SIEMENS

eco, From Detection to Response, Thomas Schreck, 19.02.2015

Incident Response from a Global Enterprise Perspective

Siemens

Customer value chain

Design & engineering	Operations	Maintenance
Productivity & time-to-market	Flexibility & resilience	Availability & efficiency

Digital Factory  Streamlined product to automation design — Vertical software	**Energy Management**  Optimized grid automation integrating renewables — Enhanced E&A	**Wind Power**  Data-driven upgrades, moving to self-learning — Enhanced E&A	**Power & Gas, Power Generation Services**  Analytics-based availability and performance guarantees — Digital services
Process Industries & Drives  Integrated process & plant engineering and operation — Vertical software	**Healthcare**  Image-guided therapy for novel surgery procedures — Vertical software	**Building Technologies**  Data-driven advice for building efficiency — Digital services	**Mobility**  Guaranteed availability via predictive maintenance — Digital services

Corporate Technology - RTC

Software Architecture Development

- Software architecture
- Software test and system qualities
- Development efficiency
- Product lines and SW Ecosystems

HQ [1]: Munich
RGs [2]: 8

IT Platforms

- SW / System integration
- Middleware, cloud
- Enterprise IT

HQ: Munich
RGs: 10

IT Security

- Security architecture & lifecycle
- CERT services
- Embedded security

HQ: Munich
RGs: 8

Business Analytics & Monitoring

- Decision support
- Knowledge discovery
- Condition monitoring

HQ: Munich
RGs: 9

Automation & Control

- Modeling & simulation
- Engineering
- Runtime & optimization
- Solutions

HQ: Princeton, US
RGs: 12

Networks & Communication

- Wireless & industrial networks
- Internet of things

HQ: Munich
RGs: 6

Systems Engineering

- Usability design
- Engineering
- Reliability
- Manufacturing solutions
- Process support

HQ: Munich
RGs: 12

Imaging & Computer Vision

- Image reconstruction and visualization
- Computer vision
- Image processing & video analytics
- Cardiovascular, onco and neuro imaging
- Interventional imaging
- Computational imaging

HQ: Princeton, US
RGs: 13

Materials

- Innovative materials and coatings
- Advanced manufacturing technologies
- Analytics

HQ: Berlin
RGs: 8

Electronics

- Electronic design & processing
- Radio frequency solutions
- Integrated technologies
- Manufacturing technologies

HQ: Munich
RGs: 8

Sensor Tech-nologies

- Sensor devices & system integration
- Inspection & test

HQ: Erlangen
RGs: 8

Power & Energy Technologies

- Power management
- Switching
- Power electronics
- Energy storage
- Electromagnetic systems & mechatronics
- Energy & industrial processes

HQ: Erlangen
RGs: 12

IT security covered by the eight research groups of the technology field

SIEMENS

Technology Field IT-Security – Head: Dr. Rolf Reinema

Corporate CERT Services
Udo Schweigert

Incident handling and technical policies on behalf of CIT

ProductCERT Services
Udo Schweigert

Incident handling and vulnerability monitoring for Siemens products and solutions

CERT Security Assessments
Sven Lehmberg

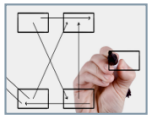
Friendly hacking and assessments of products, solutions, applications and processes

Cyber Security for the Americas
Dr. Martin Otto

- Regional Support for the Americas
- Regional Security topics, e.g., NERC-CIP, HIPAA, DIACAP

Security Lifecycle
Dr. Holger Dreger

Sustainable integration of systematic security activities into product and solution lifecycle processes



Security Architecture
Uwe Blöcher

Domain specific security architectures. Best practice use of COTS and Open Source security

Security for Embedded Systems
Dr. Wolfgang Klasen

Design, integrate, and realize security for embedded systems, customize algorithms and protocols

Add-on IT Security China
Dr. Ming Zhu Li

- Regional Support for China
- Regional Security topics, e.g., Industrial Control Systems Security

SIEMENS

CERTs @ Siemens

CERT

- Security Checklists
- Security Hardening
- Vulnerability Alerting
- Incident Response
- Forensic Analysis
- Threat Monitoring

ProductCERT

- Vulnerability Handling
- Vulnerability Monitoring
- Security Testing
- Threat Alerting

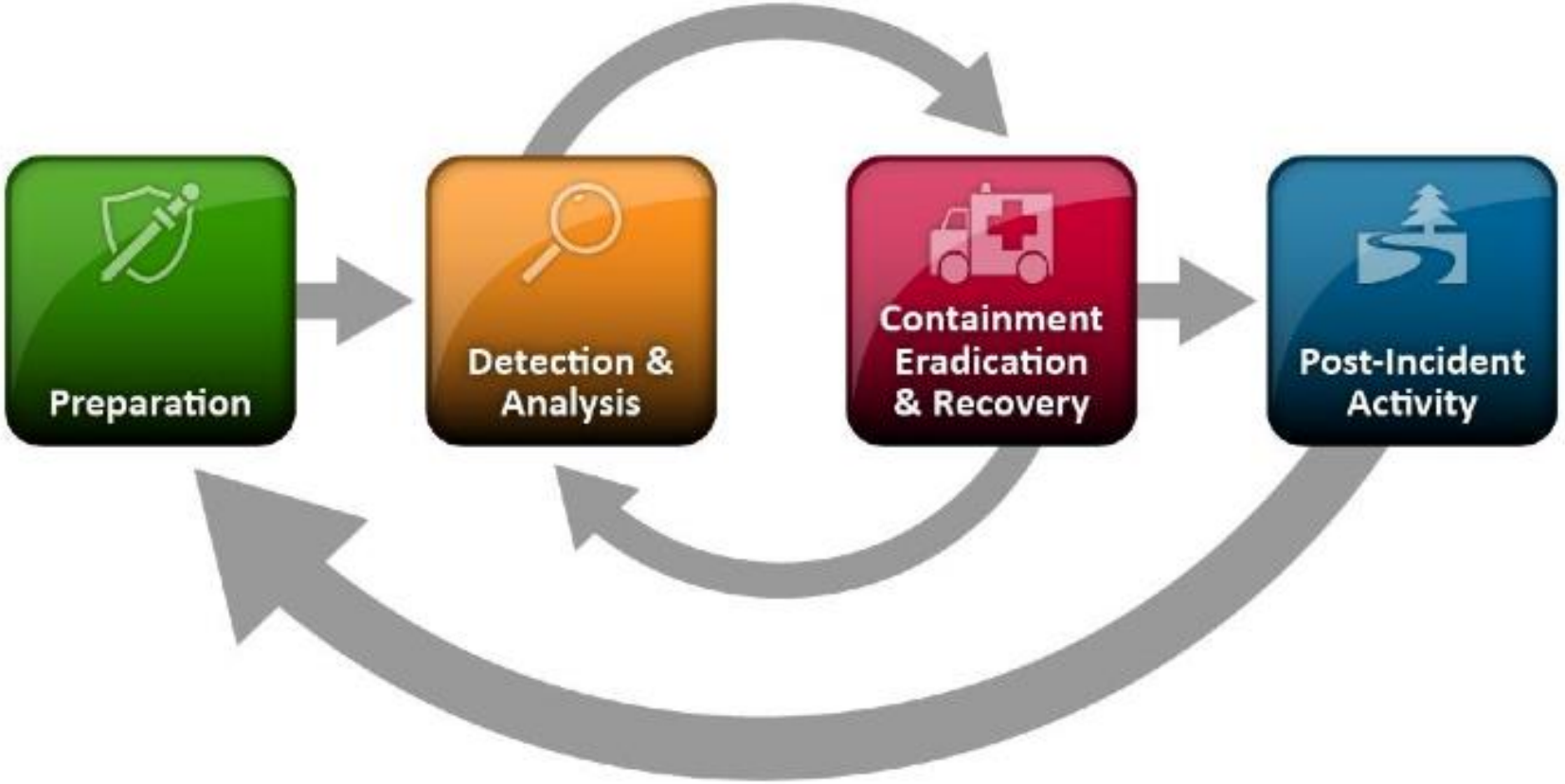
CERT Services

Proactive Services	Reactive Services	Security Quality management services
• Alerts and Warning • Announcements • Configuration and maintenance of security tools, applications, and infrastructure • Press and Media monitoring • etc.	• Incident Handling • Artifact Analysis • Abuse Handling • Threat Intelligence • etc.	• Risk Analysis • Education/training • Product evaluation

Long Term resiliency services

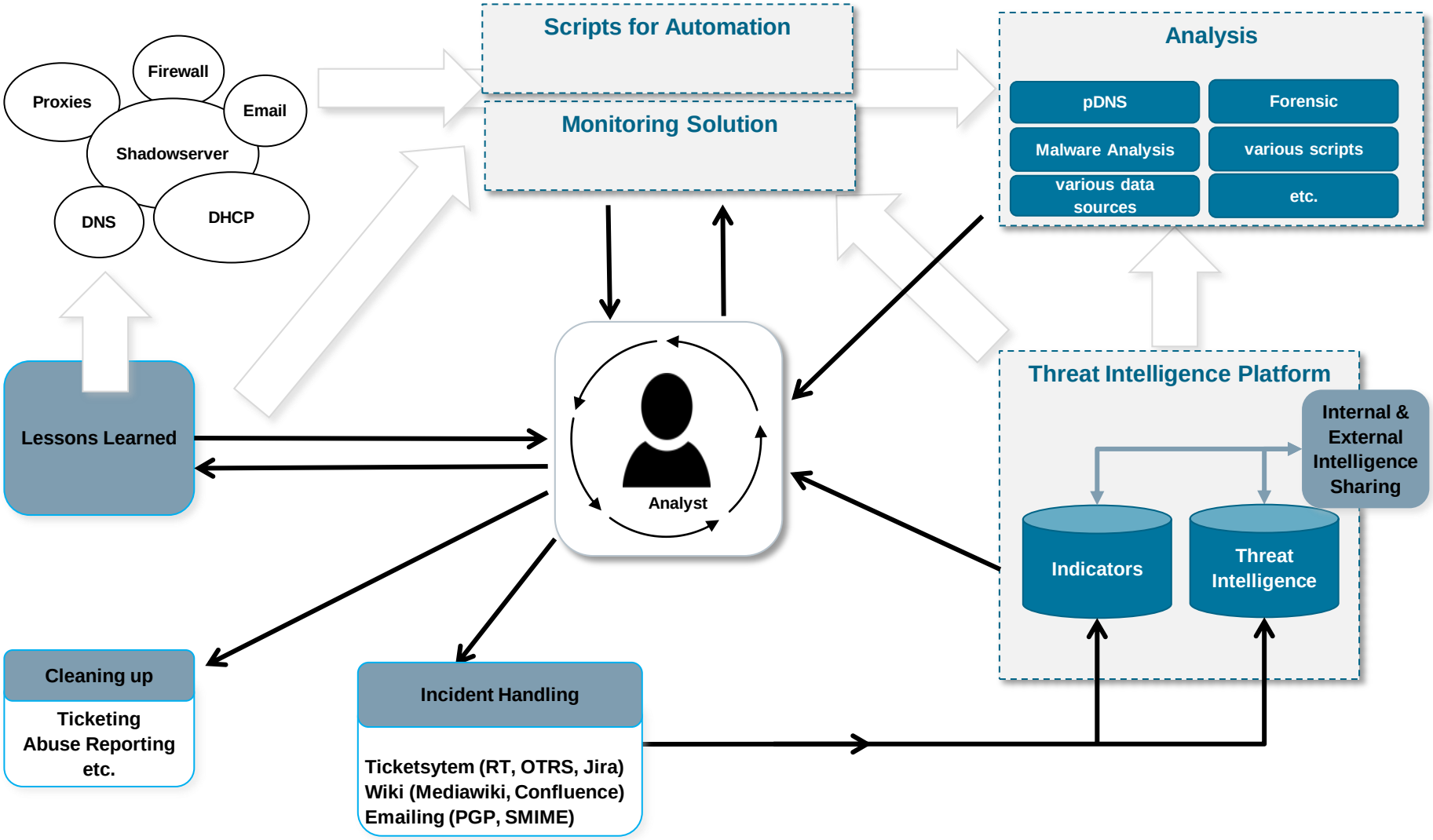
- Knowledge sharing for critical infrastructure
- Research and education
- Point of contact

Incident Response Process

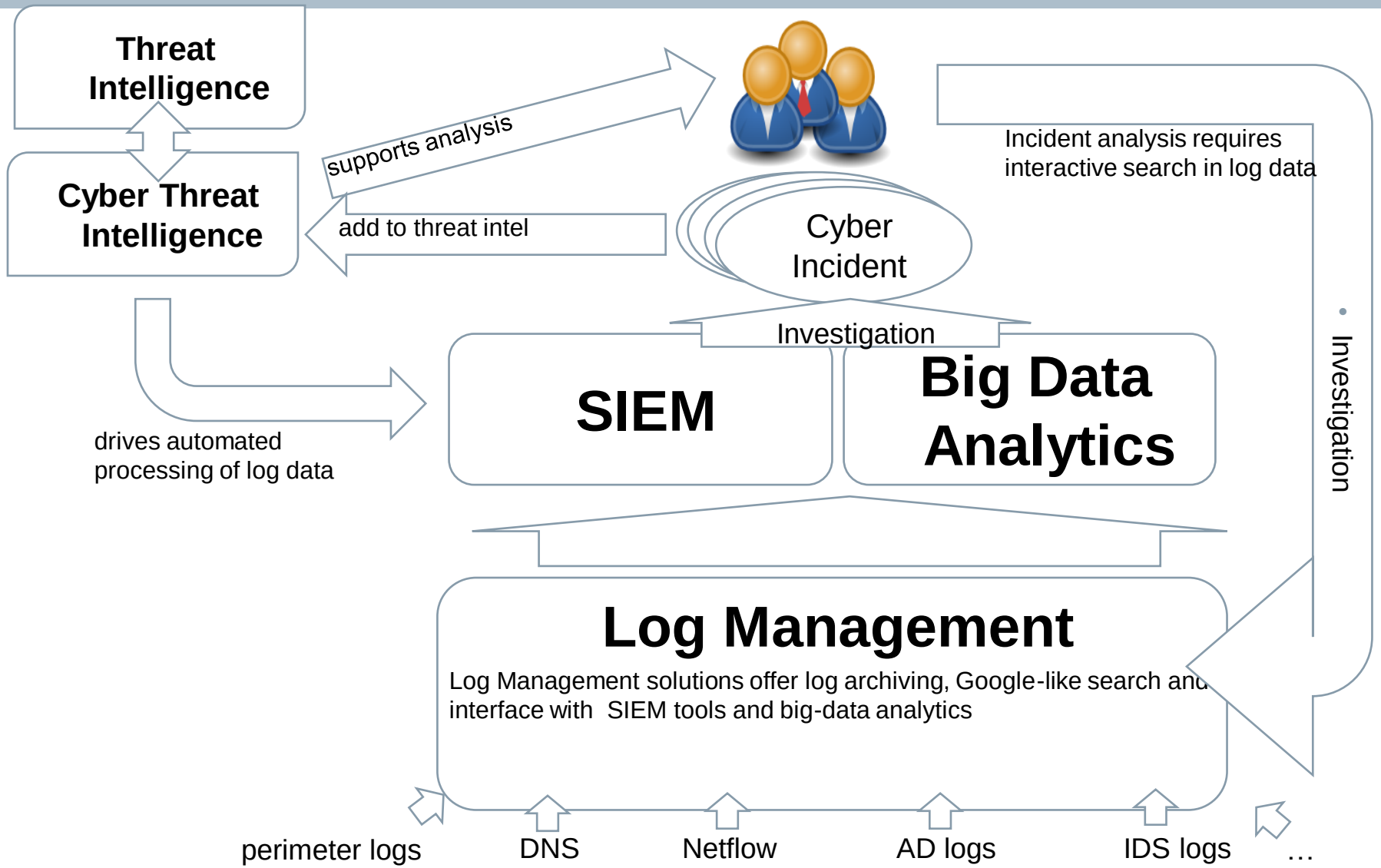


Kill-Chain-Model

Incident Response



Threat Intelligence



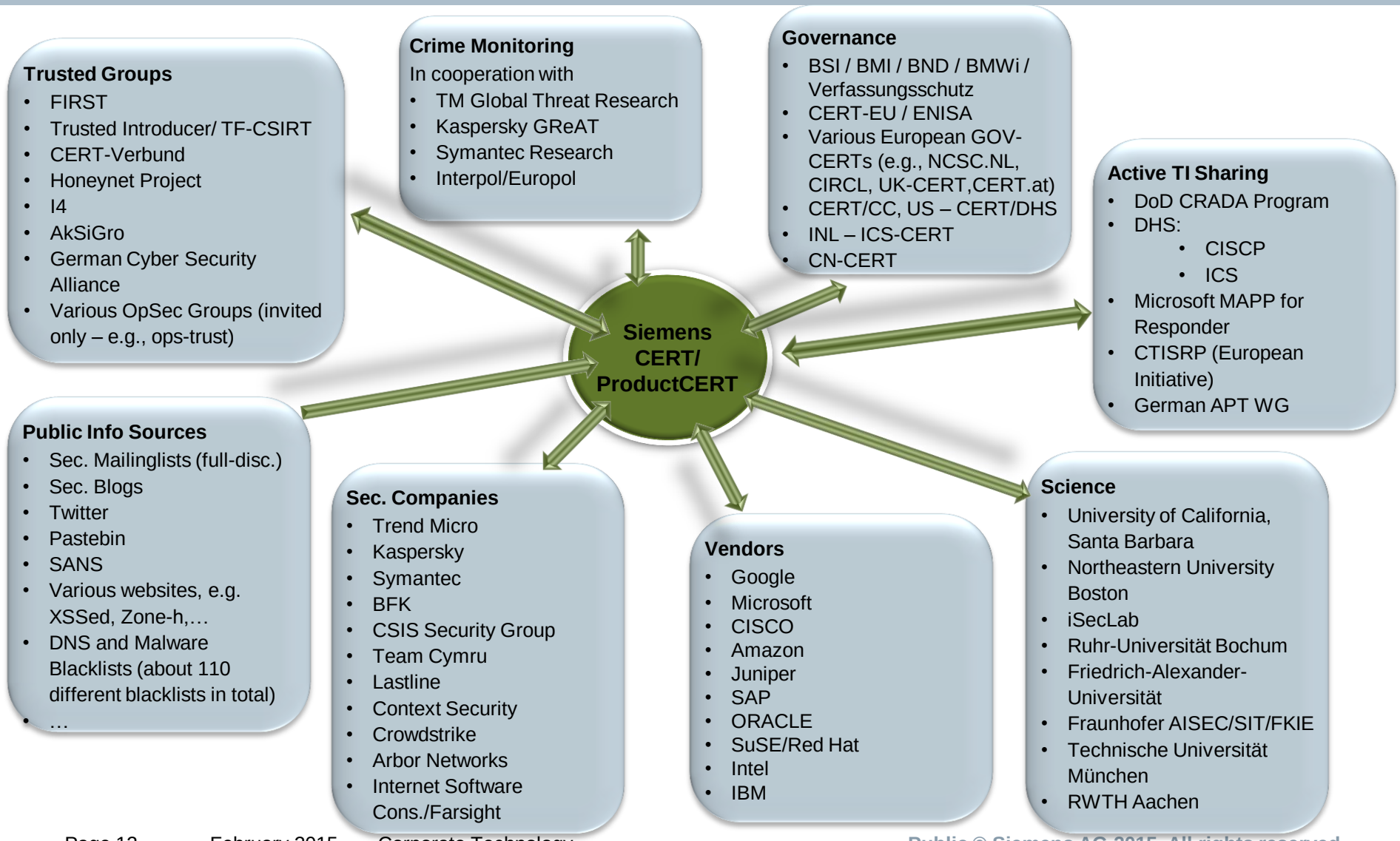
Recommendations

1. **Team members**
   - Skills in all technologies used within the company
   - People with broad security know how and deep technical skills
   - ability to think out of the box
   - Communication and Management skills important during incident response

2. **Team**
   - Good connections to various operational IT departments
   - Very good team spirit is essential
   - Contacts to various other companies and communities essential

3. **Infrastructure**
   - Abuse Handling must be automated
   - Broad tool landscape must be installed and regularly used
   - Running our own IT infrastructure helps

External Contacts



Contact

Thomas Schreck
Senior Key Expert
CT RTC ITS CSI-DE / Siemens CERT

Otto-Hahn-Ring 6
81739 Munich

E-mail: t.schreck@siemens.com

https://www.siemens.com/cert