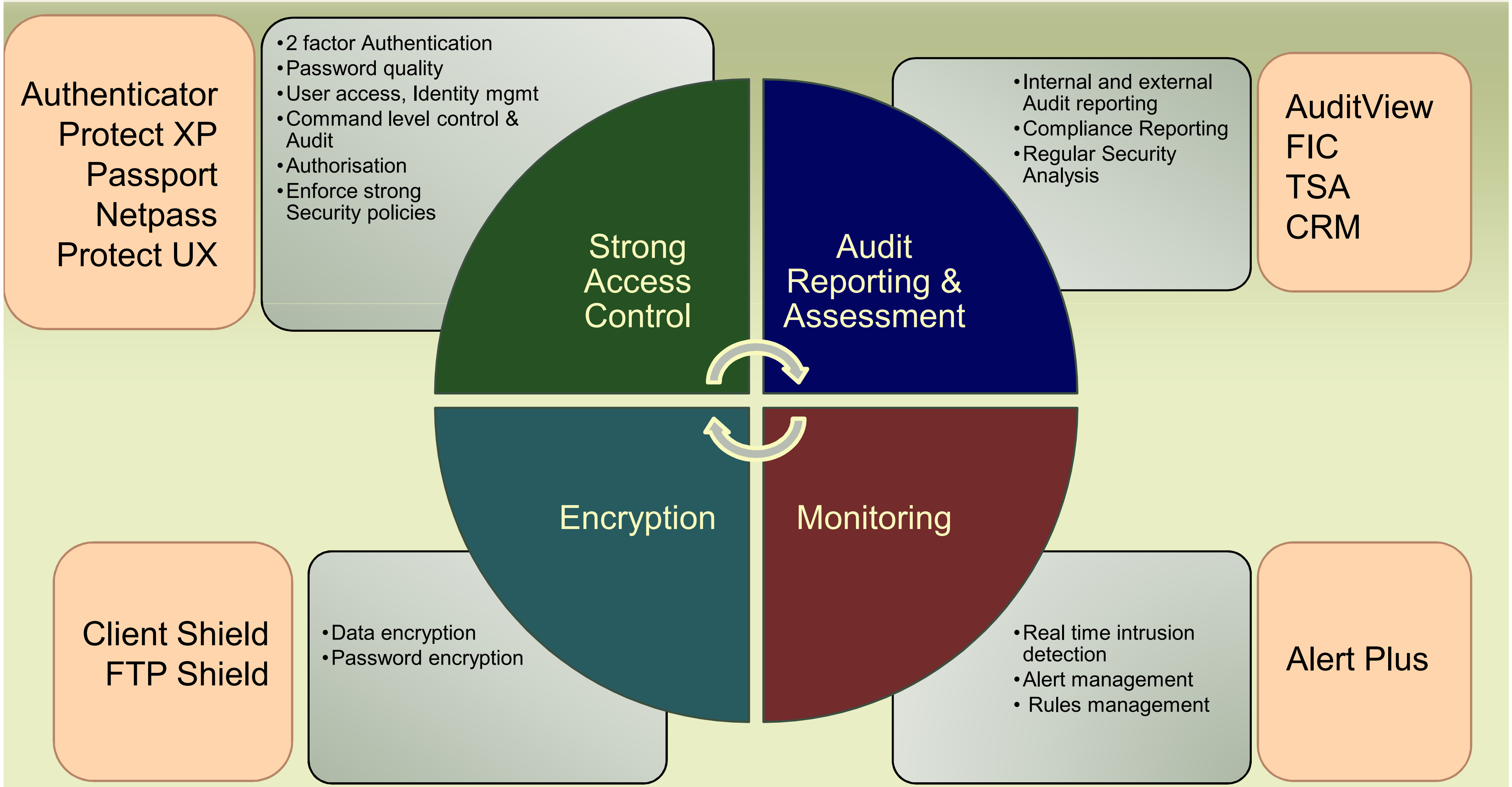
What of internal attacks ?

How do we block the weakest link ?

What’s missing ?

- Session/Command control/auditing
- Strong Authentication
- Assurance/Compliance?
- Easy User Interface
- LAN Encryption
- Intrusion Detection
- Real-Time Alerting

CSP Solution Portfolio



Authenticator
Protect XP
Passport
Netpass
Protect UX

- 2 factor Authentication
- Password quality
- User access, Identity mgmt
- Command level control & Audit
- Authorisation
- Enforce strong Security policies

Strong Access Control

Audit Reporting & Assessment

- Internal and external Audit reporting
- Compliance Reporting
- Regular Security Analysis

AuditView
FIC
TSA
CRM

Encryption

Monitoring

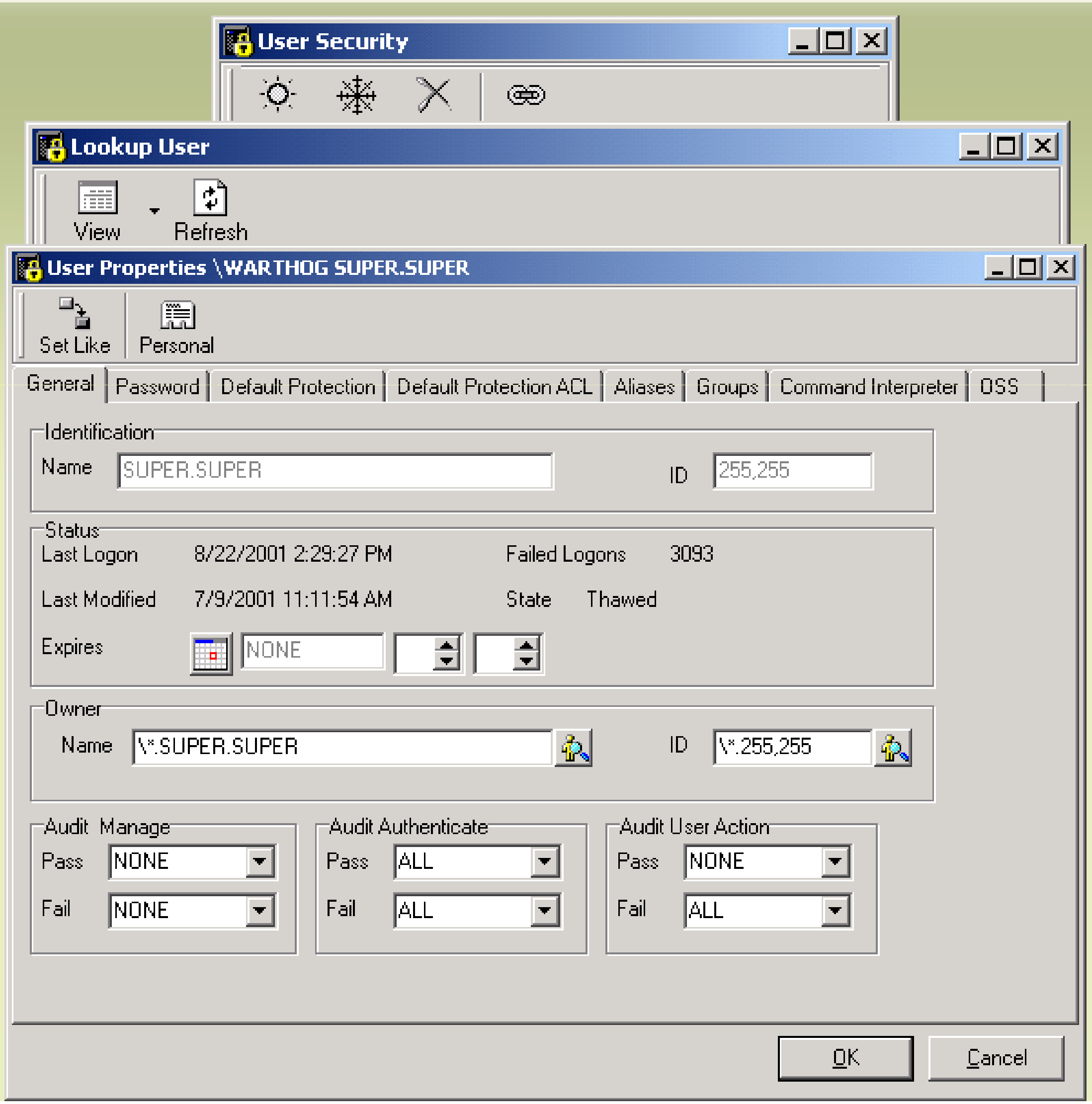
Client Shield
FTP Shield

- Data encryption
- Password encryption

- Real time intrusion detection
- Alert management
- Rules management

Alert Plus

Easy GUI



User Properties \WARTHOG SUPER.SUPER

Identification
Name: SUPER.SUPER
ID: 255,255

Status
Last Logon: 8/22/2001 2:29:27 PM
Failed Logons: 3093
Last Modified: 7/9/2001 11:11:54 AM
State: Thawed
Expires: NONE

Owner
Name: *.SUPER.SUPER
ID: *.255,255

	Audit Manage	Audit Authenticate	Audit User Action
Pass	NONE	ALL	NONE
Fail	NONE	ALL	ALL

Solution

Compliance AND efficient security

NonStop Security – Best of Breed

Past

Reporting – **AuditView**

Present

Real-time alerting – **Alert-Plus**

Protection

Protect XP

Passport

CRM and FIC

Client and FTP Shield

Thank you !

**„Distrust and Caution
are the parents of Security.“**

(Benjamin Franklin)

For additional information please contact

Thomas Leeb (CSP Sales)
thomasl@CSPsecurity.com
+43 699 1856 3888

support@cspsecurity.com