SIEMENS

Dr. Markus Preidel

Product Security for Medical Device Software

MEDCONF 2014, MÜNCHEN

What is Product Security?

Safety

- Protection against consequences of random failure, damage & accidents that happen unintenionally.

Security

- Protection against the consequences of planned, deliberate incidents (attacks)

Product Security of Medical Devices:

Protection of medical devices and software products against the consequences of planned, intentional incidents (attacks)

SIEMENS

Background

Product Security for Medical Devices – Why?

Because we have ignored Security for too long!

Industry Myths:

- Our customers are trustworthy
- Our machines are only used in closed laboratories
- Our products are not connected to the Internet
- There are no regulatory requirements for product security
- There are no problems in the field
- Customers do not demand security
- It is too expensive

That is not true any more!

We have to address Product Security for Medical Devices Now!

Medical devices: In the Crosshairs

After Stuxnet, hackers and researchers targeted Industrial Control Systems

Recently, security researchers started investigating vulnerabilities in medical devices.

The eye is turning in our direction.

“Siemens, Philips, Honeywell, and GE … medical device security problems [are similar to those] seen firsthand with ICS [industrial control] products

‘They don't change their habits. The mentality we see and the attitudes are exactly the same’ when it comes to security.”

Sources, darkreading.com January 17, 2013
Billy Rios, Terry McCorkle (Cylance)
http://www.digitalbond.com/blog/2013/02/15/s4x13-video-security-of-medical-devices/

Security Expert Coverage

It's Insanely Easy to Hack Hospital Equipment

BY KIM ZETTER 04.25.14 | 6:30 AM | PERMALINK

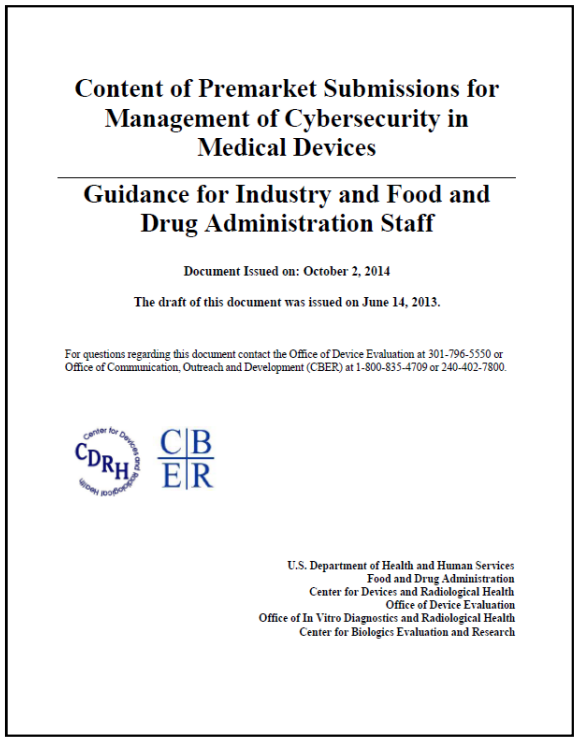
When Scott Erven was given free rein to roam through all of the medical equipment used at a large chain of Midwest health care facilities, he knew he would find security problems–but he wasn't prepared for just how bad it would be.

In a study spanning two years, Erven and his team found drug infusion pumps–for delivering morphine drips, chemotherapy and antibiotics–that can be remotely manipulated to change the dosage doled out to patients; Bluetooth-enabled defibrillators that can be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring; X-rays that can be accessed by outsiders lurking on a hospital's network; temperature settings on refrigerators storing blood and drugs that can be reset, causing spoilage; and digital medical records that can be altered to cause physicians to misdiagnose, prescribe the wrong drugs or administer unwarranted care.

Erven's team also found that, in some cases, they could blue-screen devices and restart or reboot them to wipe out the configuration settings, allowing an attacker to take critical equipment down during emergencies or crash all of the testing equipment in a lab and reset the configuration to factory settings.

Source: Wired, 2014-04-25

Justification – Regulatory Authorities



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

Government

- FDA: Cybersecurity Guidance (Oct 02, 2014)
- Cybersecurity Framework for Critical Infrastructure
- DIACAP for US DoD, expanding to other government sectors

Standards and Regulations

- HIPAA/HITECH, European privacy and data protection laws
- CLSI AUTO11 standard for IT Security of IVD

Justification - Necessity

Customer Demand

- Required for certain market segments
  - Government
  - US Department of Defense
- Increasing IT sophistication in our customers
  - Strong interest sparked by Windows XP phaseout
  - Customers are increasingly demanding Security Features (Regulatory and internal compliance burden for customers)

Quality

- Threat of accidental exposure or theft of Protected Health Information (PHI)
- Potential to compromise the integrity or availability of medical devices
- Serviceability – the daily cost of compromised systems in the field

Justification – Competitive Advantage

Competitive Advantage

If we do it right

- Focusing on the most important aspects of security through prioritization and a well defined roadmap

If we do it well

- Quality through building security into our products
- Incorporating security in our processes

If we do it soon

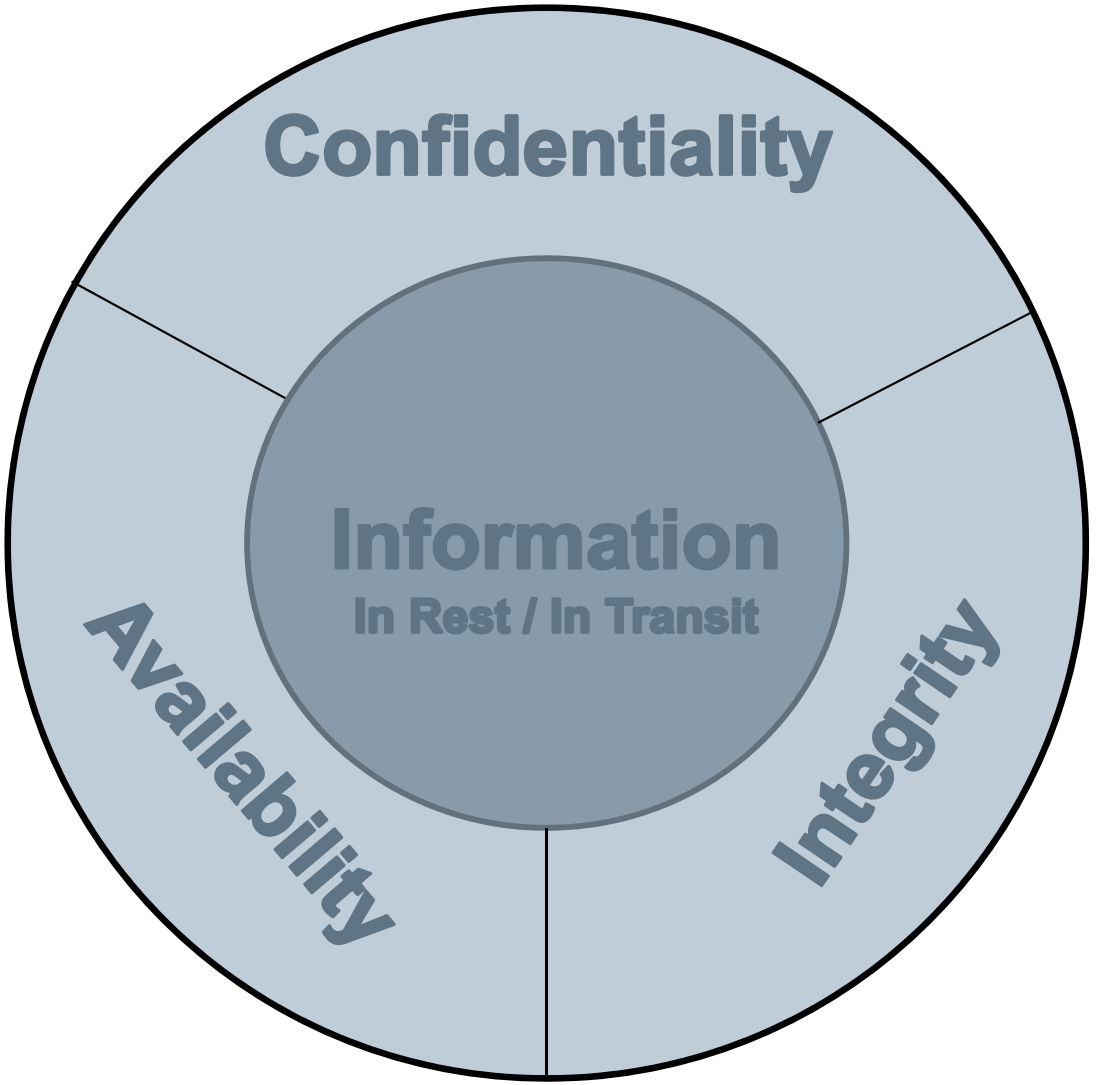
- Time is of the essence

Product Security can become a competitive advantage

SIEMENS

Threat Landscape

Risk categories: CIA



Potential Attackers

Curious Hacker

Skilled Hacker

Governments

User

Administrator

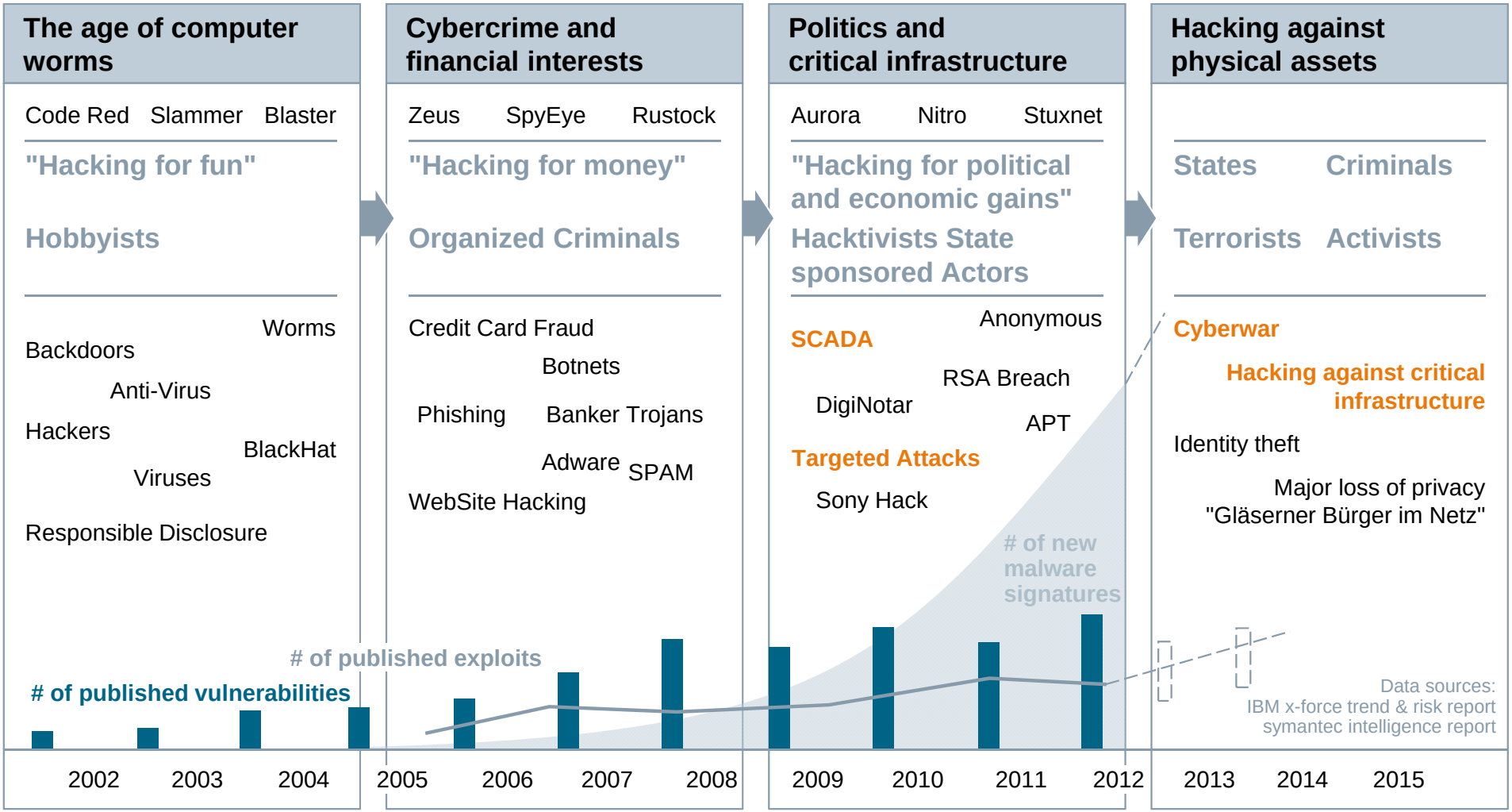
Company Insider

Competitor

Threat level rises - attackers targeting critical infrastructures

SIEMENS

Evolution of attacker motives, vulnerabilities and exploits



Heartbleed: Vulnerability in encryption software makes confidential data open to attackers

SIEMENS

Security issue example: Heartbleed

What is Heartbleed?

- The Heartbleed Bug is a **serious vulnerability** in the popular OpenSSL **encryption software** disclosed in April 2014
- It allows attackers to **steal information** usually protected by the encryption
- SSL/TLS encryption provides communication security and privacy for online applications such as **web, email, instant messaging** (IM) and some virtual private networks (VPNs)

Source: http://heartbleed.com

What is the risk?

- Anyone on the Internet can read the memory of the systems protected by encryption software, e.g. **user names and passwords**, instant messages, emails and **business critical documents** and communication
- This allows attackers to eavesdrop on communications, **steal data** directly from the services and users and to **impersonate services and users**

Bash Shellshock: Vulnerability in Bash Shell allows Remote Atteckers to execute code

SIEMENS

Security issue example: Bash / Shellshock

What is Shellshock?

- The Shellshock Bug is a **serious vulnerability** in the **Bash shell software** used on many Linux-based or Unix-like systems, disclosed in September 2014
- It allows attackers to **execute code** remotely when a web server or similar service is used in a product in combination with the bash shell

What is the risk?

- Anyone on the Internet can **insert and execute code** on servers
- This allows attackers run malicious code on the server, possibly **spread malware, steal data** or **manipulate the server's function**
- The bug is also included in the **firmware** of multiple Linux based devices that are very hard or impossible to patch (routers, repeaters….)

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

Consequences can be far-reaching

Typical consequences of product and solution security issues

Safety (e.g. hacking of medical devices resulting in loss of life)

Degradation or disruption of customer business (degree of inconvenience, duration, cost of restoration)

Breaches of legal and regulatory requirements (e.g. privacy laws)

Breaches of contractual requirements

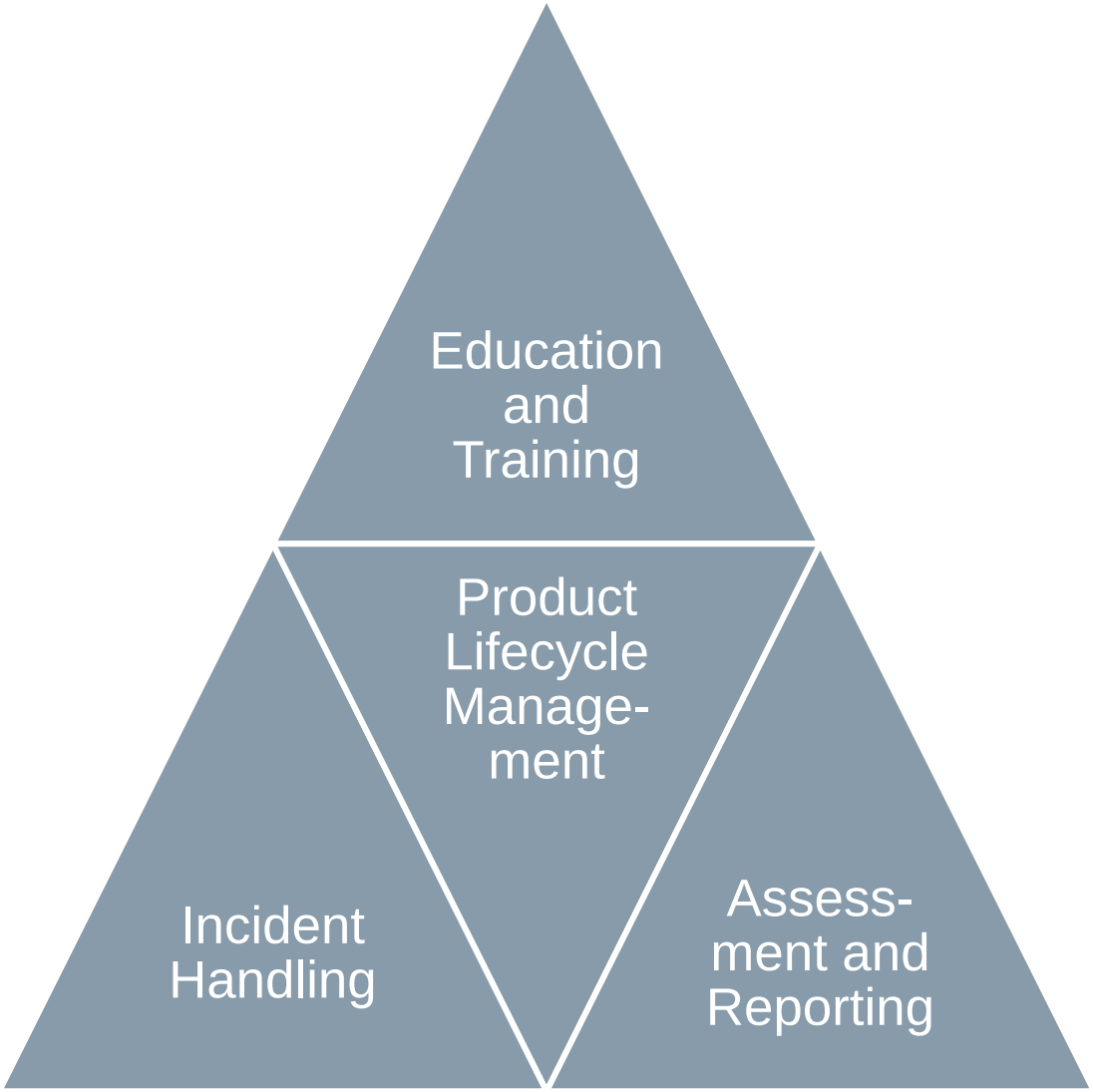
Loss of intellectual property or license fraud

Loss of reputation, customers or market share

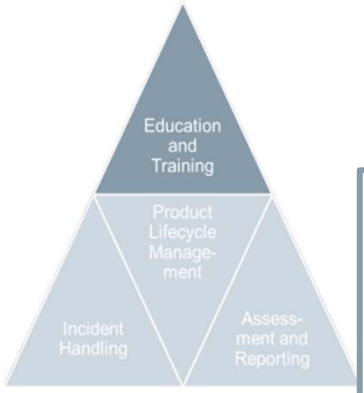
SIEMENS

Addressing the Need

Product Security activities



Product Security activities



Education and Training

Awareness

- Organization-wide
- All functions involved in product development and product health

Functional Training

- R&D – Secure coding practices
- Service – Incidents and technical
- Core Team
- Element Teams

Product Security Processes

- PDP
- Product Health
- Incident & Vulnerability Handling
- Escalation

Certifications

- Product & Solutions Security Expert
- Certified Information Systems Security Professional [CISSP]

Product Security activities

Vulnerability Assessment and Reporting

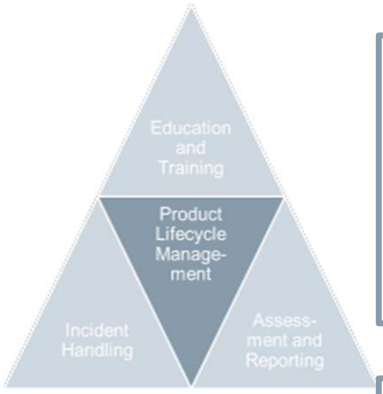
- “State Of The Nation” current snapshot of the security risk level for each relevant product line.
- Security Risk Assessment will guide development teams to reduce the security risks to an acceptable residual risk level
- Periodic scanning (assessment) to accommodate new software and new vulnerabilities
- Proactive monitoring of newly discovered vulnerabilities Corrective measures for affected products
- Regular reports showing quantitative measure of the product security risks at a given time

Product Security activities

Incident Handling

- Establish classification of security events and incidents
- Report product security incidents regularly
- Institutionalized escalation process
- Common incident handling database
- Established incident handling procedure & team

Product Lifecycle Management: requirements



Three types of requirements

Process

- Integrating with existing process and deliverables
- Examples: Product Security Management Plan, Incident Handling Process

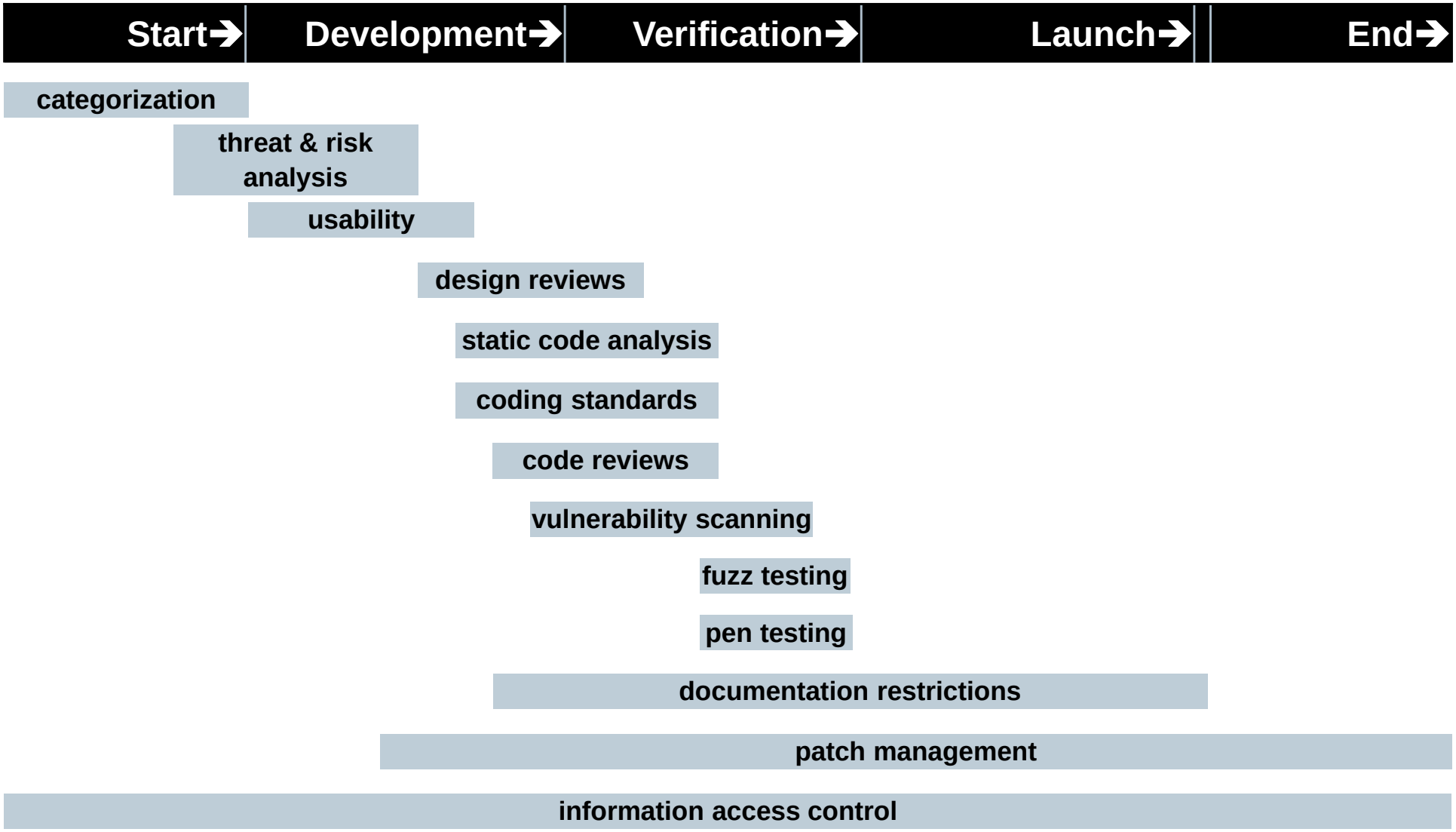
Development

- Master Requirements
- Techniques and activities required to develop software securely
- Examples:
  Secure Coding, Tools, Secure Code Repositories, Security Testing

Product

- Standard functions as defined in the Master Requirements
- Product functionality tailored to the characteristics of each product
- Examples:
  User Authentication, Malware Protection, Encryption, Hardening

Project Activities



SIEMENS

Responsibilities by Function

Supply Chain Mgmt.	Product Management	Product Security Office	Software Engineering
Secure supplier selection	Includes security in DIR Review new requirements Task force participation	·Master requirements ·Guidelines & standards ·Testing toolkit ·Risk tools ·Product dashboard ·Source testers ·Guidance documents	Review new requirements Task force participation Lead risk assessments Analyze/tailor requirements New development activities Manage SVM* Security testing Security Management Plan Security architecture Review secure suppliers Evaluate usability Project PSS classification Project security champion Project security lead
Communications			
Task force participation			
Quality Management	**Program Management**		
Task force participation	Assess project impact Review deliverables		
Legal		**Product Security Officer**	
Task force participation	**Service & Support**		
Change Review Board	Review new requirements Commercial readiness Patch distribution Incident monitoring Task force participation	·Review exceptions ·Source reviewers ·Task force participation ·Verify SVM registration	
Handle change requests			
Product Steering Board			
·Approve exceptions			

*Software Vulnerability Monitoring

SIEMENS

Master Requirements

Operation:

- Backup & restore
- Patching of operating system and software

Protection:

- Prevent execution of unknown software & detection of malware
- Integrity of software & configuration data protected (e.g. signing)
- Expose only minimum ports, addresses and services
- Minimum privileges for software execution
- Operating system hardening
- Outside (remote) access protected & authorized by local user
- No backdoors, hard coded passwords, development users

Master Requirements

User Management:

- Access only by authorized, named users with defined roles
- Password rules (length, complexity, change, expiration intervals…)

Logging:

- Security relevant activities are logged
- Logfiles are protected
- Audit trail

Information Protection:

- Protected Health Information – encrypted in rest and in transit, can be fully deleted
- Passwords, configuration data, calibration data encrypted
- Backups encrypted
- Exported data anonymized

SIEMENS

Ongoing Activities

Incident Handling

Security Incident:

Unwanted / unexpected events that compromise operations and threaten information security [ISO 27000:2012]

Incident Handling:

- Process established to detect and to report security incidents
- Incident Handling Task Force exists
  - Receives and assesses incident reports
  - Guides the handling of incidents

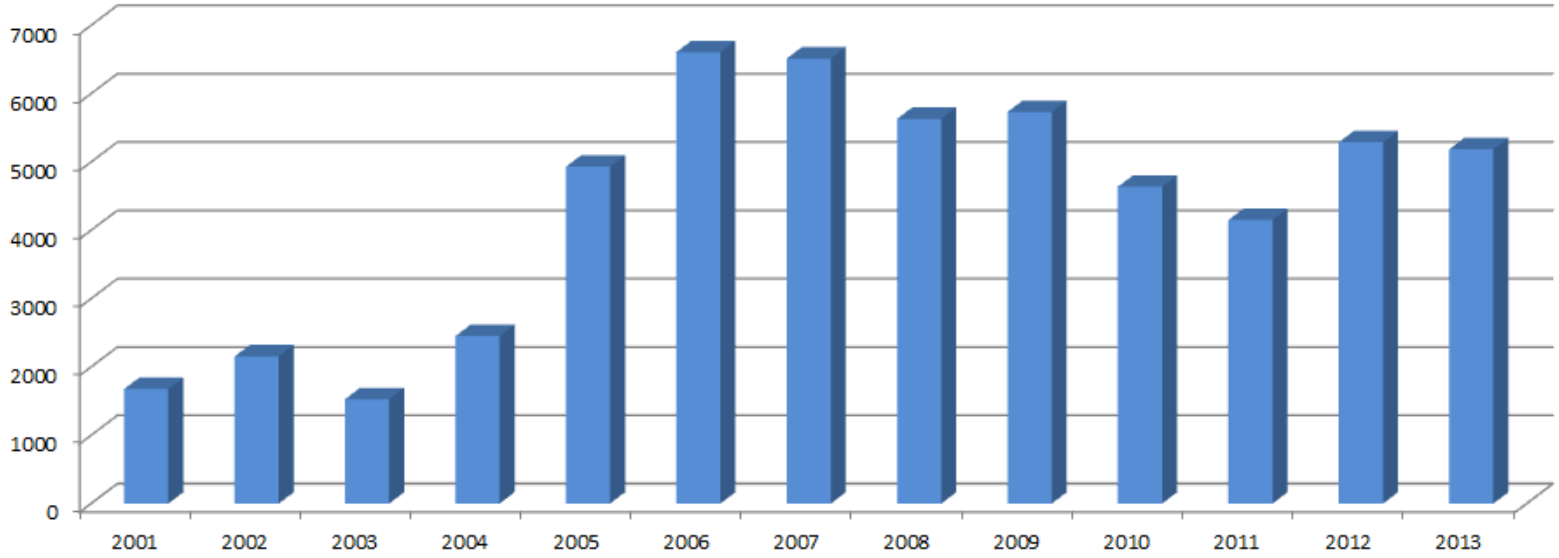
Steps:

- Clarification of incidents
- Information to customers, service, management and public
- Solution of the problem

Security Vulnerability Monitoring

Security Vulnerability:
Weakness of an asset or control that can be exploited [ISO 27000:2012]

- 90% of successful cyber attacks are based on known vulnerabilities for which patches are available!
- Only 2% of all equipment is completely patched
- Information about vulnerabilities is available from a multitude of sources that need to be monitored



Source: http://nvd.nist.gov

Security Vulnerability Monitoring

Vulnerability Monitoring:

- Process established to detect vulnerabilities in existing products
- Permanent team monitors weaknesses in software products

Preparation:

- Determine sources to monitor
- Create list of components to monitor, covering own products
- Prepare regular security scanning

Monitoring:

- Analyse & assess vulnerabilities that affect products (e.g. CVSS* score)
- Identify feasible actions
- Create and distribute patch if required

* http://nvd.nist.gov/cvss.cfm

Sources for Vulnerability Information:

Secunia	http://secunia.com
NIST	http://nvd.nist.gov
US CERT	http://www.us-cert.gov/

Vulnerability scanning software

Nessus	http://www.tenable.com/products/nessus
OpenVAS	http://www.openvas.org
Greenbone	http://www.greenbone.net/

Patch Management

Security Patch:
Software change applied to a product to correct a vulnerability. Usually executable code or parameter files

Patch management:
Process dealing with management and remediation of vulnerabilities in products via software fixes

- Ensure that products can be patched
- Establish infrastructure for secure distribution of patches

- Distributed patches if required by vulnerability management or incident handling within limited time.
  Typical goals: critical patches 30 days / significant product patches 90 days

Dr. Markus Preidel
Director Software Development
Siemens Healthcare Diagnostics Products GmbH

Am Kronberger Hang 3
65824 Schwalbach

Germany

Phone: +49 (6196) 806-415
Fax: +49 (6196) 806-320

E-mail:
markus.preidel@siemens.com

siemens.com/answers

Courses & Certifications

Shortname	Title	Organisation	URL
HCISPP℠	**HealthCare Information Security and Privacy Practitioner**	**(ISC)²®**	https://www.isc2.org/HCISPP/Default.aspx
SSCP®	Systems Security Certified Practionier	(ISC)²®	
CAP®	Certified Authorization Professional	(ISC)²®	
CSSLP®	Certified Secure Software Liefcycle Professional	(ISC)²®	
CISSP®	Certified Information Systems Security Professional	(ISC)²®	
CCFPSM	Certified Cyber Forensics Professional	(ISC)²®	
CISA	Certified Information Systems Auditor	ISACA	
CISM	Certified Information Security Manager Learn more about CISM	ISACA	
CGEIT	Certified in the Governance of Enterprise IT	ISACA	
CRISC	Certified in Risk and Information Systems Control	ISACA	
GSEC	**GIAC Security Essentials**	**SANS**	http://www.giac.org/certification/security-essentials-gsec
GCIH	**GIAC Certified Incident Handler**	**SANS**	http://www.giac.org/certification/certified-incident-handler-gcih
GCIA	GIAC Certified Intrusion Analyst	SANS	
GCFA	**GIAC Certified Forensic Analyst**	**SANS**	http://www.giac.org/certification/certified-forensic-analyst-gcfa
GPEN	**GIAC Penetration Tester**	**SANS**	http://www.giac.org/certification/penetration-tester-gpen
GSLC	GIAC Security Leadership	SANS	
GWAPT	GIAC Web Application Penetration Tester	SANS	
GSNA	GIAC Systems and Network Auditor	SANS	
GPPA	GIAC Certified Perimeter Protection Analyst	SANS	
GREM	GIAC Reverse Engineering Malware	SANS	
GCWN	GIAC Certified Windows Security Administrator	SANS	
GCFE	GIAC Certified Forensic Examiner	SANS	
GISF	GIAC Information Security Fundamentals	SANS	
GISP	GIAC Information Security Professional	SANS	
GAWN	GIAC Assessing and Auditing Wireless Networks	SANS	
GCUX	GIAC Certified UNIX Security Administrator	SANS	
GCED	GIAC Certified Enterprise Defender	SANS	
GSSP-JAVA	**GIAC Secure Software Programmer-Java**	**SANS**	http://www.giac.org/certification/secure-software-programmer-java-gssp-java
GXPN	GIAC Exploit Researcher and Advanced Penetration Tester	SANS	
GWEB	GIAC Certified Web Application Defender	SANS	
GLEG	GIAC Law of Data Security & Investigations	SANS	
GMOB	GIAC Mobile Device Security Analyst	SANS	
GSSP-.NET	**GIAC Secure Software Programmer- .NET**	**SANS**	http://www.giac.org/certification/secure-software-programmer-net-gssp-net
GCPM	GIAC Certified Project Manager	SANS	
GICSP	Global Industrial Cyber Security Professional	SANS	
GCCC	GIAC Critical Controls Certification	SANS	

Example Secure Software Programmer:
.NET Authentication
.NET Authorization
.NET Data Validation
.NET Encryption
.NET Exception handling and logging
.NET Framework Security
.NET Session Management
Common Web and .NET Application Attacks
Secure SDLC

Tool Set

- ISO27002/11/19, Code of practice for information security management; domain-specific profiles 27011 and 27019 (http://www.27000.org/iso-27002.htm)
- HIPAA Security Rule, Health Insurance Portability and Accountability Act (http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule)
- IEC 62443, Security for industrial automation and control systems (http://goo.gl/1dlcxp)
- WIB, WIB report M-2784-X-10. PCS Security Requirements for vendors (http://www.wib.nl/)
- SAMM, Software Assurance Maturity Model (http://goo.gl/xaL76d)
- KALI, Security Toolkit (http://www.kali.org)