



Workshop on Building Security
Checklists for IT Products
September 25-26, 2003

***Vendor Session – Business Case Analysis for Checklist
Development***

2:00-3:30 September 25

***Dennis R. Moreau
CTO, Configuresoft, Inc.***

***Vendor Session – Business Case Analysis for
Checklist Development***

Vendor panel to discuss the business case advantages and disadvantages for the internal development of checklists for the products they produce. The panel will also focus on the advantages the checklists provide to the consumers of the vendors' products.



Internal Development of Product Security

Checklists: Business Drivers

- Reduction in risk of product-related exploit
- Large increase in customer interest in documentation of product security configuration recommendations (Security teams); will grow to include SE
- Specific segments increasingly requiring listing and or certification as part of procurement (military, government, financial, medical ...)
- Elevated customer expectation from competing and complementary product announcements (MS, IBM, ...)
- Improved customer perception => potentially improved prospects

© Configuresoft, Inc. 1999, 2003



Internal Development of Product Security

Checklists: Improved Efficiencies

- Product security depends on security of underlying facilities (OS, DB, services, protocols...). => Can leverage secure configuration recommendations, less validation of plumbing
- Reduction in development costs by creating early focus on security configuration requirements (late stage accommodation is very expensive)
- Reduction in reactive pre-sales support costs (collateral, rfp responses ...)
- Reduction in post-sales support costs by establishing tested product security checklists

© Configuresoft, Inc. 1999, 2003



Internal Development of Product Security Checklists: Other Security Efforts

- Cost of security certification is becoming barrier to entry for ISVs - *Gartner, IT Security Summit 2003*
- CC - \$300,000 (limited claims)
- FIPS - \$150,000
- Export Approval
- ...

Costs, process delays and ambiguity diffuse investment in product security

© Configuresoft, Inc. 1999, 2003



Internal Development of Product Security Checklists: Leveraging Effort

- Isolate encryption, authentication, RBAC, transport, ... functionality into discrete subsystems (decouple from core product)
- Consolidate and harden external interfaces
- Document and track security configuration dependencies on underlying facilities (e.g. OS, DB, services, RPC ...)
- ...

Can consolidate some costs across compliance efforts
Can isolate parts of product from potential delays (code review, waiver .. processes)
Can leverage design documentation efforts

© Configuresoft, Inc. 1999, 2003



Customer Advantages

Selection: Up front indication of security driven configuration constraints and capabilities

Operational: Streamlined assessment & remediation. Reduced risk.

Compliance: Potentially simplified audit and compliance efforts

Future: Normalization of evaluation of product security provisions/limitations

© Configuresoft, Inc. 1999, 2003