# Security Monitor

## *Automated Security Management - Possibilities and Limitations*

Chris Wahl; atsec information security GmbH

for

Gesellschaft für Informatik e.V., Fachgruppe SECMGT

*Workshop: Managed Security vs. Security Management*

# Agenda

- Security management challenges and questions
- A solution: the Security Monitor
  - Scenarios for the Security Monitor
  - Concept and principles
  - Implementation overview
  - Possibilities and Limitations of the components
- Conclusion
- Questions and Discussion

# Questions of InfoSec People

- Are there new **vulnerabilities** in the products used ?
- How are system management teams **informed** about security problems of individual components ?
- How to **monitor** and **track** if security problems are taken care of ?
- How to continuously **monitor** and **document** the overall security status?
- How to do all this in a revisable manner?

# Some more of it …

- Are all systems **configured securely** ?
- **System configurations** change quite often – how secure is a system after a change is made ?
- Have important **files** or **configuration parameters** changed?
- Have **access rights** to critical resources changed ?
- Are my systems **under attack** ?
- How to monitor, control and document the current configuration when running **n x 100 servers** ?

# Challenge

Implement a solution that:

- monitors the security situation of an IT environment
- uses existing infrastructure
- includes IDS and CERT architecture
- integrates in an existing FLS and SLS environment
- allows to identify and trace activities to improve the security situation
- supports monitoring of the BS 7799 controls

→Automate as much as possible

→Integrate as much as possible

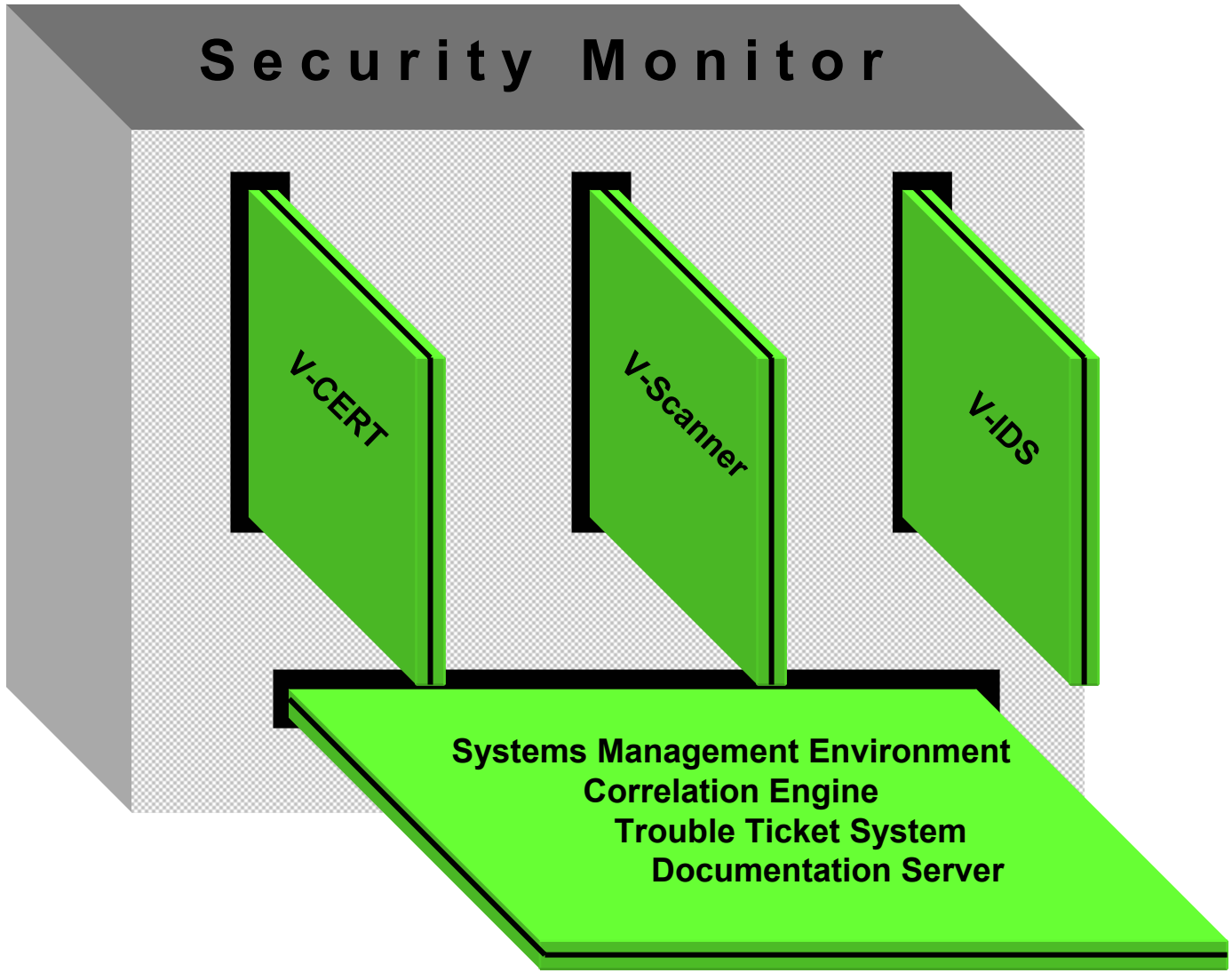
# Security Monitor

## Gives a solution that

- automates and correlates *as much as possible* (monitoring, tracing, CERT, IDS…)
- integrates automated tasks into the existing systems management environment
- allows to trace activities to improve the security situation

  *However, human interaction, thinking and reaction is required (e.g. to resolve security incidents)*

# Security Monitor Components



# Features

## V- SCANNER

Checks the configurations of system components for compliance with the defined security profiles and the absence of known vulnerabilities and informs SLS teams using the trouble ticket system

## V- CERT

Warns when new vulnerabilities or incidents are published (e. g. CodeRed or Blaster)

## V- IDS

“Sensors” detect attacks and critical modifications in real time and inform the SLS teams (Trouble Tickets)

## System Support

Documenting the reaction to trouble tickets.

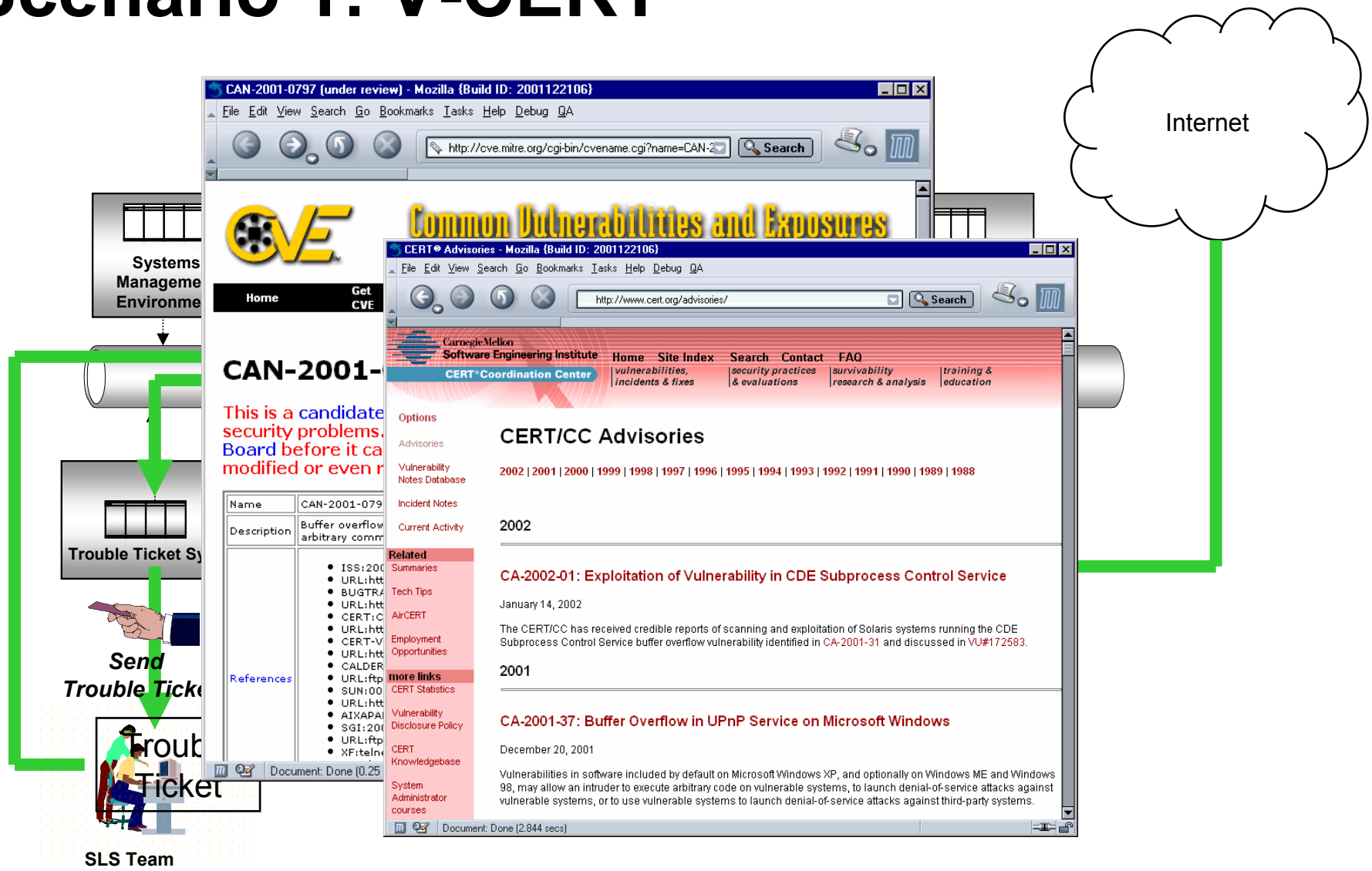
Adapting V-Scanner profiles and V-IDS signatures

Security Status View shows security situation

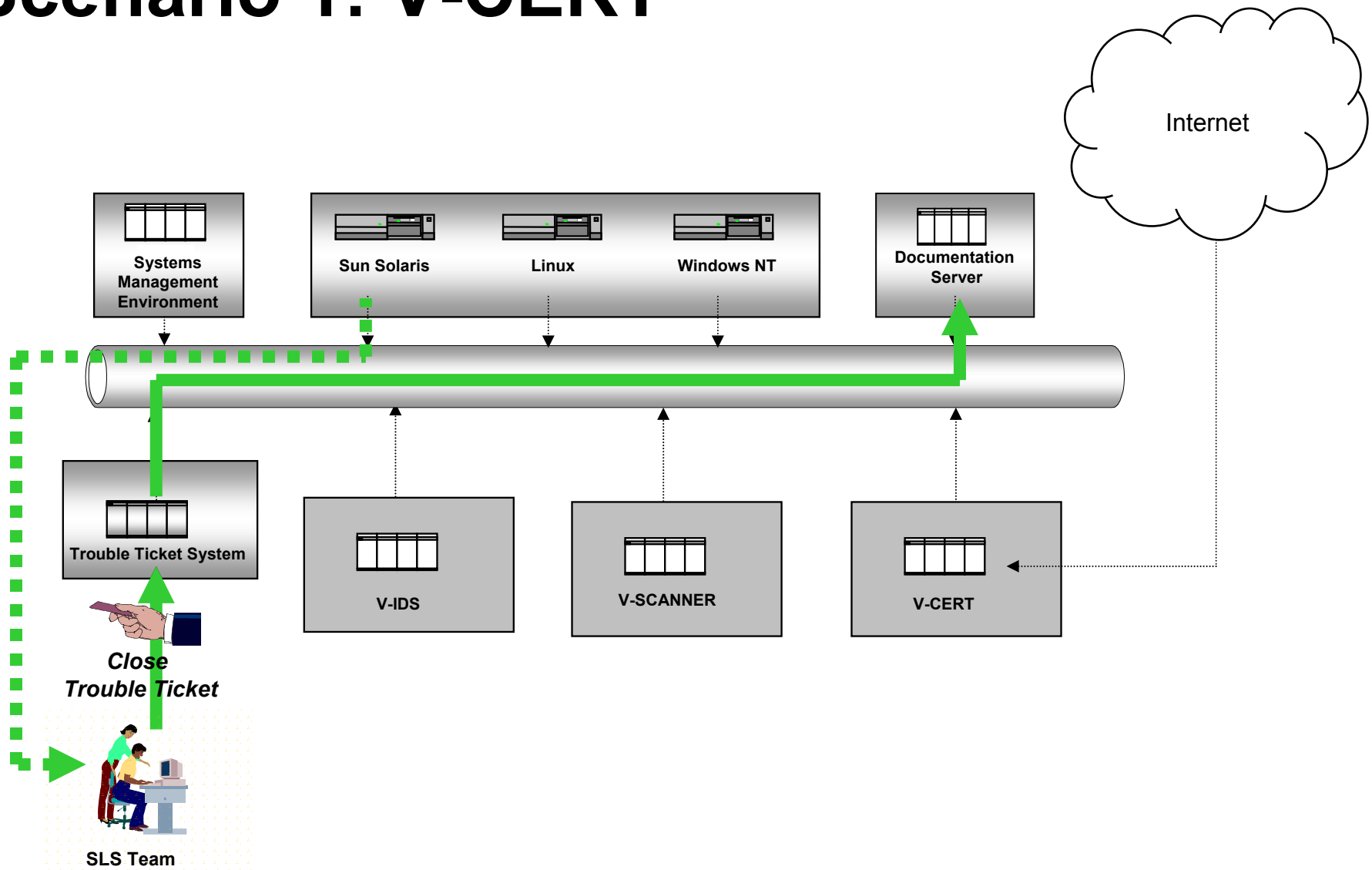
….

….

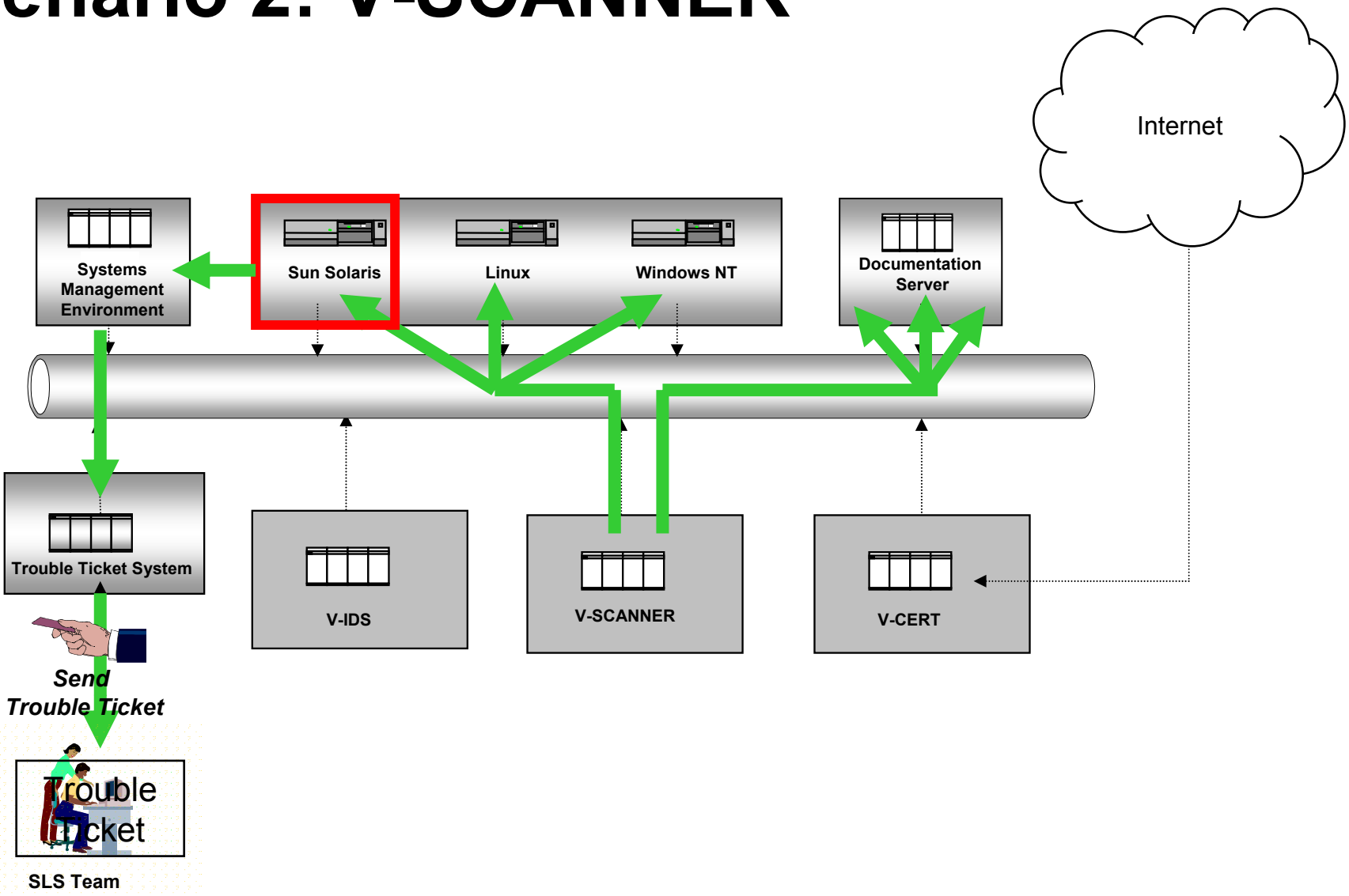
# Scenario 1: V-CERT



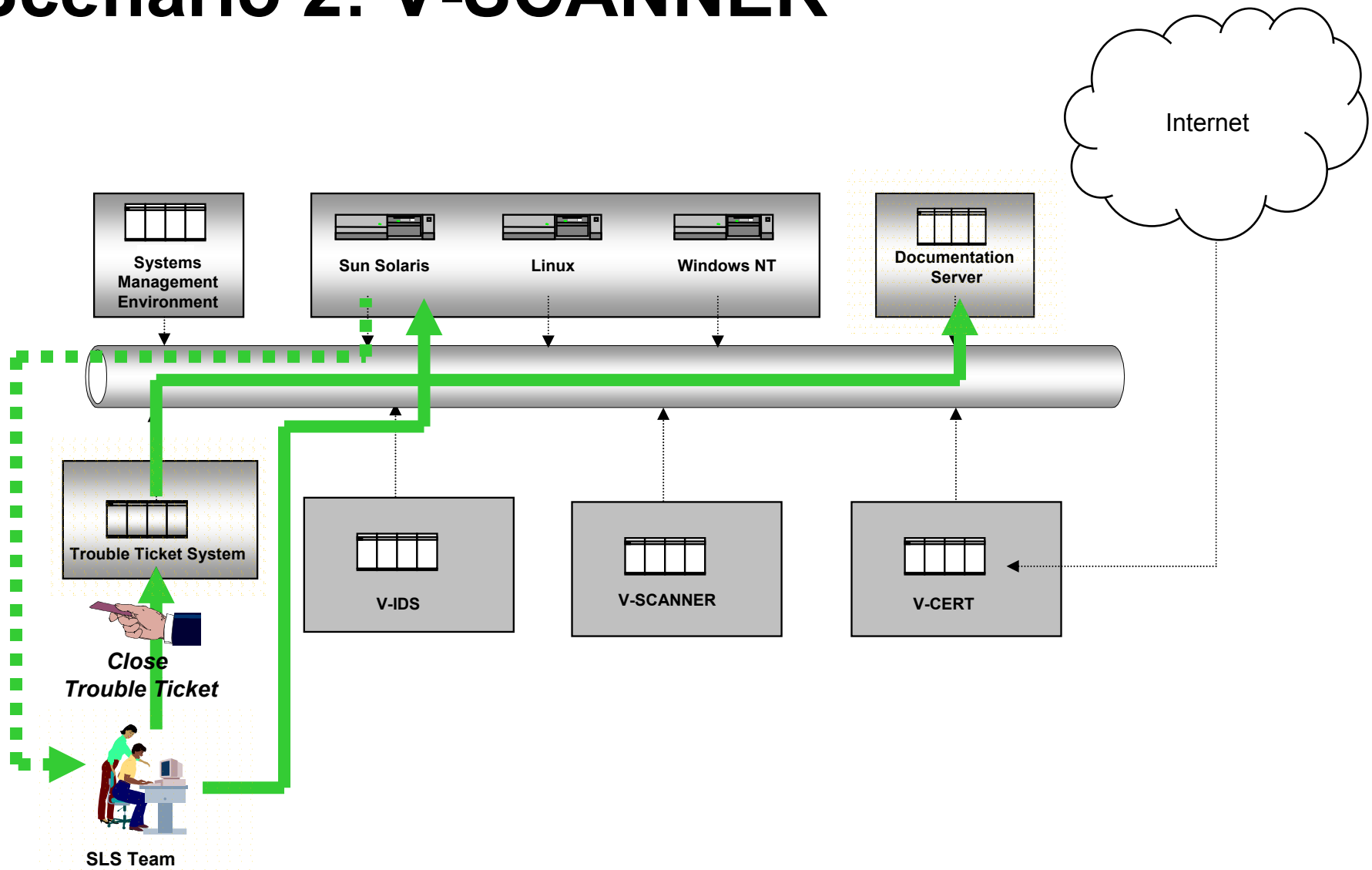
# Scenario 1: V-CERT



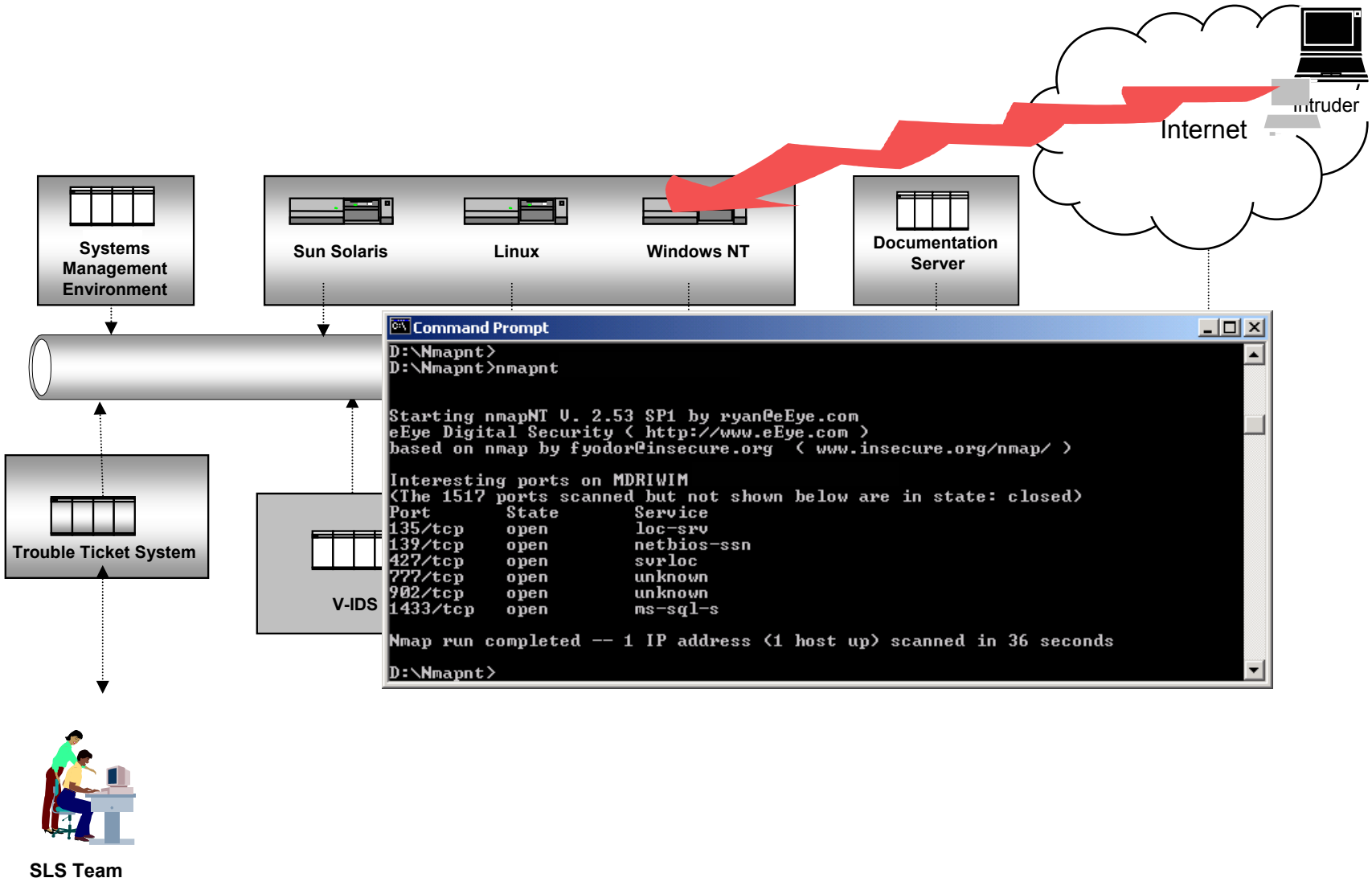
# Scenario 2: V-SCANNER



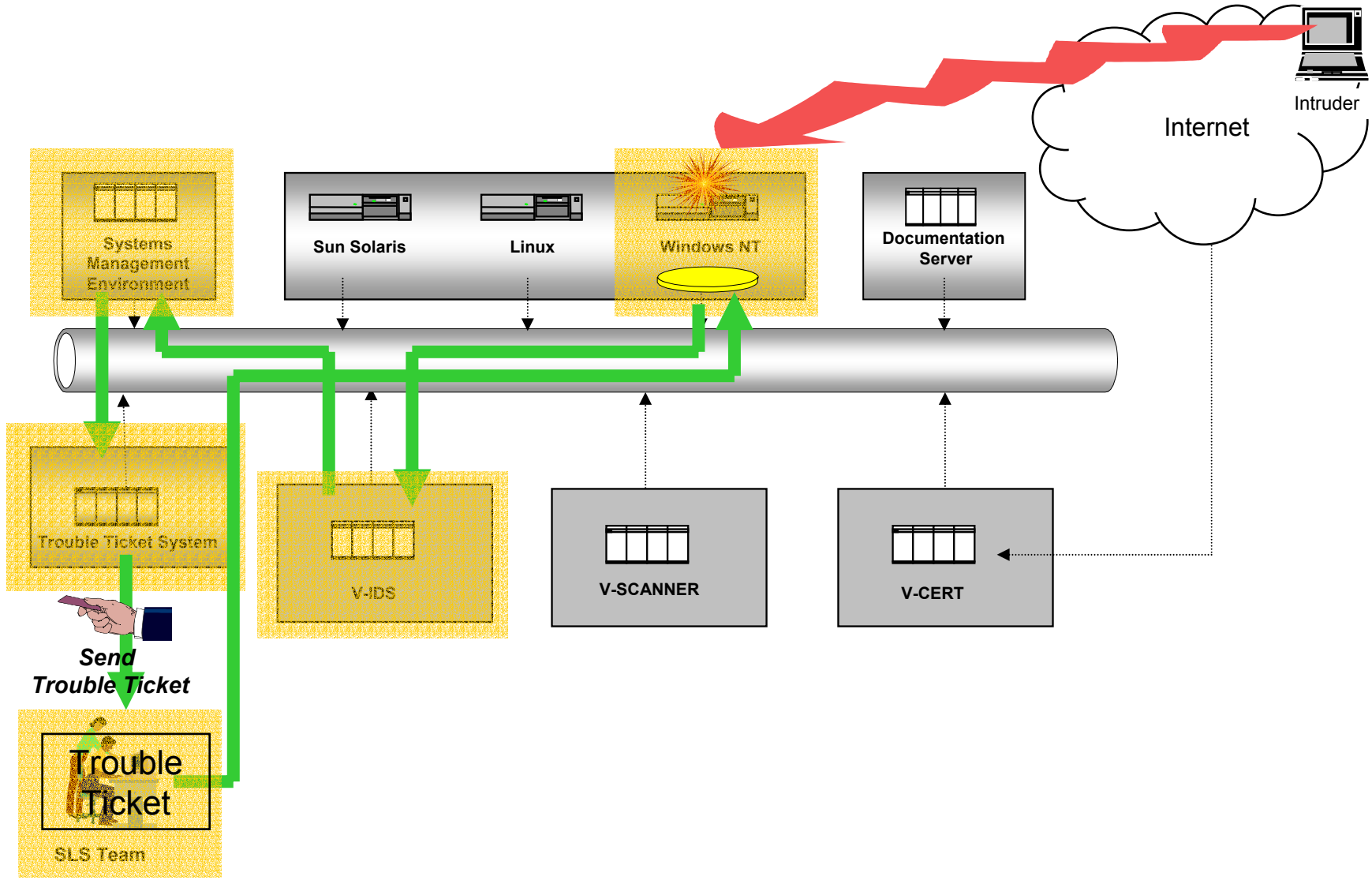
# Scenario 2: V-SCANNER



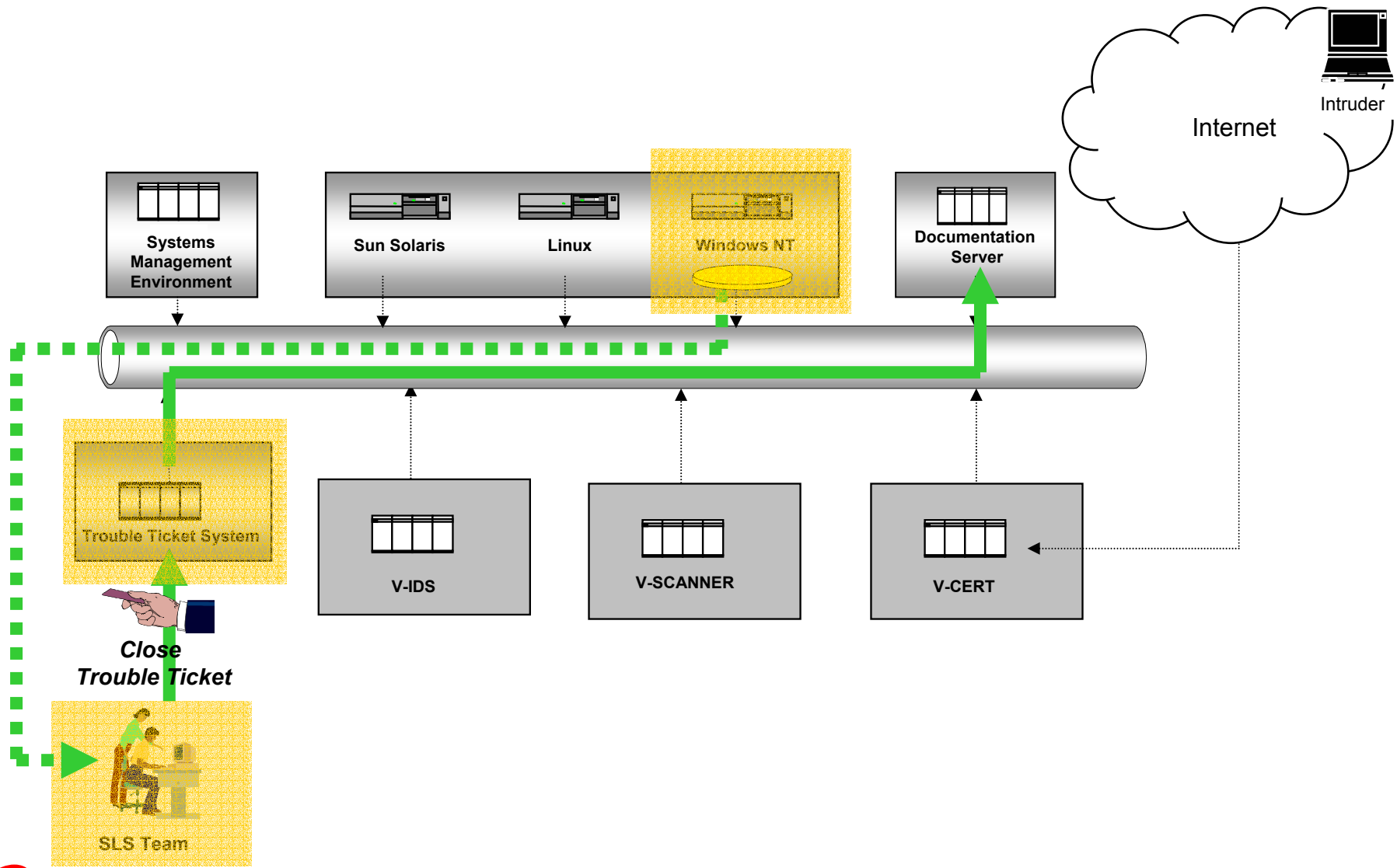
# Scenario 3: V-IDS



# Scenario 3: V-IDS



# Scenario 3: V-IDS



# Concept

- **Prevention**
  - Definition of “Security Profiles” and hardening measures
  - Control of the configuration of system components, comparison with the Security Profiles
  - Testing systems if they are exposed to the vulnerability
- **Warning**
  - Informing teams about vulnerabilities and incidents
- **Detection**
  - Detection of attacks
  - Detection of critical changes to the configuration or to critical files
- **Correction**
  - Controlling the corrective actions

# Principle

**The Security Monitor**

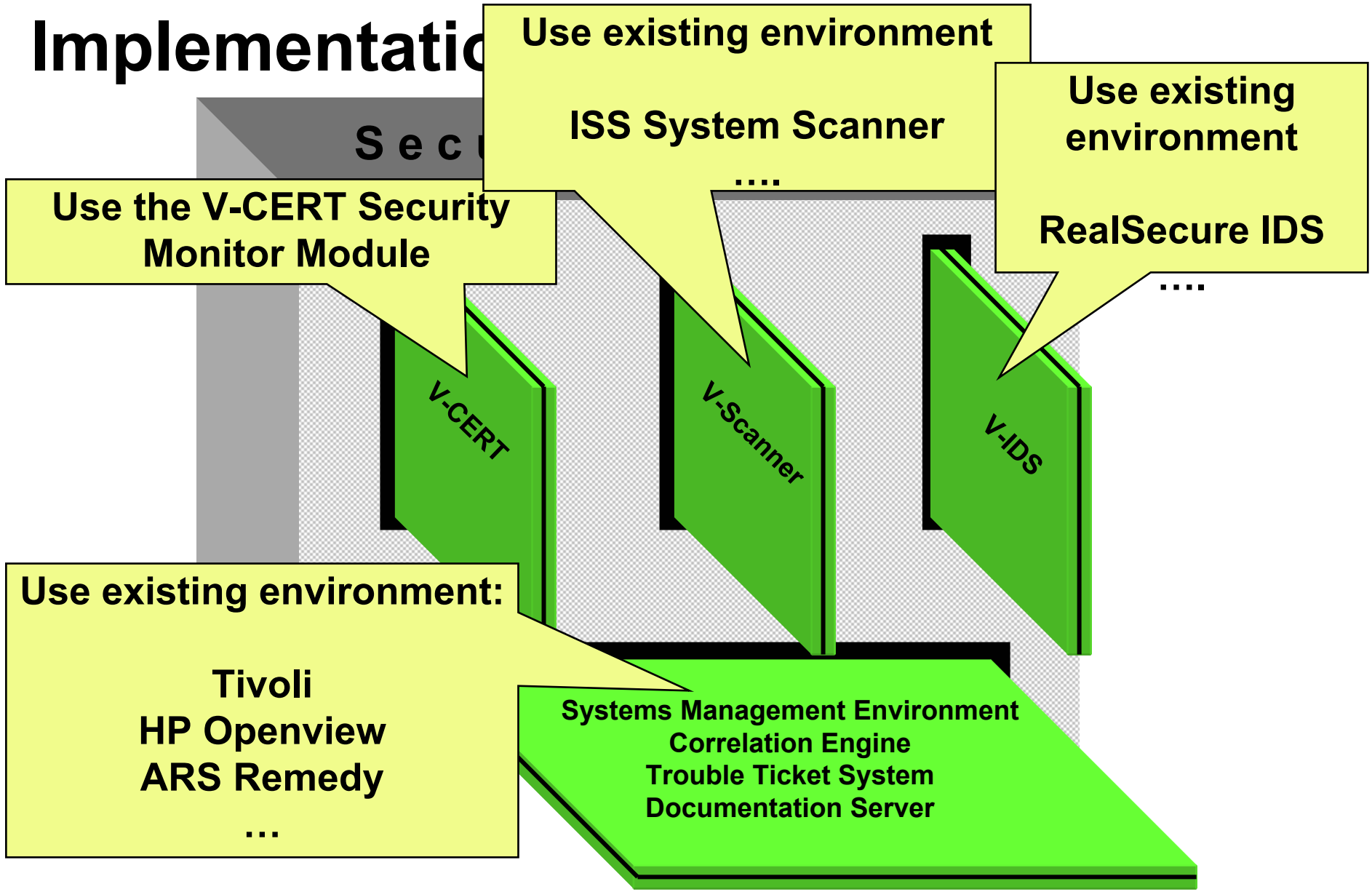
**is a**

**Concept**

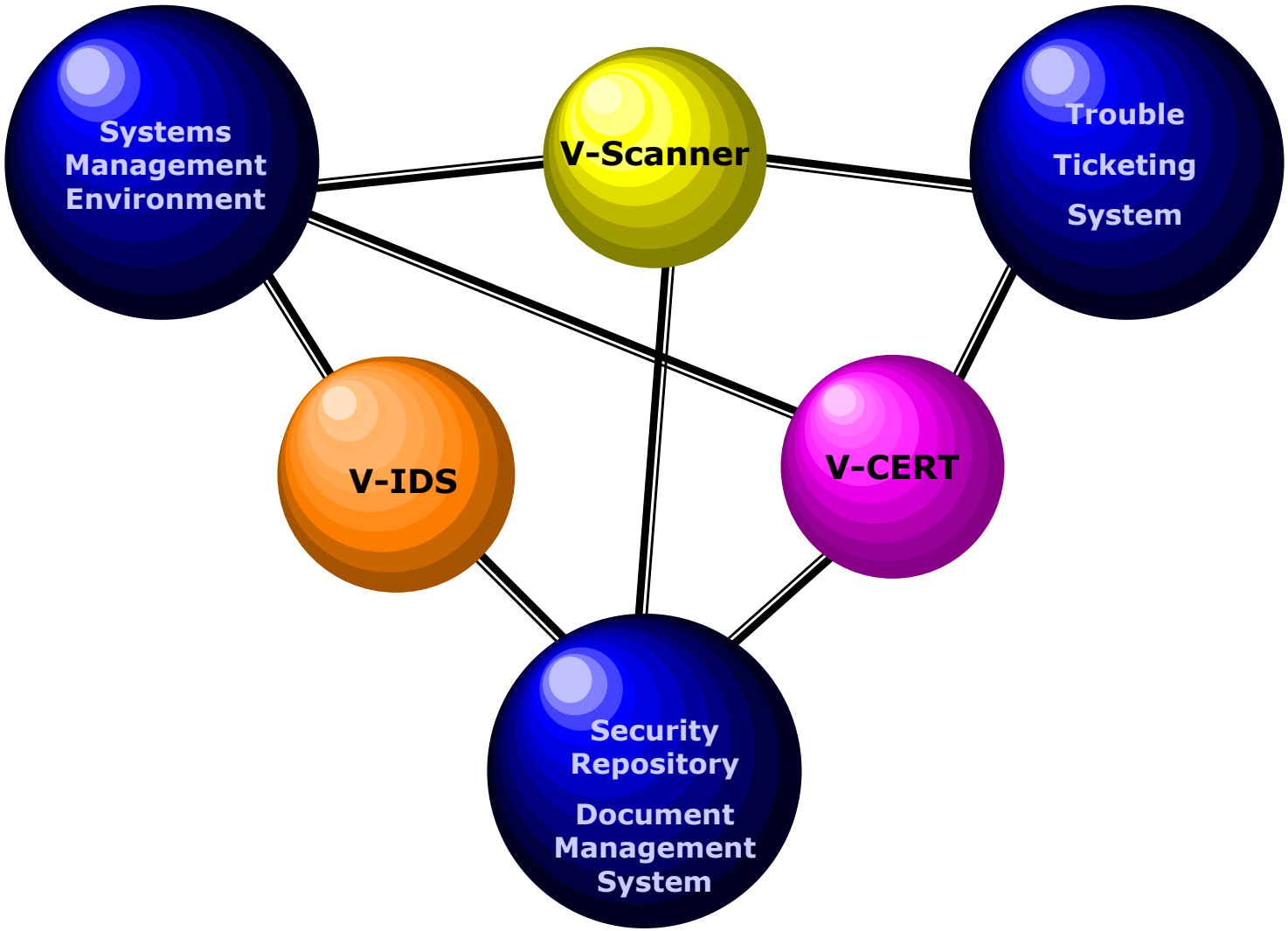
**not**

**a Product**

# Implementatio



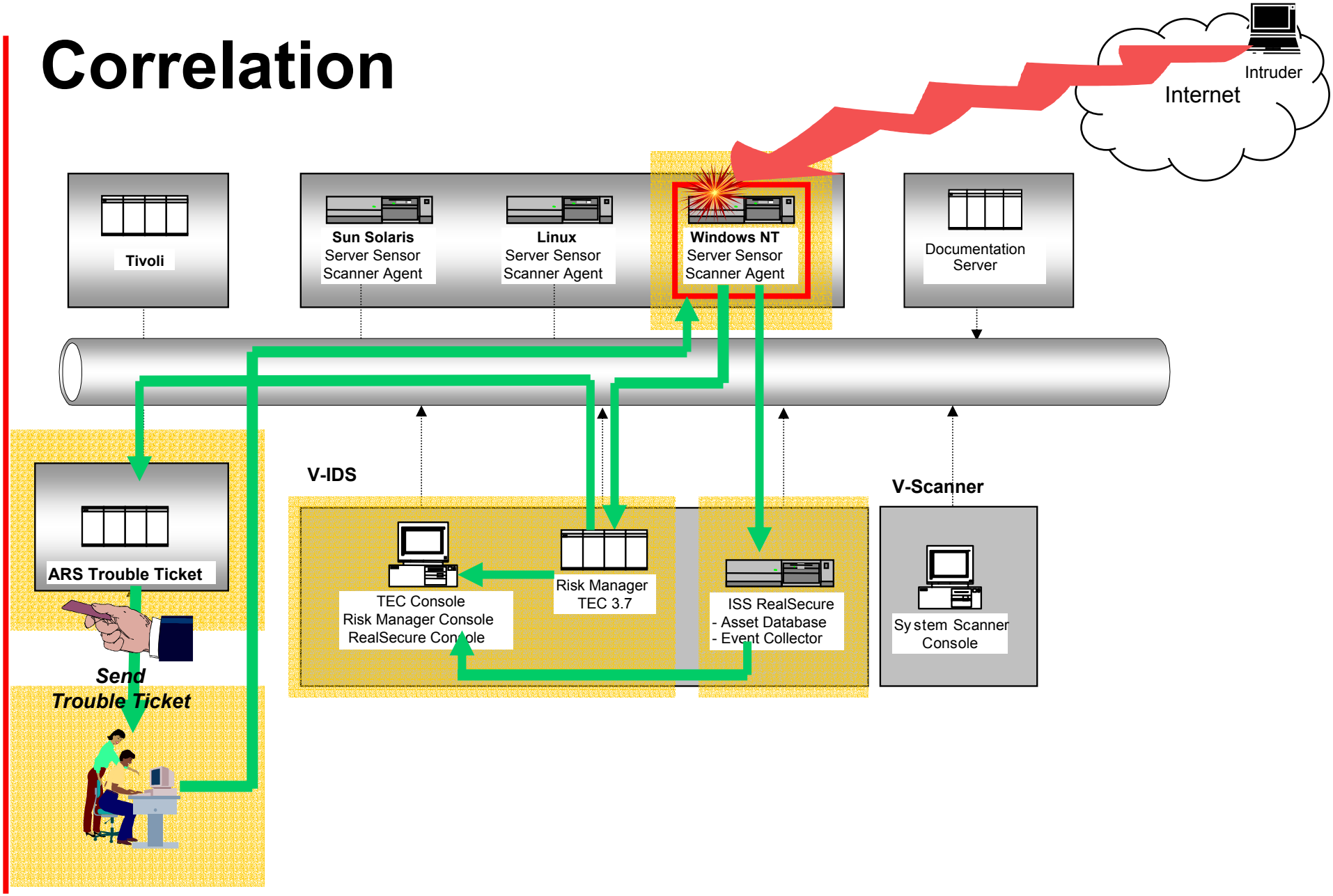
# Integration



# Correlation

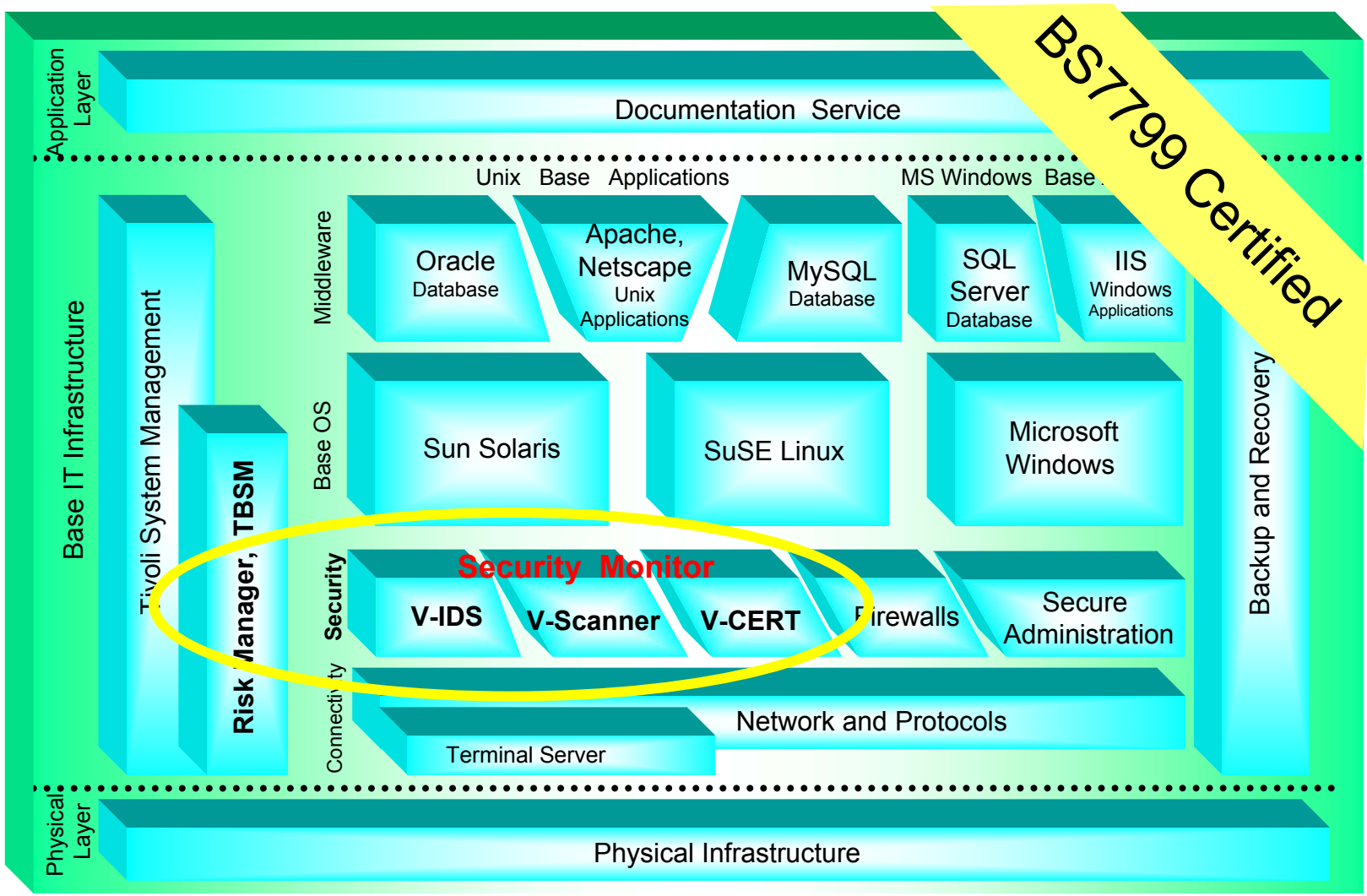
- Events can be prioritized
- Using Tivoli Risk Manager allows to correlate events
- Depending on the severity of the results of the correlation, trouble tickets are generated
- Rule base is customisable
- Integration and Configuration efforts are required to get a sound rule base and a working correlation

# Correlation



# Reference

vodafone information Systems



# V-CERT – Possibilities and Limitations

- **Possibilities**
  - Timely, automatic analysis saves time and adds security
  - Integration with other Security Monitor components
  - Tracking (trouble ticketing, archiving, reporting)

- **Limitations**
  - Not all input sources can be queried (missing patterns)
  - Automated countermeasures are not advised, administrators have to read, think and act

# V-Scanner – Possibilities and Limitations

- **Possibilities**
  - Automatic configuration checks save time and add security
  - Integration with other Security Monitor components
  - Correlation with V-CERT advisories
  - Tracking (trouble ticketing, archiving)

- **Limitations**
  - The checks are only as good as the configuration profiles
  - Overhead for heterogenous or fast changing environment
  - Automated countermeasures are not possible or desired, administrators have to check the finding, think and act

# V-IDS – Possibilities and Limitations

- **Possibilities**
  - Correlation and selection makes IDS events manageable
  - Integration and correlation with other Security Monitor components and systems management environment
  - Tracking (trouble ticketing, archiving, reporting)
- **Limitations**
  - The IDS only identifies known attacks, new attacks may go unnoticed
  - Residual risk of a critical attack missed by rating mechanism (correlation and selection of events)
  - Automated countermeasures are seldom possible or desired, administrators have to look, think and act

# Overall Possibilities and Limitations

- **Possibilities**
  - Added security by automated tasks („noone forgets“)
  - Offloads administrators of repeated tasks
  - Integration and correlation of tools add some „intelligent behaviour“
  - Integration with systems management environment makes security „part of everyday administration“
  - Chance to track and measure
- **Limitations**
  - The configuration still has to be done manually (mostly)
  - Tool logic is not fault-tolerant, it may miss things
  - Tools are far from intelligent, not everything is possible

# Conclusion

- Automating security management as much as possible helps a lot
- Integration with systems management environment is a good approach
- Not all tasks can be automated, sometimes people have to think what to do

→ ***Tools can help but never replace an intelligent, trained administrator!***

→ ***Tools can give the admin more time to be intelligent and trained!***

# Questions?