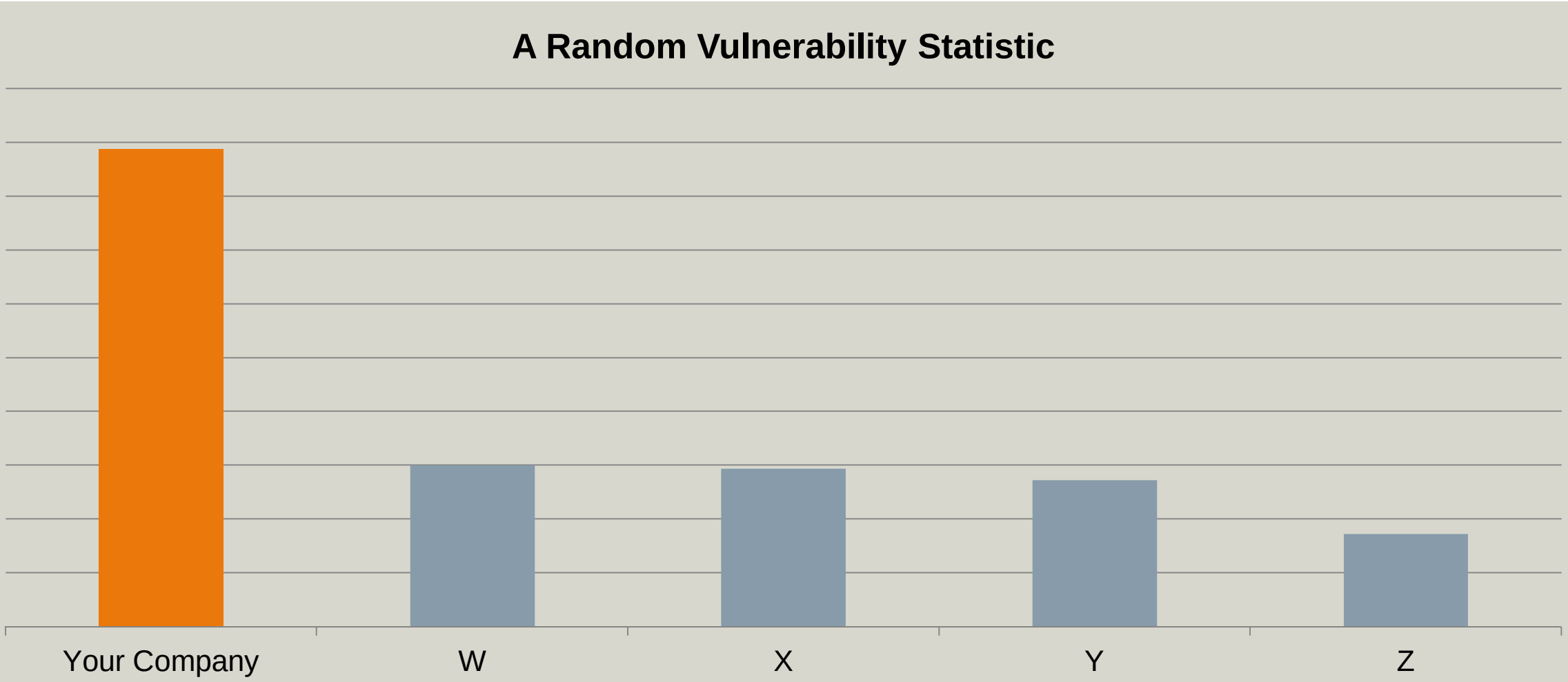
SIEMENS
Ingenuity for life

Which Kind of SDL Insight Provide Vulnerability Statistics?

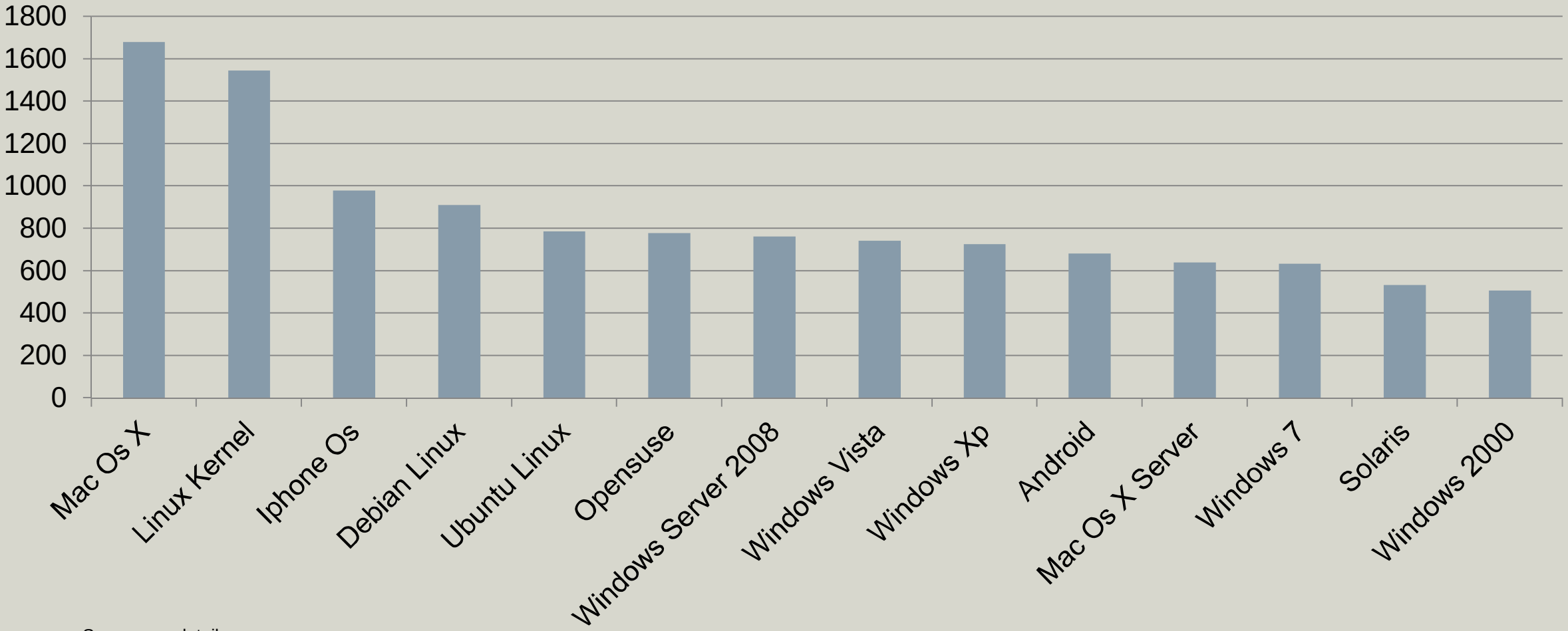
Siemens ProductCERT
Rupert Wimmer, 2017-03-02

Motivation



State of the Art: Common Aproaches and Their Shortcomings

Here: Total number of vulnerabilities in some Operating Systems

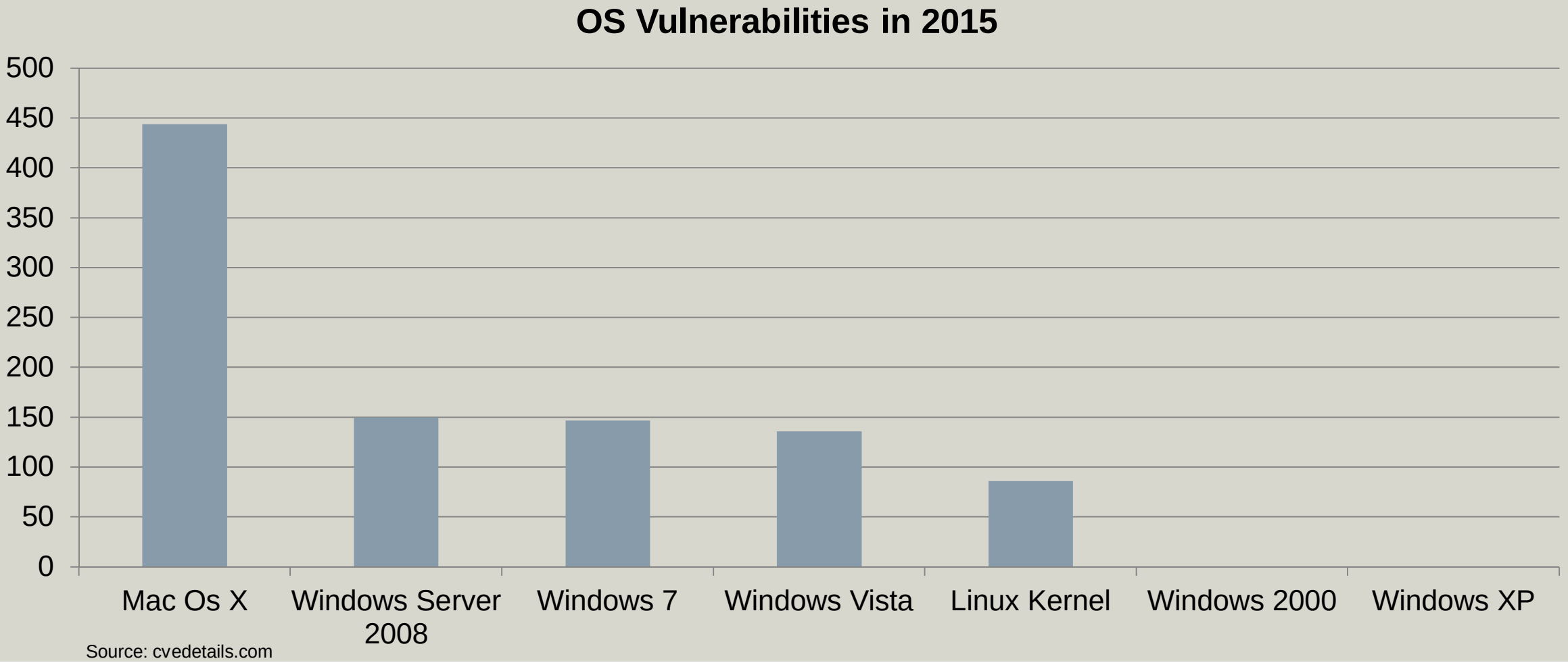


Source: cvedetails.com

State of the Art: Common Aproaches and Their Shortcomings

Here: Only Newest Vulnerabilities are Relevant

SIEMENS

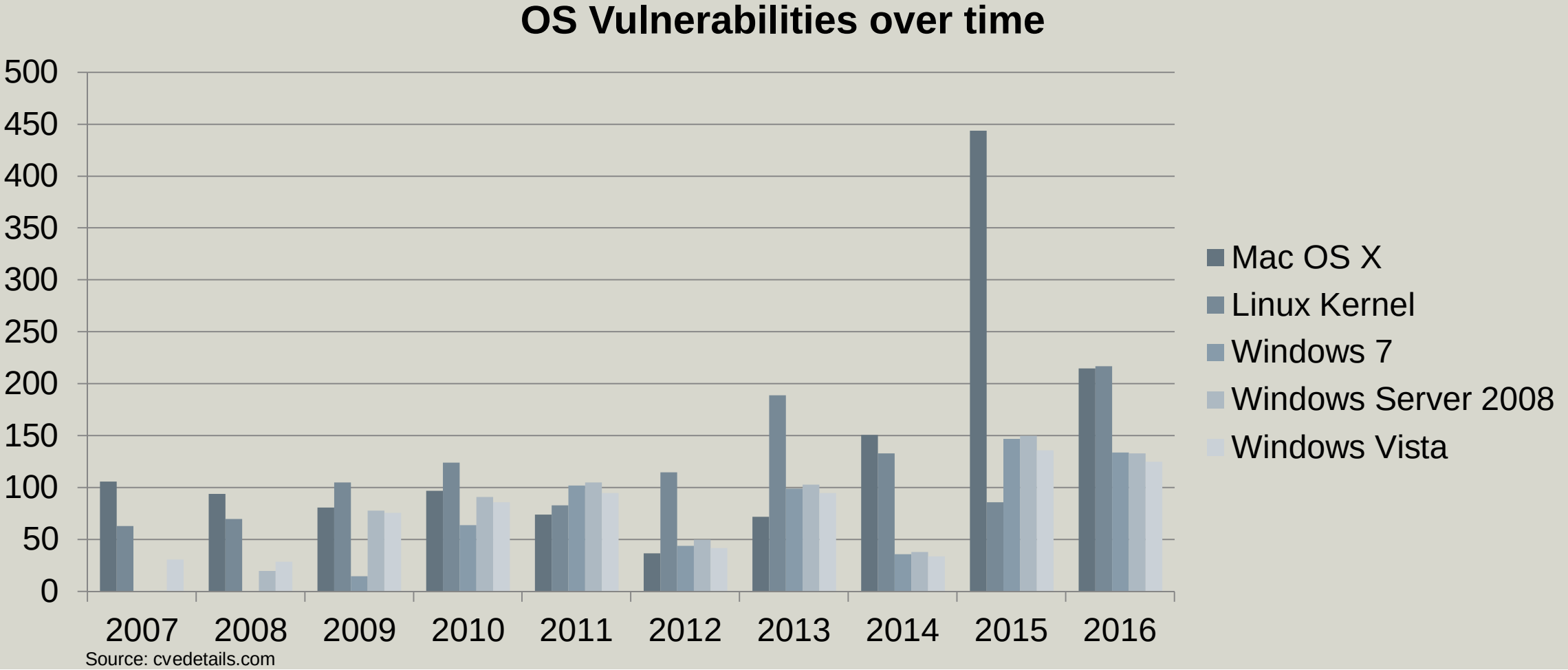


Source: cvedetails.com

State of the Art: Common Aproaches and Their Shortcomings

Here: Development Over Time and Over Different Products

SIEMENS



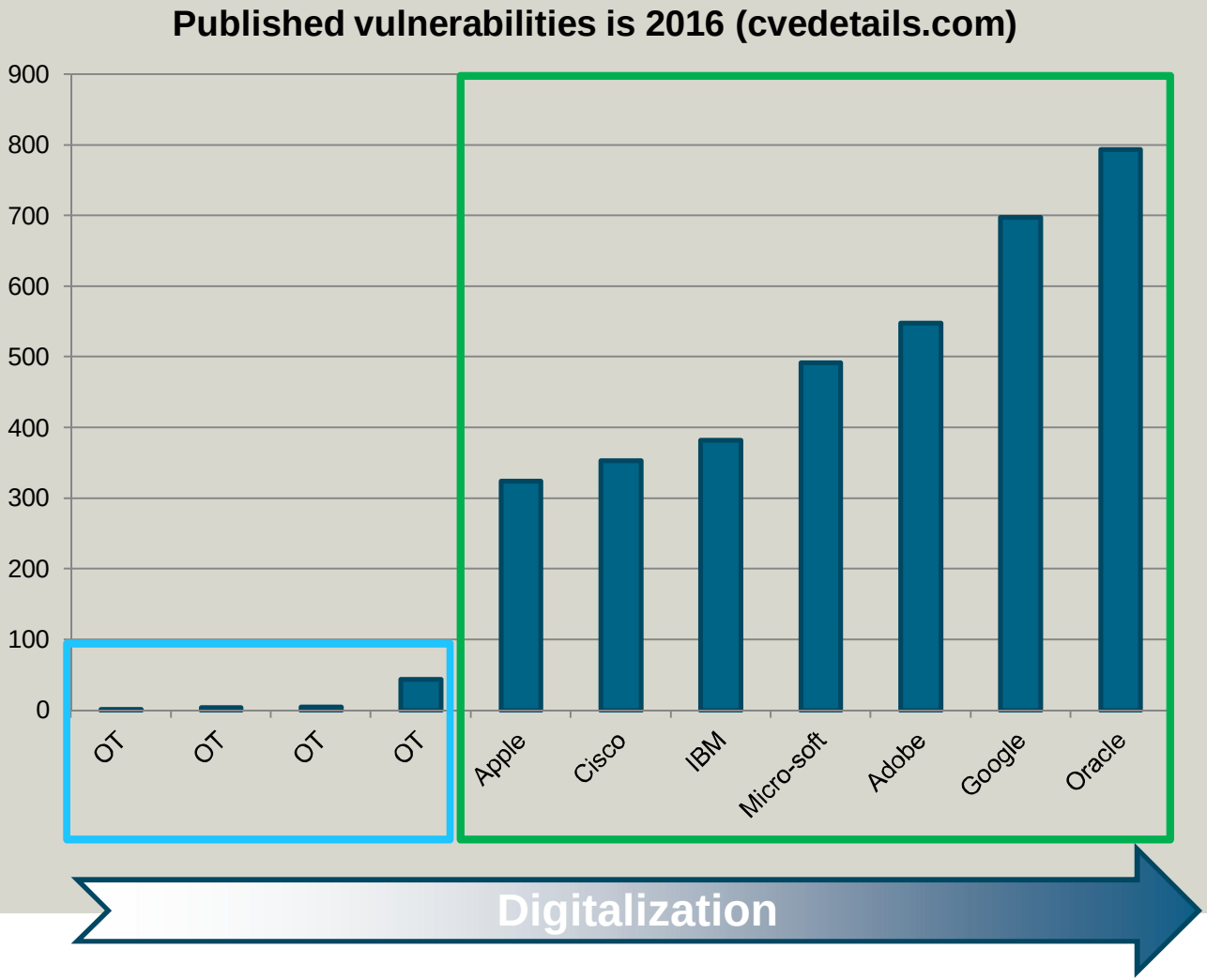
Source: cvedetails.com

Which Kind of SDL Insight Provide Vulnerability Statistics?

Proper Vulnerability Handling Becomes an Important Part of Digitalization

SIEMENS

- Advisories build trust through the consistent, transparent handling of issues
- Digitalization will shift vulnerability handling paradigms of industrial vendors towards the strategy of leading software vendors such as Microsoft, Apple, Oracle…



The Bigger Picture: Further Aspects Providing Insight in SDL
Microsoft‘s recommended Sofware Lifecycle

SIEMENS

Vulnerability handling capabilities are only one factor of secure software lifecycle:

1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

Source: https://www.microsoft.com/en-us/SDL/process/response.aspx

Further KPIs for Estimating Security Maturity

SIEMENS

2. Establish Security Requirements

Security requirements include setup and deployment requirements

- Are these mentioned in manuals?

4. Perform Security and Privacy Risk Assessments

Remaining risks have to be communicated to customers

- Are these mentioned in manuals?

8. Use Approved Tools

Security Tool Vendors like to present their cooperations

- Any indication of cooperation with security tool vendors?

16. Certify Release and Archive

Certifications of security ensure a certain level of security

- Any security certifications for this product?

Conclusion

SIEMENS

- Interpretation of vulnerability statistics is tricky.
- Vulnerability Statistics can provide *some* SDL insight.
- Siemens ProductCERT will continue with the transparent vulnerability handling approach.
- For risk and security evaluation, customers will require and request KPIs.
- Siemens ProductCERT encourages to provide and advertise KPIs for SDL insight.

Siemens ProductCERT
Contact and Information

Rupert Wimmer
Siemens ProductCERT
Otto-Hahn-Ring 6
81739 Munich
Germany

Internet
https://siemens.com/cert

E-Mail
productcert@siemens.com

PGP Key Fingerprint:
1C36 704D 88D7 0A12 00B3 1A56 6E75 3C94 F2EB CF9C