

# Tools of the Trade

Lessons Learned from (C)ISOs' Desks

Matthias Luft, [mluft@ernw.de](mailto:mluft@ernw.de)



# ERNW

Providing Security.



- Highly specialized security consulting & assessment services company, since 2001
- Independent of vendors, financial obligations, share holders.
- Our customers are mainly very large, global enterprises
- #whoami
  - Team Lead Vulnerability Research and Information Security Management
  - Long-time-pentester-who-became-team-lead








**FAST FITNESS**

**BEFORE**

**AFTER**

**PERSONAL TRAINING**  
Real results at affordable prices  
\$300 for 15 hours with a trainer

**2 FREE TRIAL SESSIONS\***

**FAST FITNESS PERSONAL TRAINING**  
SMS THE WORD 'NOW' to 0414 645 156  
& RECEIVE TWO FREE TRIAL SESSIONS WITH A TRAINER

15 Lawrence Street, Freshwater  
99397793 // [www.fastfitness.com.au](http://www.fastfitness.com.au)


\*FOR NEW CLIENTS ONLY

Download Image Rights and use the code to view our website



VIA 9GAG.COM



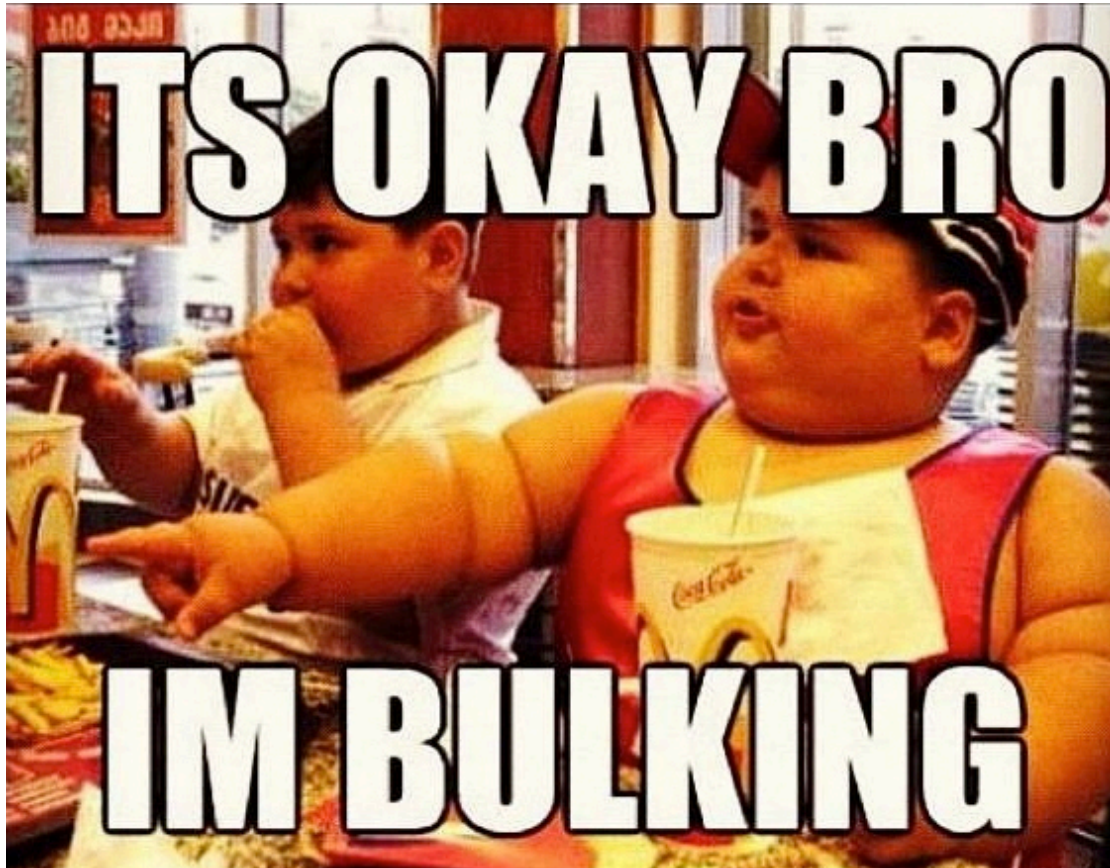


Hi I'm going to demonstrate how to do a squat  
bicep and shoulder press combination. Free

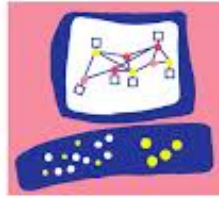


## 5-Minute Workout: Triple Your Workout Results









# Check Point®

SOFTWARE TECHNOLOGIES LTD.

- **Real-Time protections** – The IPS Software Blade is constantly updated with new defenses against emerging threats. Many of the IPS protections are pre-emptive, providing defenses before vulnerabilities are discovered or exploits are even created.



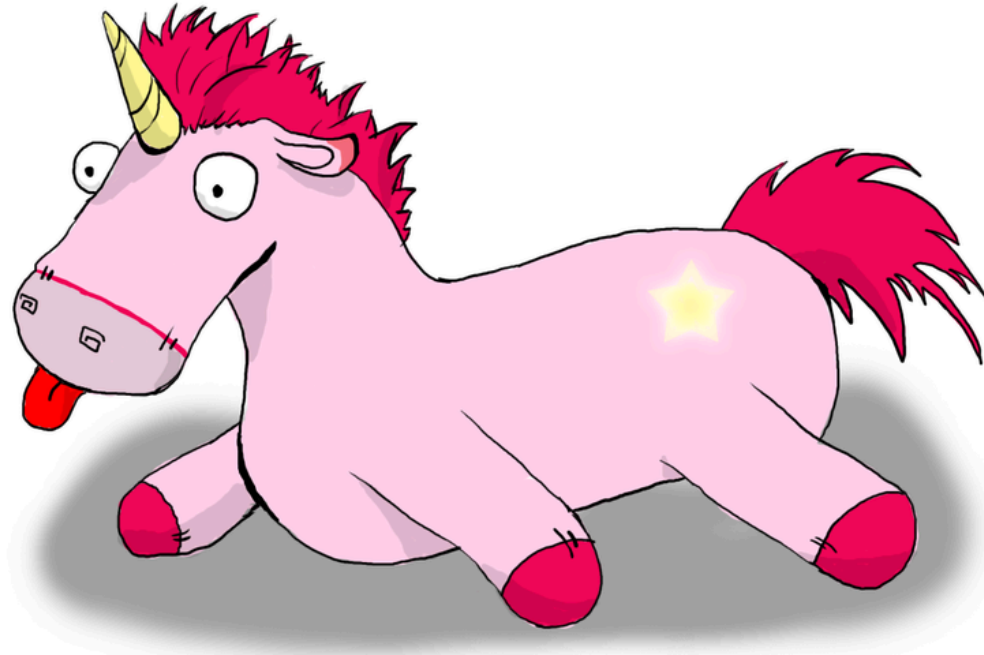
**Complete protection** — Today, antivirus alone isn't enough to defend against sophisticated, stealthy malware and attacks. The highest scoring vendor in an NSS Labs comparative test of current defenses against evasion attacks, McAfee finds, fixes, and freezes malware fast with multiple layers of protection. And strong encryption secures your vital confidential data and prevents unauthorized access to PCs, Macs, laptops, and removable media — transparently and without slowing system performance. Behavior and reputation systems integrate with the cloud-based McAfee Global Threat Intelligence to protect against emerging cyberthreats across all vectors — file, web, message, and network.



FireEye cyber security products combat today's advanced persistent threats (APTs). As an integral piece of an Adaptive Defense strategy, our state-of-the-art network security offerings protect against cyber attacks that bypass traditional signature-based tools such as antivirus software, next-generation firewalls, and sandbox tools. [View](#) the FireEye Corporate Brochure to learn more about our offerings.



# APT Protection\*



\* or Advanced/Next-Generation  
malware detection/protection – or one of the other terms.

# The one we can rely on?

## Top Three Firewall Configuration Best Practices:

- **White List (Deny by Default)**-When you implement a white list the “Deny All” rule is located at the bottom of the list and considered the “catch all”. As needed, rules can be added to the list to allow traffic through the firewall. Although this is the most secure way and the best practice to set up a firewall, it is the least used because it is somewhat time consuming; especially in a

[msdn.microsoft.com/en-us/library/windows/desktop/cc307394.aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/cc307394.aspx)

## Least Privilege

[www.sans.org/reading-room/whitepapers/bestprac/implementing-privilege-enterprise-1188](http://www.sans.org/reading-room/whitepapers/bestprac/implementing-privilege-enterprise-1188)

## Firewall

To support ‘least privilege’ and separation the following general rules should be applied when configuring a firewall:

- Control connections from the Internet to the DMZ by only allowing protocols that are needed by the applications or services that are being offered (i.e. HTTP, HTTPS, perhaps SMTP if there is a mail server)
- Only allow Internet connections to the DMZ, by implementing a ‘deny all’ approach if connections to other zones are attempted.

practical. When not practical, the threat model should explicitly call out the reasons why.

# Network Security in 2015?



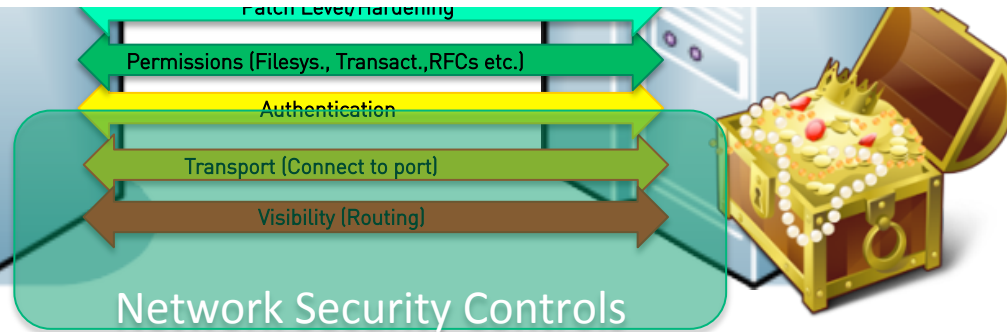


## Security Controls

# Microsoft Security Bulletin MS15-034 – Critical Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)

Published: April 14, 2015 | Updated: April 22, 2015

Version: 1.1



## Least Privilege Approach

Deny everything except for \$SOMETHING



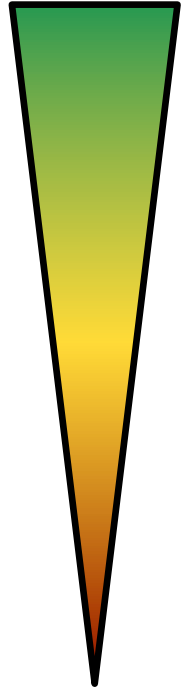
- Whitelist = Identify the positive.
- Requires *contextual information*.

## Filtering Controls

---

- Choke point firewall
- Host-based/NIC-level Firewalls

Level of  
Centralization



# Here's some Dilemma

Infosec people == Centralized least privilege controls

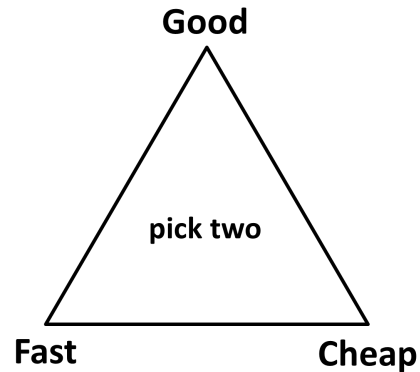
Unfortunately:  
Infosec people != contextual information





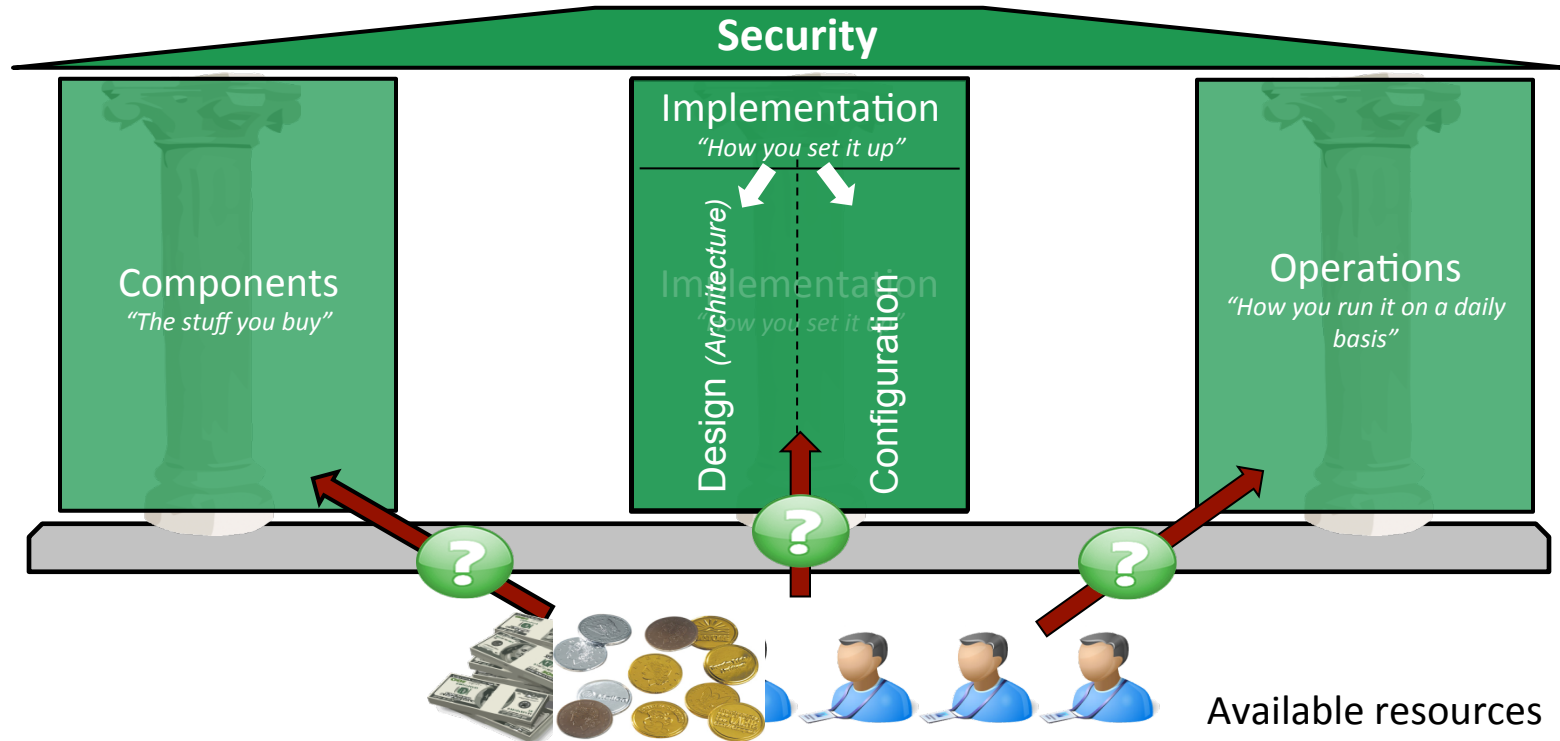
## The Dilemma

---



- Least privilege rules
- Centralized enforcement
- Security operations should strive for *efficiency*.

# Efficiency – Operations is key



## Efficiency

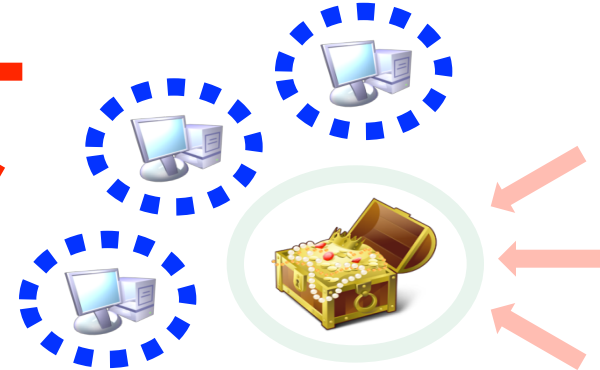
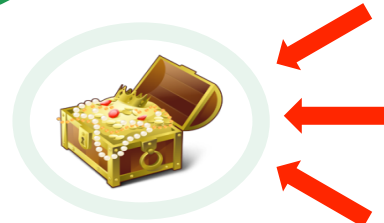
Read: in pretty much all sufficiently large organizations...



— You have to accept a trade-off!

# Least Privilege?

- Protection need
- Network Exposure
- Vulnerability Factor
- Trust (worthiness)





# Sample Classification

			Segmentation	Filtering	Access Control	Entity Protection	Visibility	Secure Management	Review & Testing
Baseline			Default shared segment	Default blacklists	Central authentication	Default	Central logging	Mandatory Jump Server usage	Vulnerability Scanning, 3 months
0	0	1	Dedicated segment	Segment-based whitelist		Default + threat-oriented hardening <sup>4</sup>	Keyword-based analysis		Vulnerability Scanning, 3 months Assessment, 24 months
0	1	0							
0	1	1	Dedicated segment			Default + threat-oriented hardening	Keyword-based analysis		Vulnerability Scanning, 3 months Assessment, 12 months
1	0	0	Dedicated segment	Segment-based whitelist					Vulnerability Scanning, 3 months Assessment, 24 months
1	0	1	Dedicated segment	Segment-based whitelist		Default + threat-oriented hardening	SIEM analysis		Vulnerability Scanning, 3 months Assessment, 12 months
1	1	1	Dedicated segment			Default + threat-oriented hardening	SIEM analysis		Vulnerability Scanning, 3 months Assessment, 12 months
1	1	0	Dedicated segment				SIEM analysis		Vulnerability Scanning, 3 months Assessment, 24 months
PN	NE	VS							

# Problems of “Security Controls”

- Costs!



- Operational impact

- Business might feel obstructed.



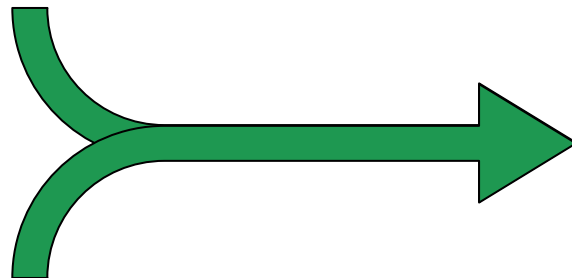
- Limitations



# Confidence



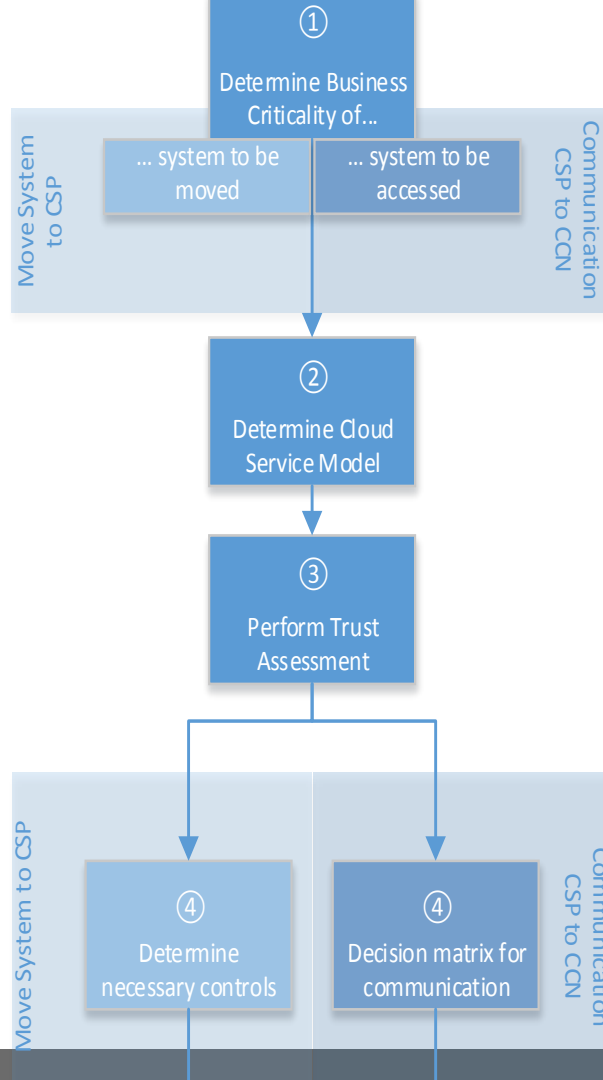
TRUST



CONTROL

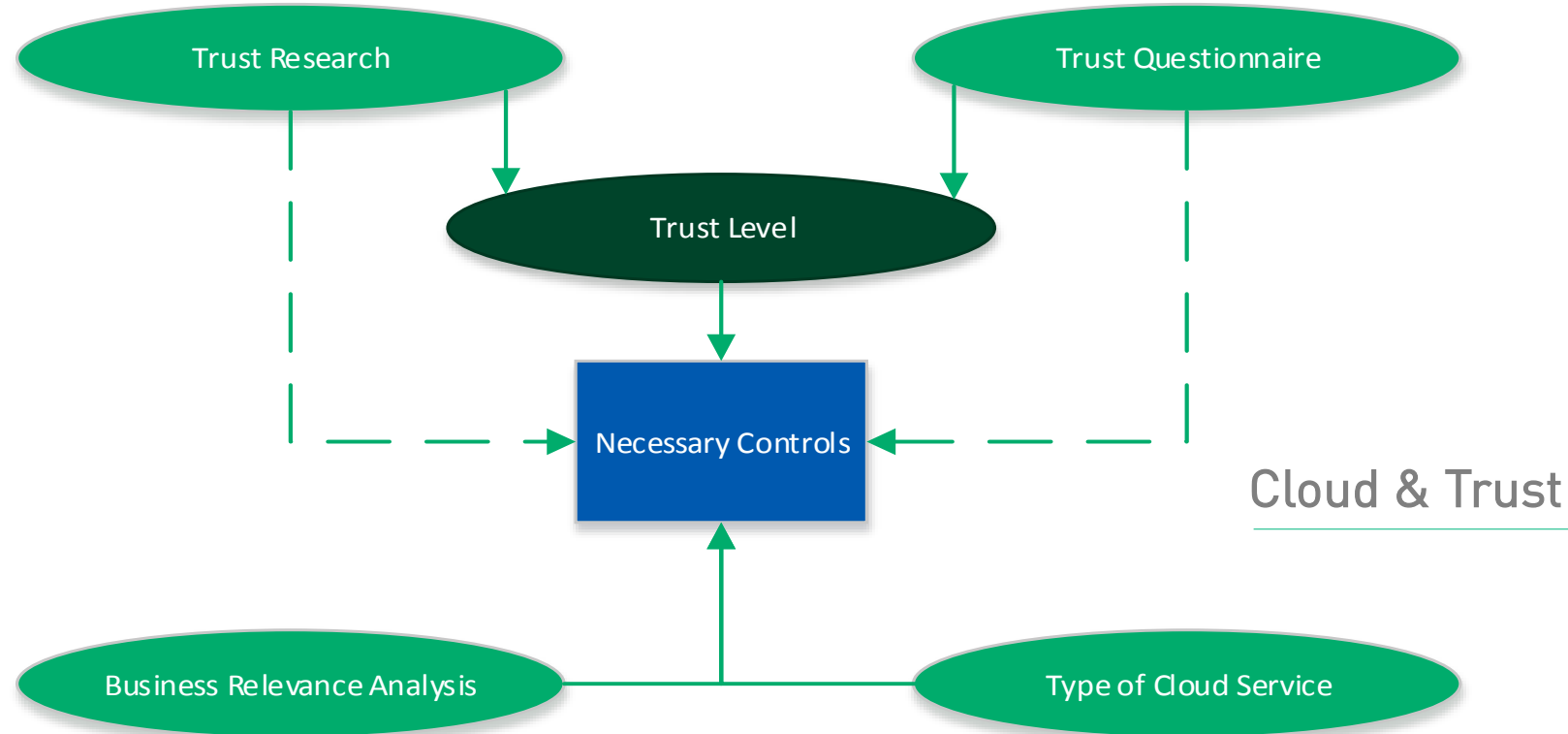
CONFIDENCE





## Cloud & Trust





## Conclusions



- Evaluate operational effort & security benefit.
- Question security best practices from a risk-based perspective.
- Evaluate trust as a source of confidence.
- Especially in very large VUCA environments!

# There's never enough time...

**Takk...**



@uchi\_mata



mluft@ernw.de



**...for yours!**

Slides & further information:  
<https://www.insinuator.net>  
(..soon)

# Disclaimer

---

All products, company names, brand names, trademarks and logos are the property of their respective owners!





# There are few things to know about TROOPERS:

**DATE:** March, 14 -18. 2016  
**PLACE:** Heidelberg, Germany  
**MISSION:** Make the world a safer place.



**REGISTRATION OPEN:** [www.troopers.de](http://www.troopers.de)

## The Archive



Jeff Gough at TROOPERS13

- Feel the spirit – TROOPERS13 Teaser:  
<https://www.youtube.com/watch?v=lfBo48r-Qho>



- TROOPERS13 Talks:
  - Videos:  
<http://www.youtube.com/playlist?list=PL1eoQr97VfJl1LdMzyQPz71uR6bwiUGog>
  - Slides: <https://www.troopers.de/archives/index.html>
- We hope to see you in 2016!