kuppingercole ANALYSTS

Cyber Threat Intelligence

IRMA, June 13th, 2017

Mike Small CEng, FBCS, CITP
Senior Analyst
Kuppinger Cole
Mike.Small@kuppingercole.com

Agenda

Mike Small
KuppingerCole

- The Cyber Challenge
- Cyber Threat Intelligence
- Building Threat Intelligence
- Sharing Threat Intelligence
- Summary

kuppingercole ANALYSTS

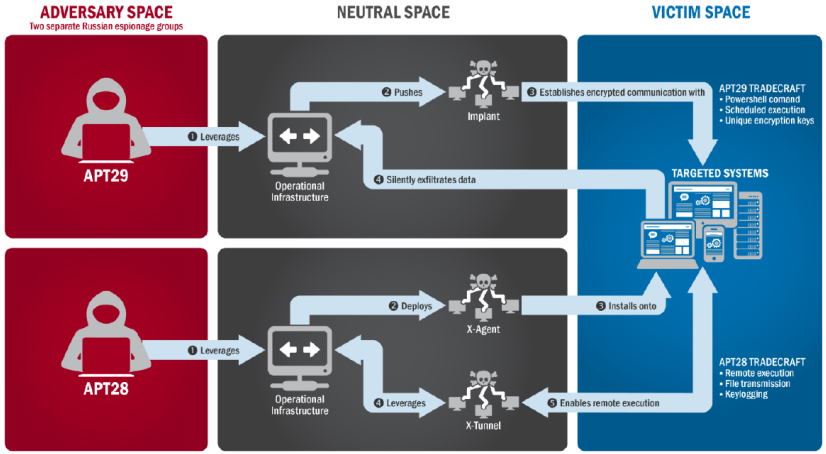
On the average the time between an organization's IT systems being infiltrated and them becoming aware of this is 200 days.

THE CHALLENGE

Cyber Challenges

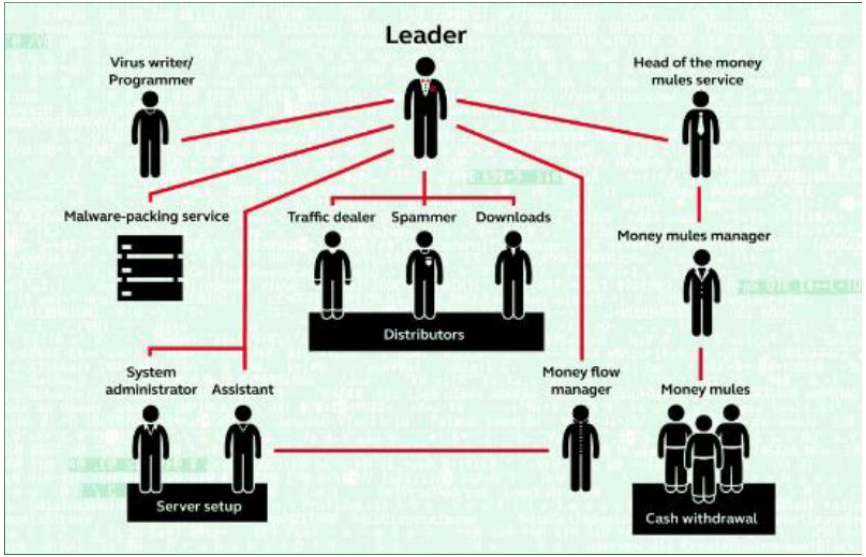
Clinton's emails hacked

- GRIZZLY STEPPE – Russian Malicious Cyber Activity
- https://www.us-cert.gov/



Behind the Cyber Challenge

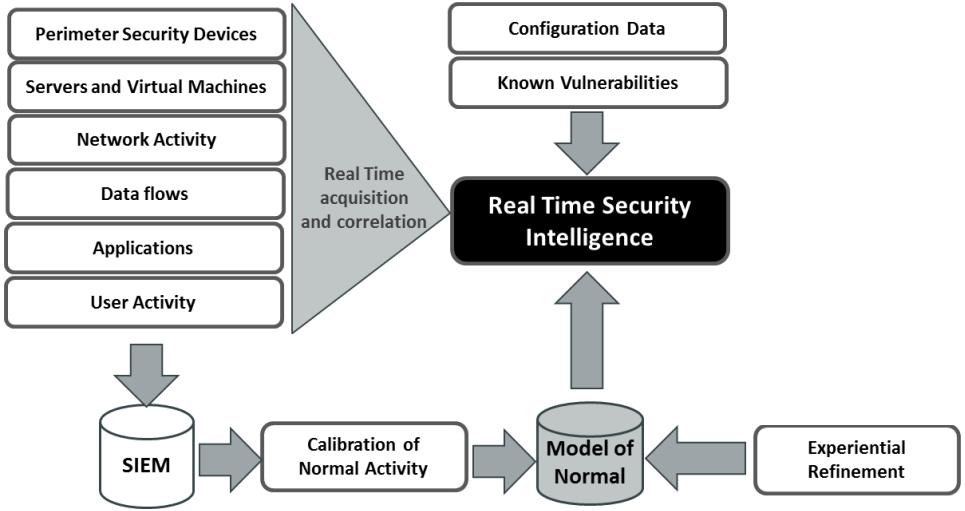
The adversaries work together so should we!



Cloutier Borderless Cyber Europe2016

Organization need Cyber-Intelligence

Organizations are collecting massive amounts of data but need intelligence to exploit it.



Sharing Cyber-Threat Intelligence

Sharing needs standards.

There have been many initiatives

OpenIOC	VERIS	CybOX
IODEF	TAXII	STIX
TLP	OTX	CIF

kuppingercole ANALYSTS

"Only through a balanced understanding of both the adversary and ourselves can we understand enough about the true nature of the threats we face to make intelligent defensive decisions."

OASIS Cyber Threat Intelligence (CTI) Technical Committee | Charter

WHAT IS THREAT INTELLIGENCE

Knowing your adversary's plans can help win battles

In 480 BC Demaratus sent a message warning of the Persian plan to invade Sparta hidden behind the wax of a blank writing tablet

- According to Herodotus

Image digitally reproduced with the permission of the Papyrology Collection, University of Michigan Library.

Kinds of Cyber-Threat Intelligence

Strategic

- Who are the adversaries?
- What are their objectives?
- What are their campaigns

Tactical

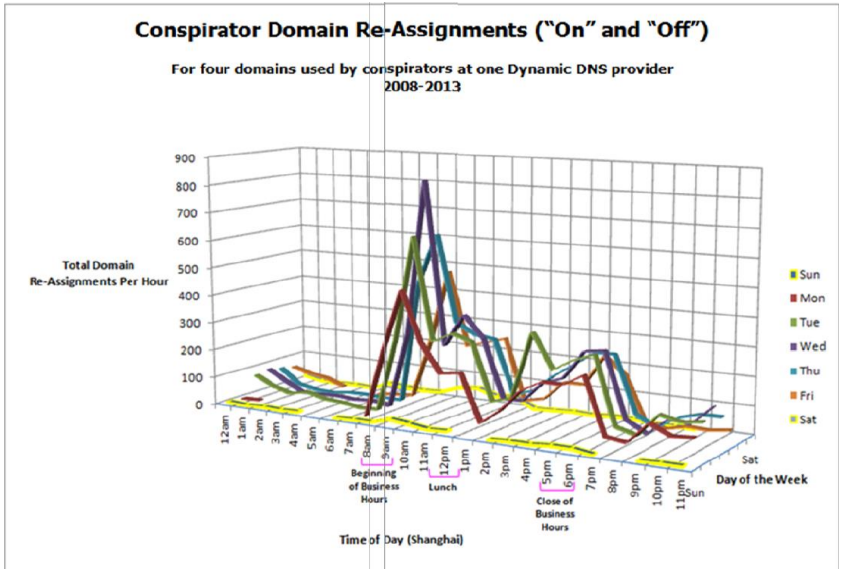
- Tools, Tactics and Procedures used
- Specific observables

Strategic Cyber-Threat Intelligence

Adversary PRC Army

Objectives - to steal US Intellectual Property

Campaigns against US companies



US Dept. of Justice Indictment Chinese Hack

Intel Driven Defence – Lockheed Martin 2010

"The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too."

Intelligence is based on Indicators:

- Observed
- Computed
- Shared

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Tactical Cyber-Threat Intelligence

Information about **threats, TTPs**, and **devices** that adversaries employ; the **systems** and **information** that they **target**; and any other **threat-related information** that provides greater **situational awareness**

Thomas Schreck | Siemens CERT
Home | Borderless Cyber Europe

- Timely
- Relevant
- Accurate
- Specific
- Actionable

Types of Indicator

IOE

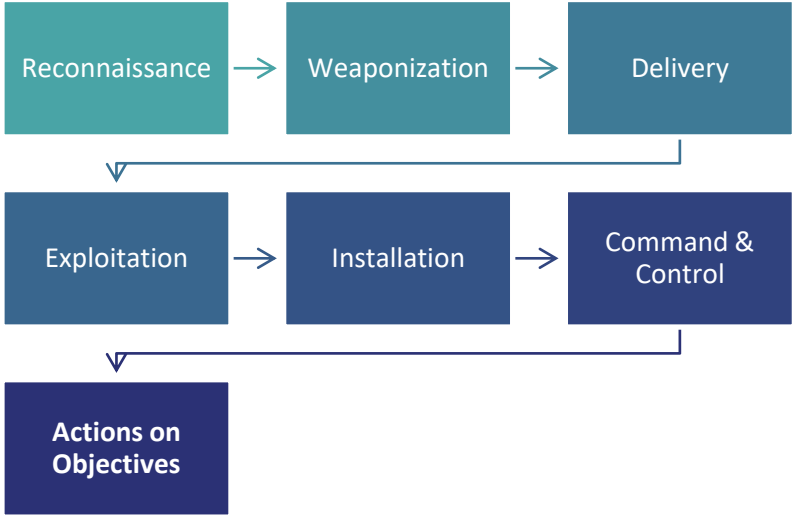
- Indicators of Exposure (aka vulnerabilities)
- Common Vulnerabilities and Exposures
- Example - missing patch

IOC

- Indicators of Compromise
- Signatures of an attack in progress
- Example – file HASH

Cyber Kill Chain

Different indicators for different stages in the adversary process.



http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

kuppingercole ANALYSTS

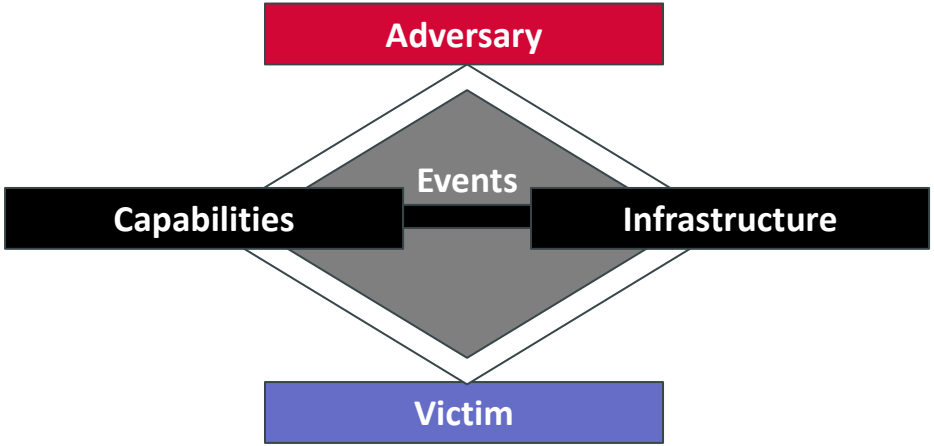
In order for a cyber attack to be economical, adversaries must re-use tools and infrastructure. By building intelligence on these, defenders force adversaries to change their approach.

BUILDING THREAT INTELLIGENCE

Diamond Model

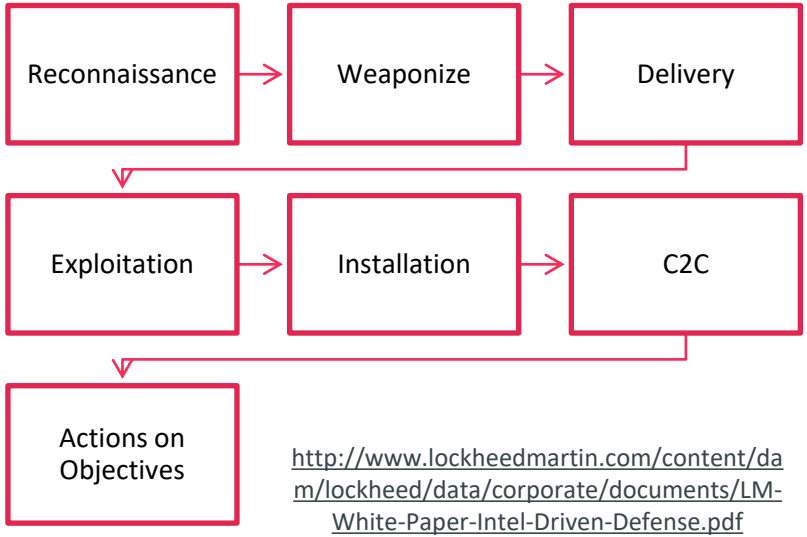
The basic atomic model of cyber intrusions

- Center for cyber intelligence analysis and threat research
- Caltagirone, Sergio ; Pendergast, Andrew ; Betz, Christopher
- July 2013

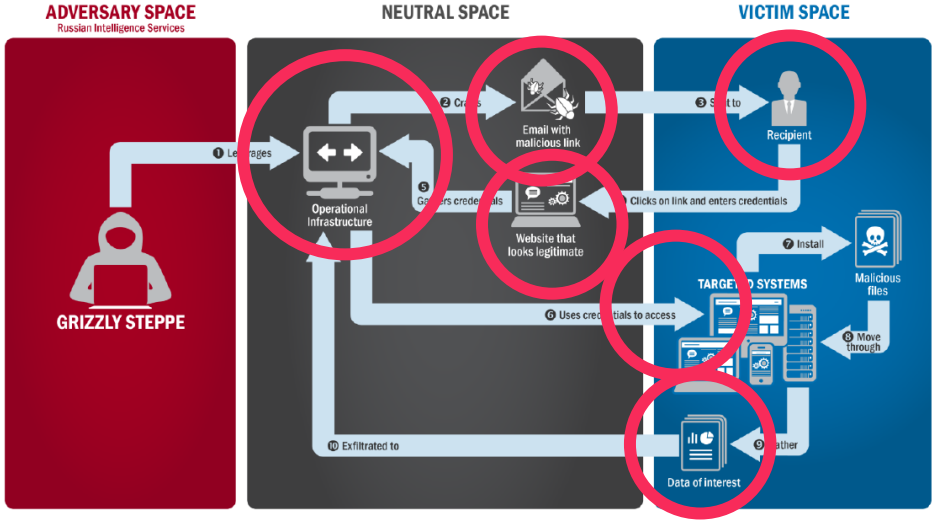


http://www.dtic.mil/docs/citations/ADA586960

Grizzly Steppe – Kill Chain Model



http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

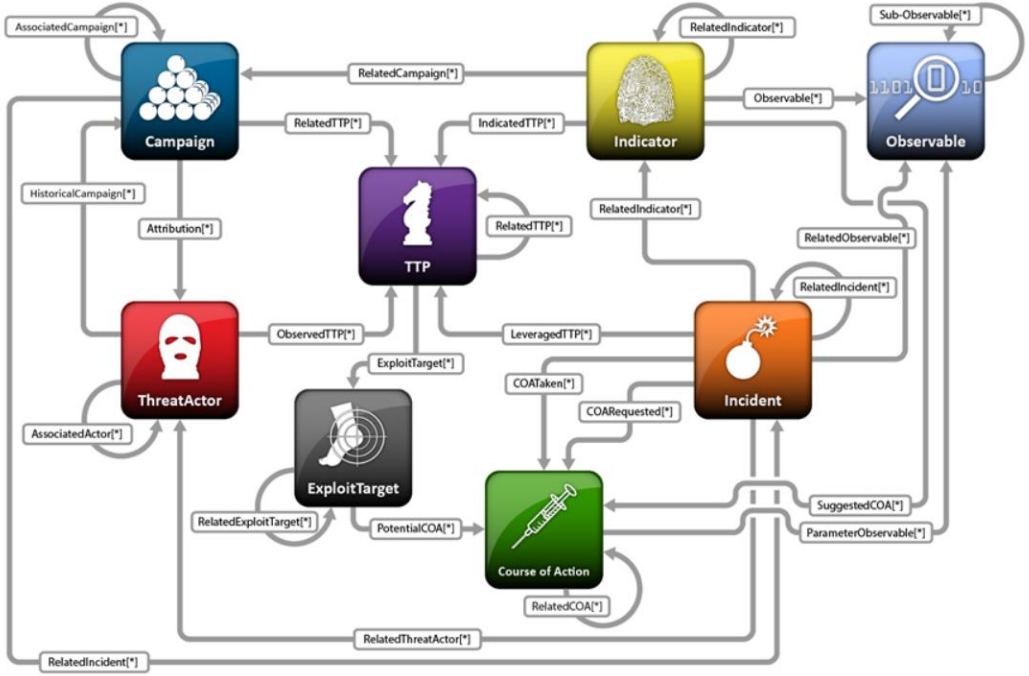


https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

A Model to Describe Indicators

Structured Threat Information Expression (STIX) Provides a machine readable interchange format.

- STIX Relationships | STIX Project Documentation



Building the Intelligence

Analysis of several data breaches

An email with common subject line

Target Bank employees

as part of a campaign

Using specific tools

By a known group

Shared description of the Threat

And the action can you take

Actionable Intelligence

The information built from the previous incidents leads to actionable intelligence

Courses of Action

Understanding the kill chain allows you to take action to pre-empt the next step.

Detect	Deny
Disrupt	Degrade
Deceive	Destroy

We need a system where actionable Cyber Threat Information is shared among private and public organizations.

SHARING THREAT INTELLIGENCE

Barriers to Sharing Threat Intelligence

Trust

- Building trust between groups to enable sharing

Legal

- Liability and privacy issues related to sharing

Technical

- Standards and trusted communications

Communities of Trust

Your organization cannot create threat intelligence on its own.

Sharing is essential to meet the challenges.

CERT UK

CERT	ISAC	NIST
ENISA	Black hat	FIRST
Vendors	Law enforcement	…

Legal Challenges to sharing

Many different privacy laws

Bilateral sharing agreements

Liability for shared data

Control over intellectual property

Traffic Light Protocol

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information.

- Traffic Light Protocol (TLP)

It is NOT an access control mechanism. Source must trust recipient.

Colour	How may be shared
Red	Recipients may not share TLP:RED information with any parties outside of the specific exchange, in which it was originally disclosed
Amber	Recipients may only share TLP:AMBER information with members of their own organization, and with others who need to know to protect themselves or prevent further harm.
Green	Recipients may share TLP:GREEN information with peers and partner organizations but not via publicly accessible channels.
White	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction

Information Exchange Policy Framework

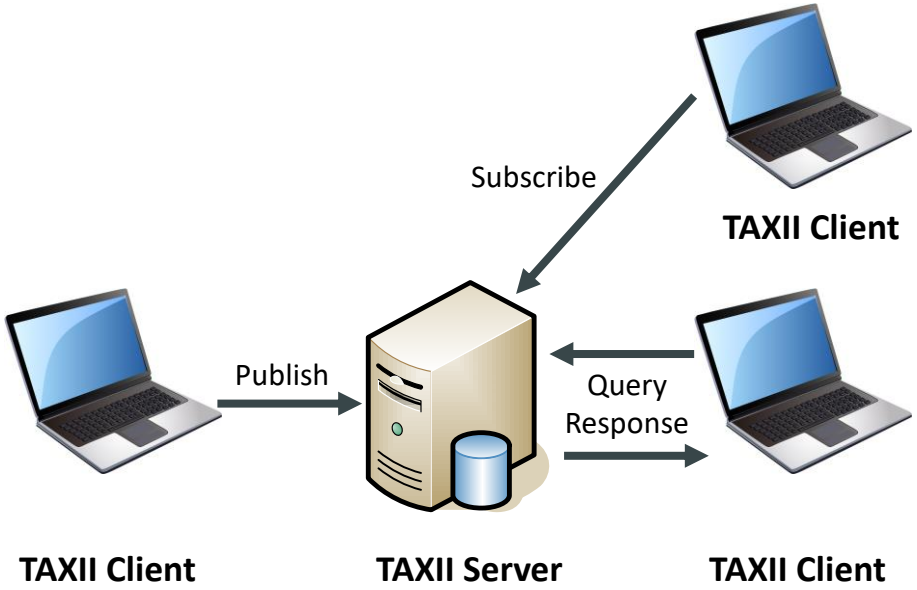
Intended to facilitate controlled automated sharing

HANDLING	ACTION	SHARING	LICENSING
• Defines obligations or controls on information received, to ensure the confidentiality	• Defines the permitted actions or uses of the information a recipient	• Defines any permitted redistribution of information that is received	• Defines any applicable agreements, licenses, or terms of use for the information being shared

FIRST.org / Global Initiatives / Standards / Information Exchange Policy (IEP)

Automated Sharing - TAXII

Trusted Automated eXchange of Indicator Information (TAXII™). Enables Secure, Authenticated Sharing of Threat Information



http://docs.oasis-open.org/cti/taxii/v1.1.1/cs01/part1-overview/taxii-v1.1.1-cs01-part1-overview.pdf

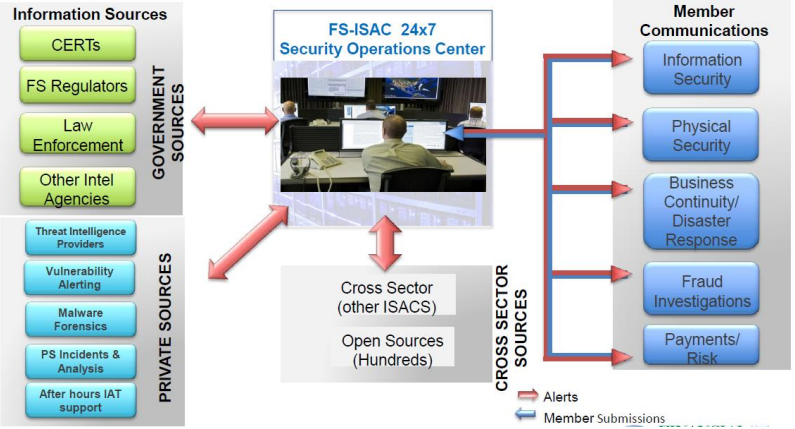
Financial Services – Cyber Threat Sharing

Belgian bank Crelan hit by a 70 million Euro fraud.

- (reportedly Business Email Compromise)
- The Brussels Times - Belgian bank Crelan hit by a 70 million Eur fraud

Head of Austrian aerospace parts maker FACC fired after a cyber fraud that cost 42 million euros.

- Austria's FACC, hit by cyber fraud, fires CEO | Reuters



FS-ISAC Using STIX and TAXII for CTI Sharing

https://www.oasis-open.org/events/sites/oasis-open.org.events/files/Carlson.pdf

US Department of Homeland Security

Homeland Security

US-CERT
United States Computer Emergency Readiness Team

Automated, near real-time indicator sharing ecosystem built on STIX/TAXII

Designed to foster widespread sharing of CTI – specifically indicators

Launched in 2014. Updated as a result of the Cybersecurity Information Sharing Act of 2015 (CISA)

https://www.oasis-open.org/events/sites/oasis-open.org.events/files/Strusev2.pdf

kuppingercole ANALYSTS

Shared Cyber Threat Intelligence is essential to effectively protect against Cyber Threats.

SUMMARY

Summary

Shared Cyber Threat Intelligence is essential to protect against Cyber Threats.

Standards make automated sharing more practical.

Your organization needs to share and exploit CTI.

QUESTIONS

The Future of Information Security – Today.

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decisions making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

Kuppinger Cole Ltd.
Headquarters
Am Schloßpark 129
65203 Wiesbaden | Germany
Tel +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com

Related Research

No.	Type	Title	L.
72528	Executive View	Emerging Threat Intelligence Standards	
71033	Advisory Note	Real Time Security Intelligence	
74001	Survey	KuppingerCole and BARC Joint Study: Big Data and Information Security	
72025	Advisory Note	Sustainable Infrastructures through IT Compliance	