



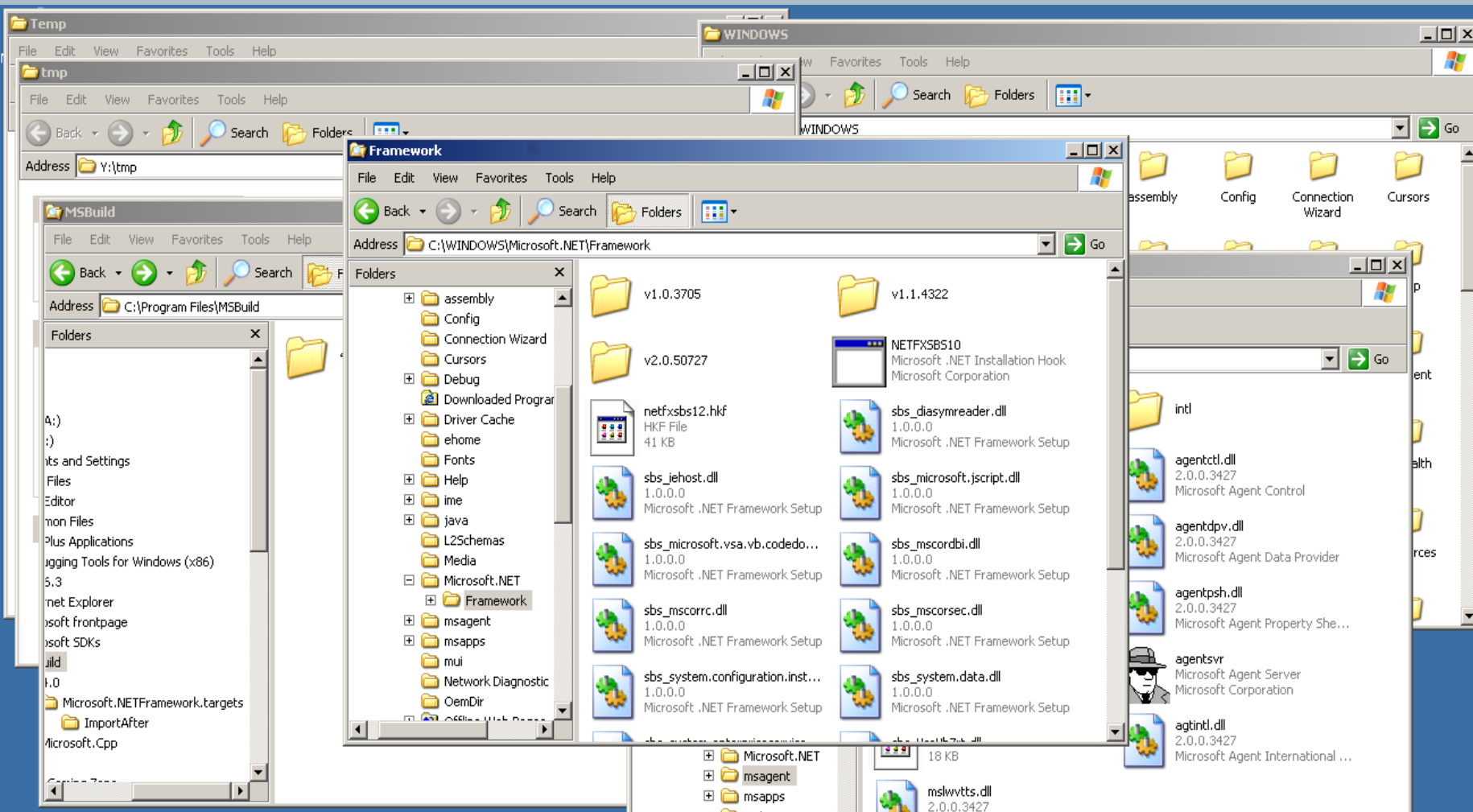
SIEMENS



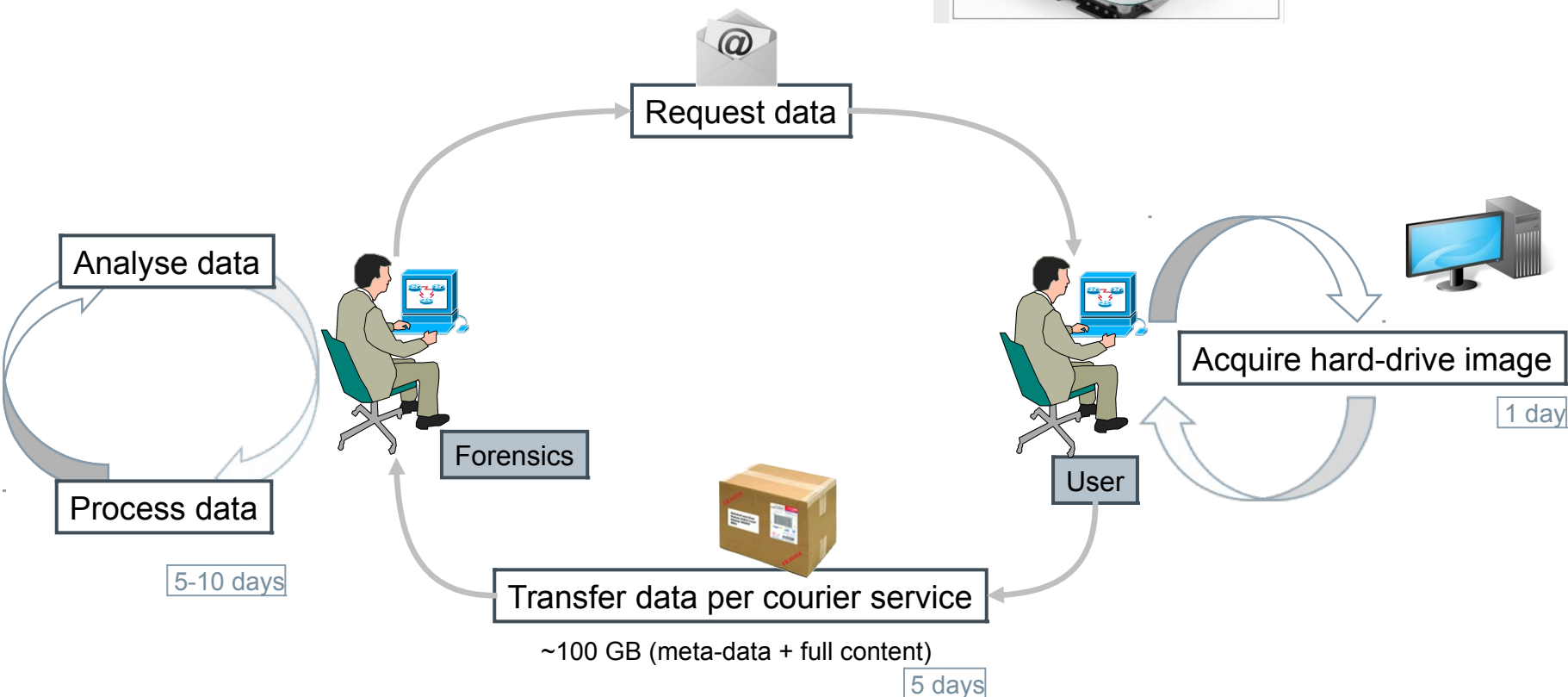
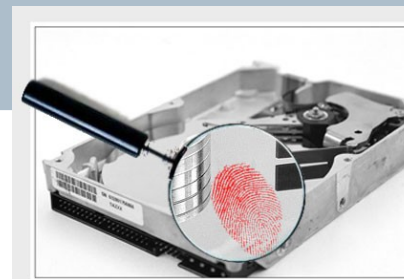
Siemens Corporate Technology

**Our Turbine got Hacked!
Performing Forensic Investigations of Industrial
Control Systems**

Heiko Patzlaff

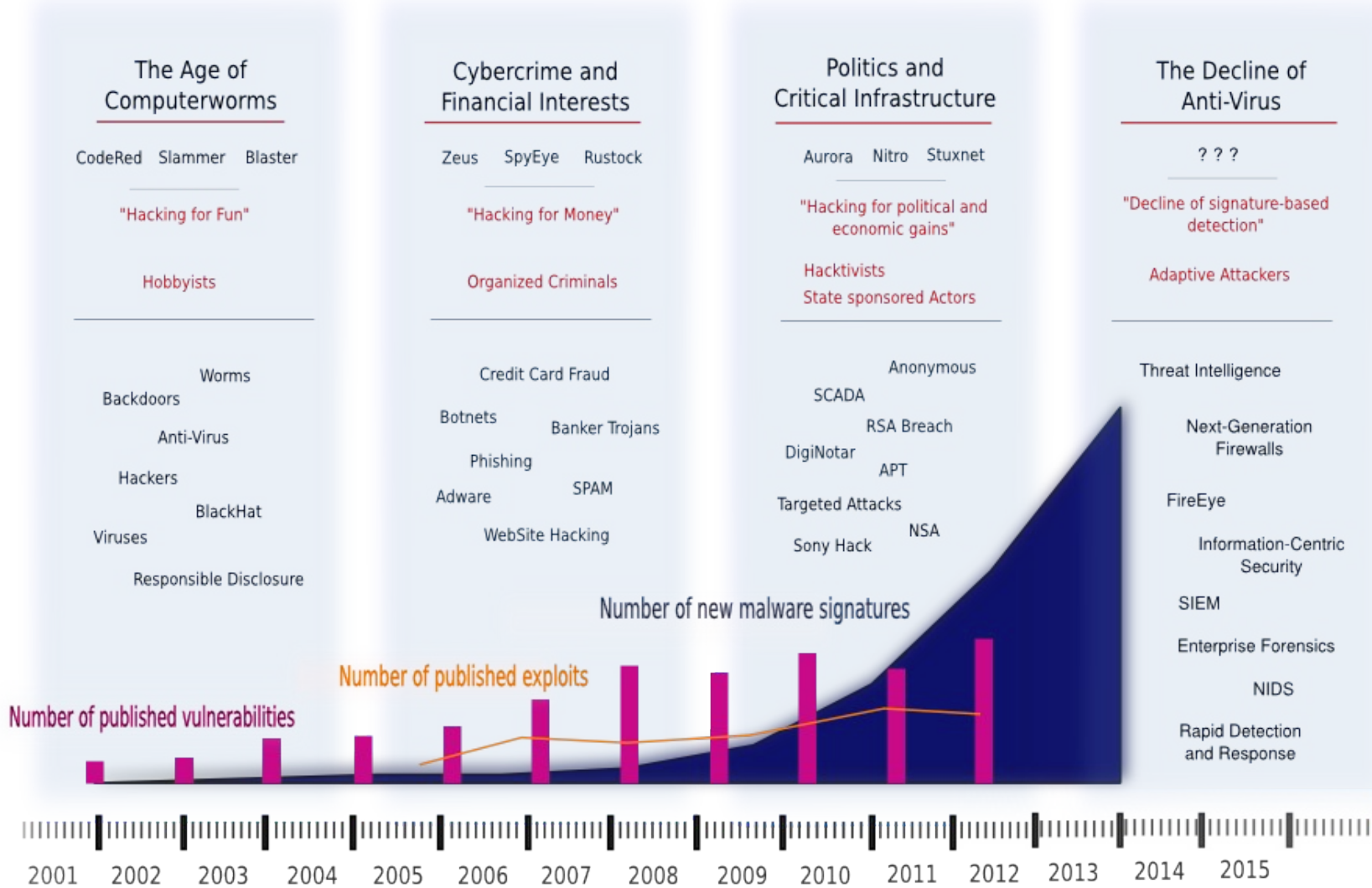


The traditional approach to host forensics



Total time per host analysis: 10-15 days!

The changing security landscape



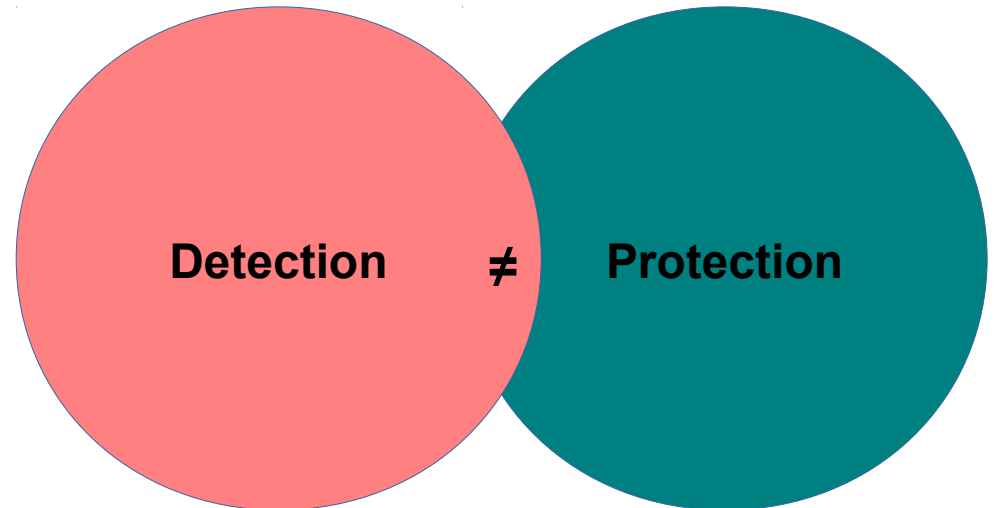
The increasing need for data and for data analysis

signature-based
methods



FP free → Fully automated

signatureless
methods



Not FP free → Requires human interpretation

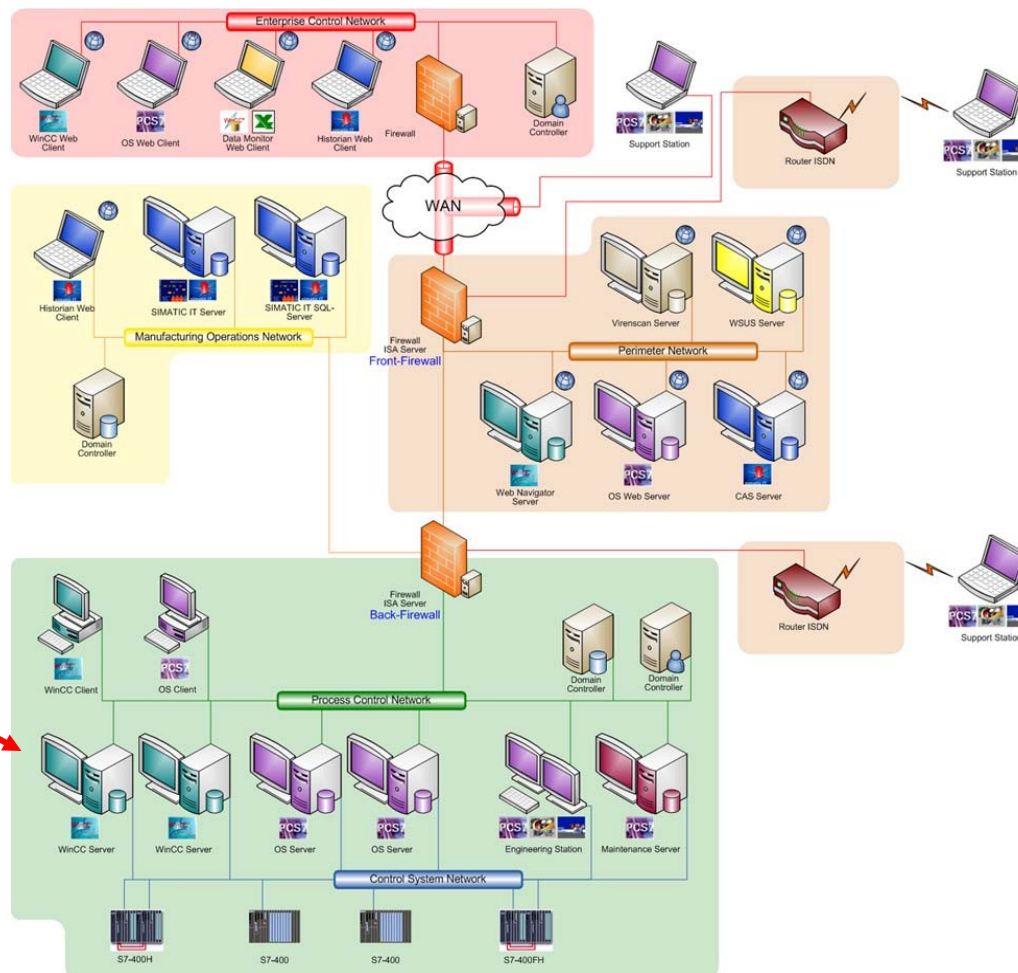
Need for data increase
Need for analysis increases
Cost per incident increases

How can this cost increase be controlled?

The Zoo of Industrial Control Systems



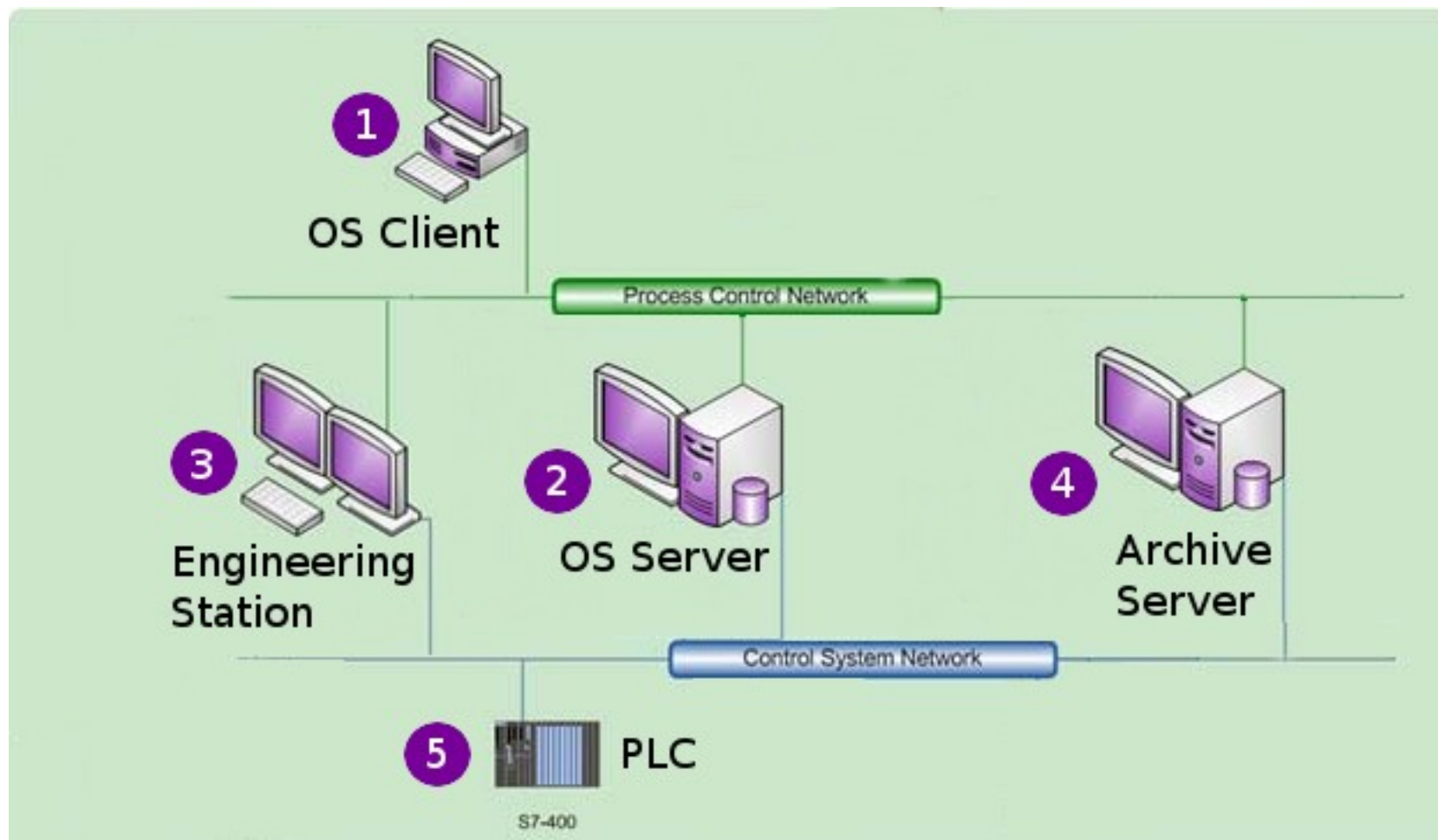
Layout of a secured industrial network (example PCS 7)



**Stuxnet target:
WinCC Server**



Layout of a secured industrial network (example)



The CRISALIS FP7 Project – Securing Critical Infrastructures



CRISALIS
SECURING CRITICAL
INFRASTRUCTURES
www.crisalis-project.eu



**Critical
Infrastructure
Security
Analysis**

Challenges

From intrusion prevention to intrusion tolerance: a layered approach is required with several safety nets and managerial procedures to handle fallback modes.

Operations: security is a secondary concern when compared to the continuous operation of the industrial process

Myth of the private network: reliance on network isolation as a main security protection is ineffective

Danger of assumptions: avoid a-priori assumptions on the attacker capabilities and modus operandi. Knowledge-based approaches are deemed to fail at detecting sophisticated attacks.

Legacy systems: industrial control system devices are often amortized over 10-15 years and cannot be easily upgraded



Security
Industry



ICS industry



UNIVERSITY OF TWENTE.

Academia

Constraints for forensic investigations in industrial settings

- **Proprietary components, interfaces, data formats and protocols**
- **Remote and distributed installations, Firewalled/Air-gaped**
- **Availability/Always on**
- **Operational constraints (real-time, low processing power, old operating systems, low bandwidth)**
- **Legal and regulatory restrictions**

Goals

- 1. develop forensic capabilities for industrial systems**
- 2. reduce cost of forensic investigations by a factor 100x**

Achieving these goals rests on three pillars:

Data Reduction

Forensic analysis is largely based on meta- and logging data.
Content information is used only very selectively.

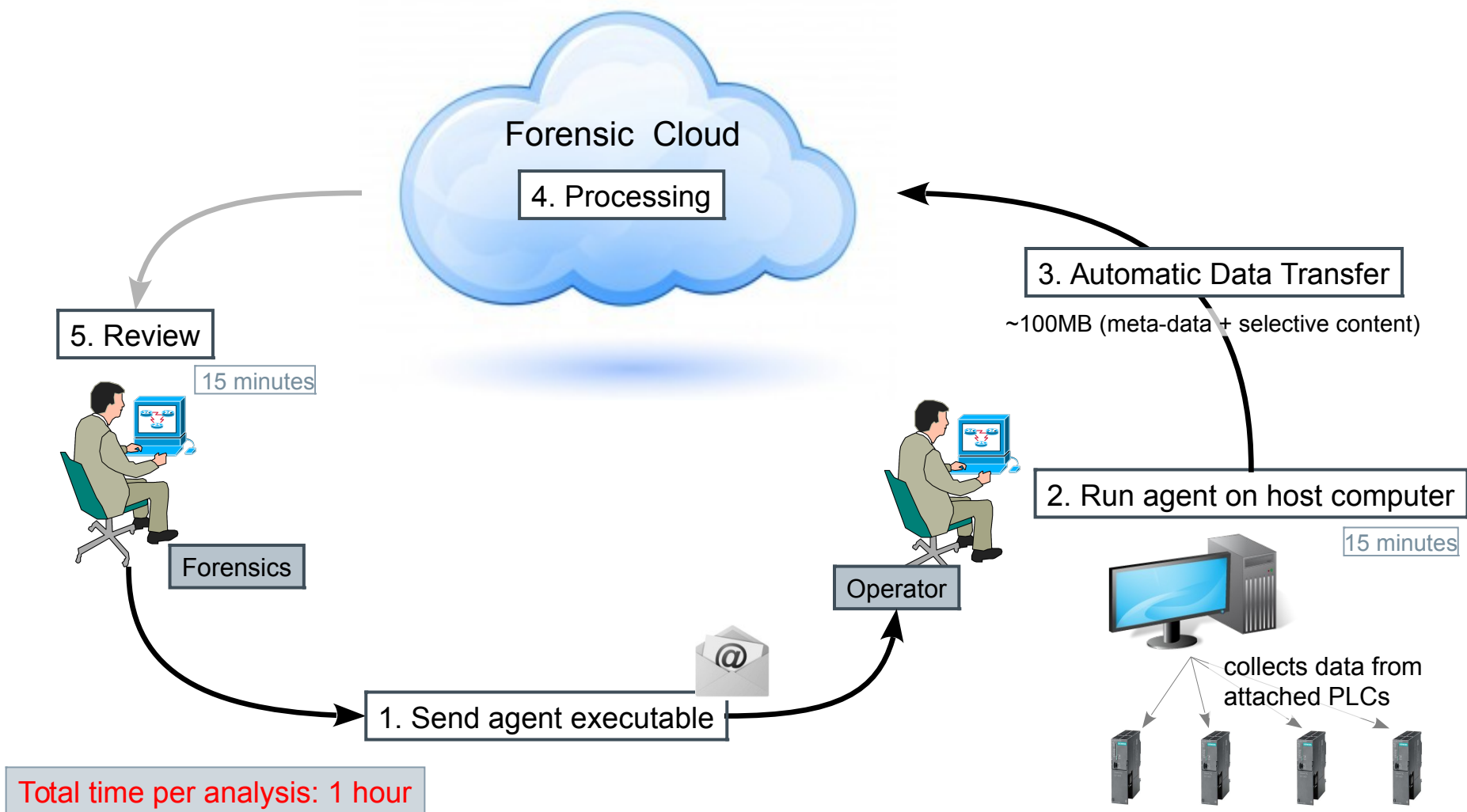
Automation

Data collection, processing and analysis is highly automated.
Human input is not required.

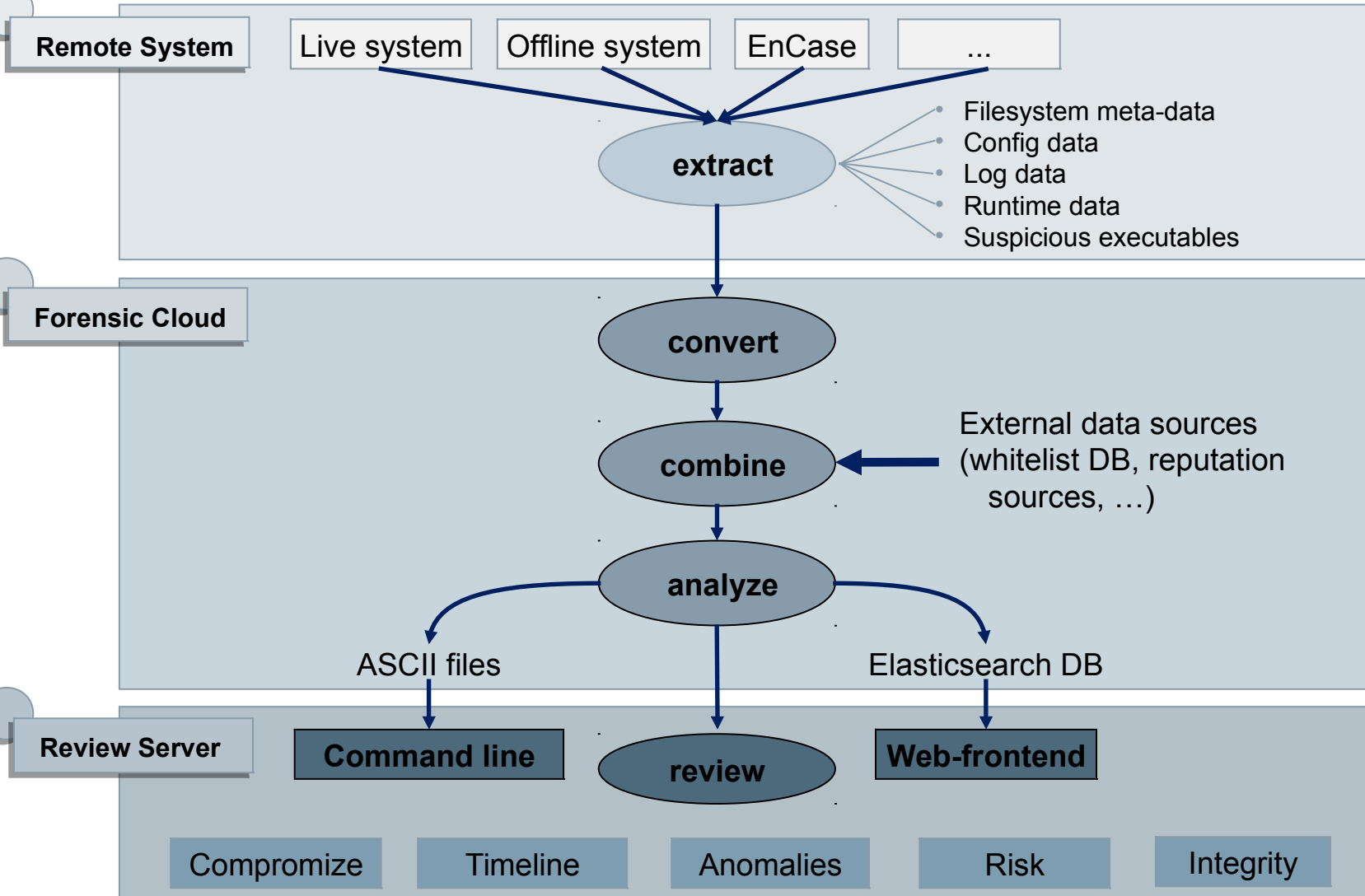
Analytics

Forensic know-how is integrated into the system (forensic knowledge system).
Requirement for human analyst is greatly reduced (Analyst → Reviewer)

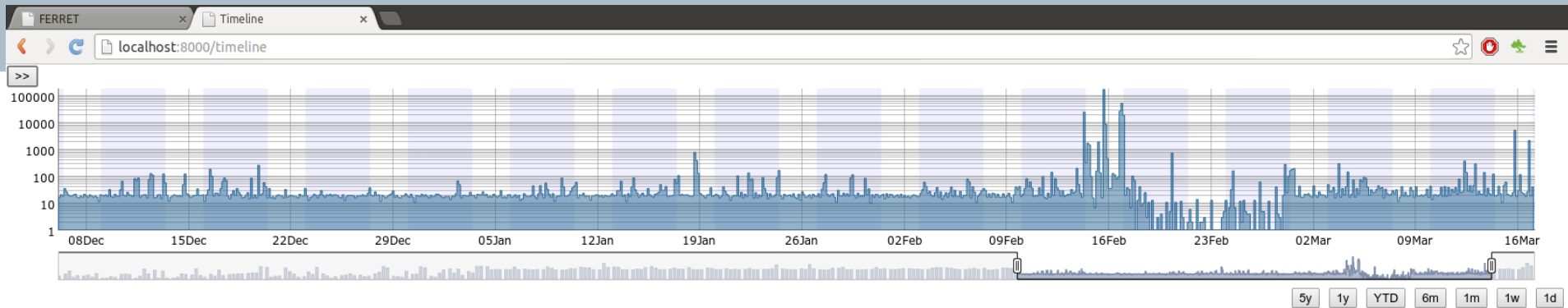
A new forensic platform



A new forensic platform



Name	Score	VT	Rep	Compile Time	Install Time	Signed	Signer	Path	Autorun	PID	Sandbox
netfilter.dll	5.71	None	0	2012-11-01T07:38:00Z	2013-12-24T03:20:01Z	Unsigned		c:\windows\system32\netfilter.dll	HKLM\System\CurrentControlSet\Services		
postlogr.dll	5.71	None	0	2012-11-01T07:35:34Z	2013-12-24T03:12:05Z	Unsigned		c:\windows\system32\postlogr.dll	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify		
nsrpm.exe	-1.4	None	0	2012-12-04T07:13:46Z	2014-03-25T14:52:41Z	Invalid	EMC Corporation	c:\program files\legato\nsr\bin\nsrpm.exe	HKLM\System\CurrentControlSet\Services		
rarext64.dll	-1.4	0	0	2005-06-07T07:26:27Z	2009-08-24T22:21:14Z	Unsigned		c:\program files (x86)\winrar\rarext64.dll	HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers		
nsrexc.d.exe	-6.3	0	0	2012-12-04T07:10:53Z	2014-03-25T14:52:41Z	Invalid	EMC Corporation	c:\program files\legato\nsr\bin\nsrexc.d.exe	HKLM\System\CurrentControlSet\Services		
maintenanceservice.exe	-8.1	0	0	2012-04-20T23:47:52Z	2012-06-01T19:17:21Z	Signed	Mozilla Corporation	c:\program files (x86)\mozilla maintenance service\maintenanceservice.exe	HKLM\System\CurrentControlSet\Services		
httpd.exe	-8.1	0	0	2013-06-29T13:39:47Z	2013-10-16T17:43:26Z	Invalid	Apache Software Foundation	c:\apache\bin\httpd.exe	HKLM\System\CurrentControlSet\Services		
tpsvc.dll	-8.1	0	0	2009-07-03T10:32:41Z	2009-09-17T10:21:12Z	Signed	ThinPrint GmbH	c:\windows\system32\tpsvc.dll	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify		
fbserver.exe	-8.1	0	0	2008-06-13T12:22:08Z	2009-03-09T12:01:19Z	Invalid	Firebird Project	c:\program files (x86)\firebird\firebird_2_1\bin\fbserver.exe	HKLM\System\CurrentControlSet\Services		
fbguard.exe	-8.1	0	0	2008-06-13T12:24:01Z	2009-03-09T12:01:19Z	Invalid	Firebird Project	c:\program files (x86)\firebird\firebird_2_1\bin\fbguard.exe	HKLM\System\CurrentControlSet\Services		
tomcat5.exe	-8.1	0	0	2004-11-13T09:28:10Z	2011-09-12T14:30:25Z	Invalid	Apache Software Foundation	d:\atlassian-jira-enterprise-3.6-standalone\bin\tomcat5.exe	HKLM\System\CurrentControlSet\Services		



5y 1y YTD 6m 1m 1w 1d

Showing 1 to 100 of 349,823 records (out of 733,716 total records) from 2013-12-06 to 2014-03-17. Show / hide columns

Date	Type	Tstamp	Name	Details
2013-12-06 02:15:11	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 02:17:47	evts	c-----	MOMLog	Health Service ESE Store; 700 (no description); HealthService 1248 Health Service Store: C:\Program Files\System Center Operations Manager\Agent\Health Service State\Health Service Store\H
2013-12-06 02:17:59	evts	c-----	MOMLog	Health Service ESE Store; 701 (no description); HealthService 1248 Health Service Store: C:\Program Files\System Center Operations Manager\Agent\Health Service State\Health Service Store\H
2013-12-06 02:26:38	evts	c-----	MOMLog	Health Service Script; 100 (no description); PRIMERGYServerDiscovery.vbs Fujitsu PRIMERGY Server TRISTK113VWS.tr001.siemens.net has no ServerView Agent installed
2013-12-06 02:30:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 02:45:11	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 03:00:11	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 03:10:21	evts	c-----	ManageSoft	Installation Agent; 1610743981 (no description); Self Heal OK ?ManagedDeviceSettings[Common](1
2013-12-06 03:15:11	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 03:20:53	evts	c-----	MOMLog	OpsMgr Connector; 1073762848 (no description); WW300SCOM010 c1470a6491000ab6909afa3c7c54ef0e
2013-12-06 03:21:13	evts	c-----	MOMLog	OpsMgr Connector; 21026 (no description); WW300SCOM010 c1470a6491000ab6909afa3c7c54ef0e
2013-12-06 03:26:39	evts	c-----	MOMLog	Health Service Script; 100 (no description); PRIMERGYServerDiscovery.vbs Fujitsu PRIMERGY Server TRISTK113VWS.tr001.siemens.net has no ServerView Agent installed
2013-12-06 03:30:11	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 03:45:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 04:00:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 04:15:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 04:26:38	evts	c-----	MOMLog	Health Service Script; 100 (no description); PRIMERGYServerDiscovery.vbs Fujitsu PRIMERGY Server TRISTK113VWS.tr001.siemens.net has no ServerView Agent installed
2013-12-06 04:30:11	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 04:45:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 05:00:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 05:15:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 05:26:37	evts	c-----	MOMLog	Health Service Script; 100 (no description); PRIMERGYServerDiscovery.vbs Fujitsu PRIMERGY Server TRISTK113VWS.tr001.siemens.net has no ServerView Agent installed
2013-12-06 05:30:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 05:45:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 06:00:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.
2013-12-06 06:15:10	evts	c-----	MOMLog	Health Service Script; 6022 (no description); LogEndToEndEvent.js This event is logged to the Windows Event Log periodically to test a event collection.


FERRET

A platform for the investigation of security incidents in industrial systems.

- **Semi-automated**
- **Cost-effective**
- **Agent agnostic**
- **Scalable**
- **Forensic and Data-Analytics capabilities**

The Siemens logo is displayed in a white rectangular box in the top-left corner of the slide. The word "SIEMENS" is written in a bold, teal-colored, sans-serif font. Below the logo box, there is a thin white horizontal line.

SIEMENS

The background of the slide is a scenic landscape photograph. It features a dense forest of tall, green coniferous trees in the foreground and middle ground. In the background, there are rugged mountains with patches of snow on their peaks and slopes. The sky is bright blue with scattered white clouds. The overall scene is a natural, mountainous environment.

Thank you for your attention

**Heiko Patzlaff
Siemens**