

Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations

Sathya Chandran Sundaramurthy
University of South Florida





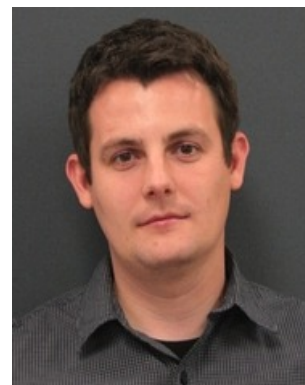
Long Term Anthropological Study of Security Operation Centers (SOCs)



Sathya Chandran Sundaramurthy
University of South Florida



Xinming (Simon) Ou
University of South Florida



Alexandru G. Bardas
Kansas State University



Yuping Li
University of South Florida



Loai Zomlot
Kansas State University
(Alumnus)



Jacob Case
Kansas State University
(Alumnus)



Michael Wesch
Kansas State University



John McHugh
RedJack, LLC



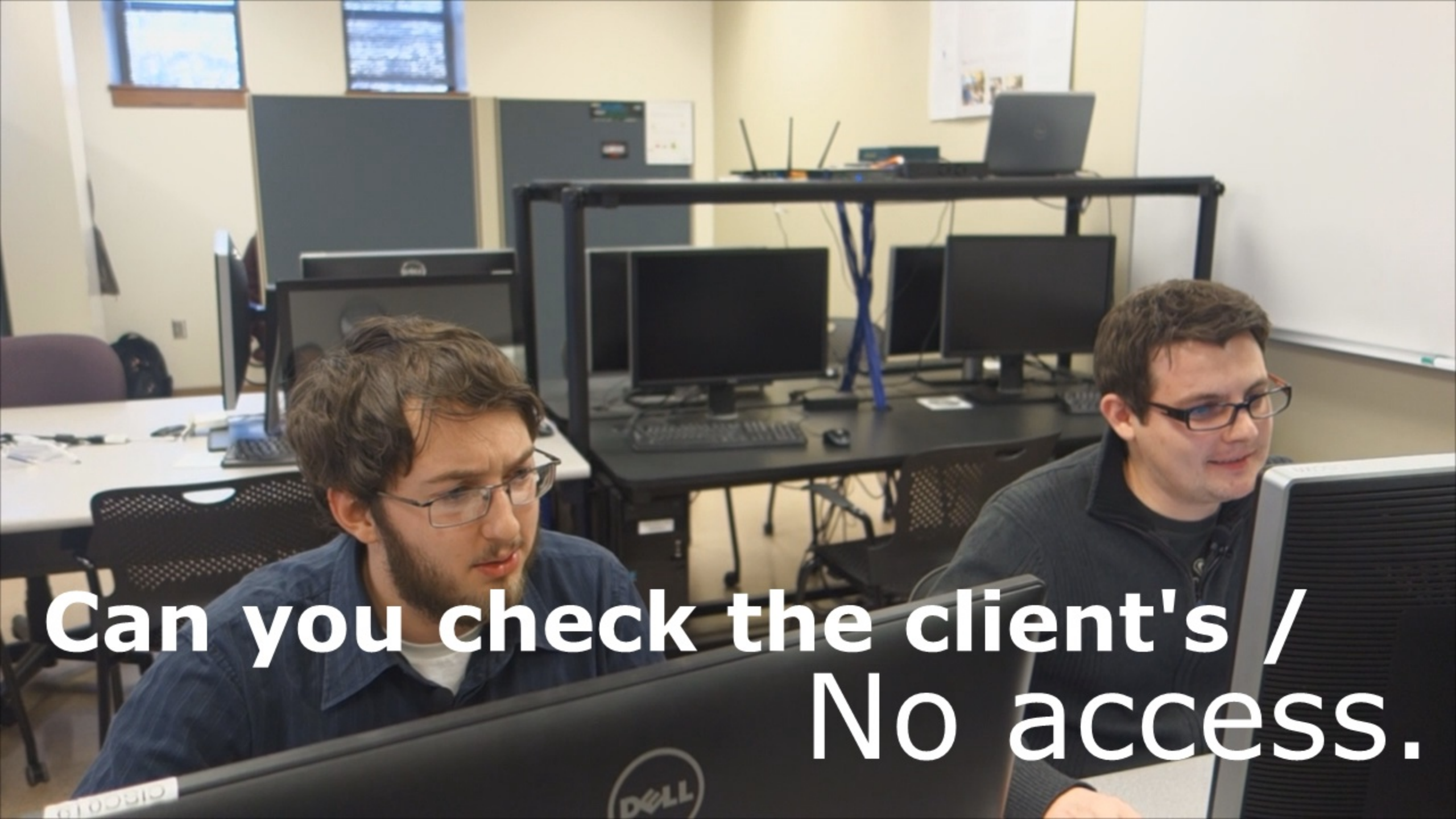
Raj Rajagopalan
Honeywell ACS Labs



A man with brown hair, a beard, and glasses is sitting at a desk in a server room. He is wearing a blue button-down shirt over a white t-shirt. He is looking at a Dell monitor. In the background, there are several other computer workstations with monitors and keyboards. The room has a blue and white color scheme.

escalate





**Can you check the client's /
No access.**

A man with short brown hair and black-rimmed glasses is smiling and looking down, likely at a computer screen. He is wearing a dark blue or black ribbed sweater. The background shows a server room or office environment with several computer monitors on desks, some with blue cables hanging from them. The lighting is somewhat dim, typical of an indoor office space.


The IP tables was blocking the loopback interface and their tools couldn't communicate

manager

Did you document that?



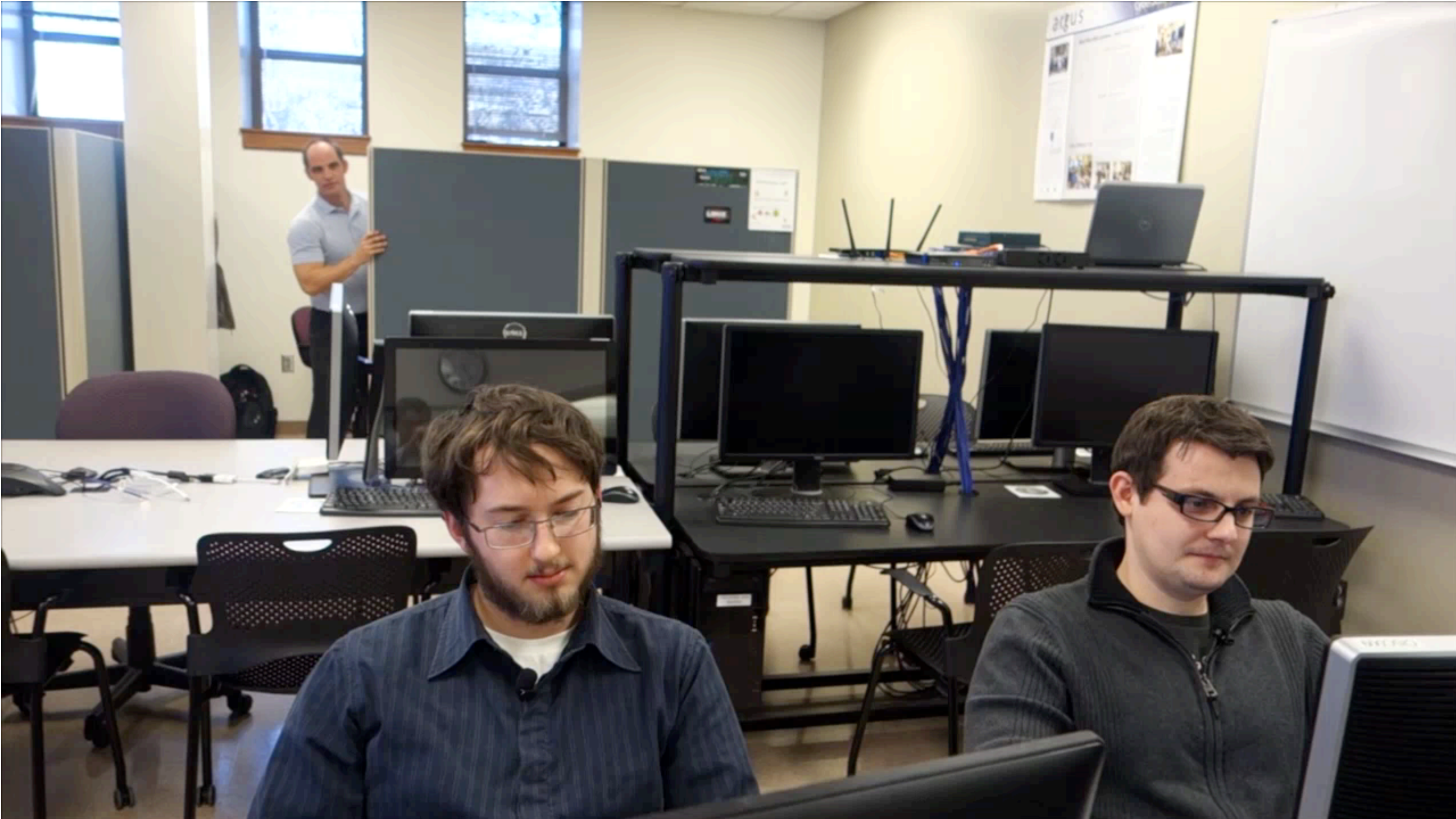




manager

Did you document that?








We need to help them.

But How?

Malware Incident Response


Network		Network Data		Submit Create Change Create Problem New Incident Queue Incident Save	
ID Number:	INC0000000	Incident area:	New		
Color:	[Redacted]	Assignment group:	Network		
Name:	[Redacted]	Assigned to:	[Redacted]		
Location:	[Redacted]	Priority:	A - High		
Business Service:	Security(Non-Prod)	Urgency:	A - High		
Device:	N/A	Operational hours:	PRODUCTION 11:00 PM		
Category:	IT Services	Opened by:	[Redacted]		
Subcategory 1:	Network core activity	Evaluation:	Normal		
Subcategory 2A:	Core Netw	Watch list:	[Add] [Remove]		
Status:	Pending	Problem ID:	[Redacted]		
Short description (viewable to user):	[Redacted]				
Description (viewable to user):					
<p>Hansen type ID security Zirconium network blockage @ different time incident ticket: 2015-07-20 11:03:36 or afterwards: 10:20:20-44 User: administrator - powerPC Building: Network 1 Dept: Network Expected resolution: Network acknowledgment of power disruption Note: Resolution ability reported by short alerts and confirmed with log files.</p>					
Additional Comments (viewable to user):					
[Green Bar]					
Work notes:					
<p>Network team, please block 90.4c.wd.47.01.95 on all networks and send the following email to SUITE CONTACTS when completed. Subject: Network Block Notification: Network 1 The following console appears to be related with Zirconium, as reported to [Redacted]. It has been blocked from the network. Knowledge</p>					
Submit Create Change Create Problem Print Report Resolve Incident Save					

 soc@ren-isac.net via [redacted]
 to [redacted]
 Greetings
 The following host(s) have been identified as the ZeroAccess Trojan.

Inc #	description	address	timestamp	s-prt	dest-addr	d-prt
VB8A	ZeroAccess	[redacted]	014-09-11T18:38:01Z	53769	184.176.138.83	16465

 key: s-prt = source port; prtcl = protocol;
 All the data that we have for each observation is provided. If data such as source port, destination address, etc, is not provided, then we don't have that data. We may have additional observations collected during the reporting period, value depending on multiple factors (NATing, source port availability, etc.)
 If you feel you've received this report in error, please let us know.
 Additional information regarding ZeroAccess Trojan is provided below.
 In order for the REN-ISAC to learn how we can best aid the education community with network security matters we'd greatly appreciate hearing back from you regarding action on this incident and how, if at all, this information proved useful.
 Research and Education Networking ISAC
 24x7 Watch Desk: +1(317)278-6630, soc@ren-isac.net
<http://www.ren-isac.net>

Jul
 Jul
 Jul
 Jul
 Jul
 Jul
 Jul
 Jul
 Jul

 soc@ren-isac.net via [redacted]
 to [redacted]

Malware Incident Response

Greetings

The following host(s) have been identified as likely compromised with the ZeroAccess Trojan.

Inc #	description	address	timestamp in UTC	s-prt	dest-addr	d-prt
VB8A	ZeroAccess	[redacted]	014-09-11T18:38:01Z	53769	184.176.138.83	16465

key: s-prt = source port; prtcl = protocol; dest-addr = destination address; d-prt = destination port

All the data that we have for each observation is provided. If data such as source port, destination address, etc, is not provided, then we don't have that data. We may have additional observations collected during the reporting period, value depending on multiple factors (NATing, source port availability, etc.)

If you feel you've received this report in error, please let us know.

Additional information regarding ZeroAccess Trojan is provided below.

In order for the REN-ISAC to learn how we can best aid the education community with network security matters we'd greatly appreciate hearing back from you regarding action on this incident and how, if at all, this information proved useful.

Research and Education Networking ISAC
 24x7 Watch Desk: +1(317)278-6630, soc@ren-isac.net
<http://www.ren-isac.net>

Malware Incident Response

soc@ren-isac.net via [REDACTED]
to [REDACTED]

Greetings

The following host(s) have been identified as likely compromised with the ZeroAccess Trojan.

Inc #	description	address	timestamp in UTC	s-prt	dest-addr	d-prt
VB8A	ZeroAccess	[REDACTED]	014-09-11T18:38:01Z	53769	184.176.138.83	16465

key: s-prt = source port; prtcl = protocol; dest-addr = destination address; d-prt = destination port

All the data that we have for each observation is provided. If data such as source port, destination address, etc, is not provided, then we don't have that data. We may have additional observations collected during the reporting period, value depending on multiple factors (NATing, source port availability, etc.)

If you feel you've received this report in error, please let us know.

Additional information regarding ZeroAccess Trojan is provided below.

In order for the REN-ISAC to learn how we can best aid the education community with network security matters we'd greatly appreciate hearing back from you regarding action on this incident and how, if at all, this

```
Jul 23 11:44:36 source dhcpd: [ID 702911 local5.info] DHCPACK to 10.131.253.44 (90:4c:e5:47:c5:95) via 10.131.248.15
Jul 23 11:44:42 source dhcpd: [ID 702911 local5.info] DHCPREQUEST for 10.131.253.44 from 90:4c:e5:47:c5:95 (Elle-PC) via 10.131.248.15
Jul 23 11:44:42 source dhcpd: [ID 702911 local5.info] DHCPACK on 10.131.253.44 to 90:4c:e5:47:c5:95 (Elle-PC) via 10.131.248.15
Jul 23 11:45:44 source dhcpd: [ID 702911 local5.info] DHCPACK to 10.131.253.44 (90:4c:e5:47:c5:95) via 10.131.248.15
Jul 23 11:46:45 source dhcpd: [ID 702911 local5.info] DHCPACK to 10.131.253.44 (90:4c:e5:47:c5:95) via 10.131.248.15
Jul 23 11:47:46 source dhcpd: [ID 702911 local5.info] DHCPACK to 10.131.253.44 (90:4c:e5:47:c5:95) via 10.131.248.15
Jul 23 11:48:56 source dhcpd: [ID 702911 local5.info] DHCPACK to 10.131.253.44 (90:4c:e5:47:c5:95) via 10.131.248.15
Jul 23 11:49:58 source dhcpd: [ID 702911 local5.info] DHCPACK to 10.131.253.44 (90:4c:e5:47:c5:95) via 10.131.248.15
Jul 23 11:51:04 source dhcpd: [ID 702911 local5.info] DHCPACK to 10.131.253.44 (90:4c:e5:47:c5:95) via 10.131.248.15
Jul 23 11:52:06 source dhcpd: [ID 702911 local5.info] DHCPACK to 10.131.253.44 (90:4c:e5:47:c5:95) via 10.131.248.15
```

Incident - Required Field

Number: INC00000000

Color: [REDACTED]

Topic: [REDACTED]

Location: [REDACTED]

Business Service: Security/Non-Private

Device: 90:4c:e5:47:c5:95

Category: IT Security

Subcategory 1: Address cache activity

Subcategory 2: [REDACTED]

Status: Resolved

Incident state: New

Assignment group: Network

Assigned to: [REDACTED]

Priority: 4 - Low

Urgency: 4 - Low

Opened by: [REDACTED]

Opened on: 2014-09-11 11:00 PM

Escalation: Normal

Watch list: [REDACTED]

Problem ID: [REDACTED]

RPC: [REDACTED]

Short description (Shrinkable to save): [REDACTED]

Discussion (Shrinkable to save): [REDACTED]

Additional Comments (Shrinkable to save): [REDACTED]

Work notes: [REDACTED]

Network team: please check 90:4c:e5:47:c5:95 on all networks and send the following email to BIRT CONTACTS when completed.

Subject: Network Block Notification - Natakulturn 8

Body: The following computer appears to be infected with ZeroAccess, as reported to [REDACTED]. It has been blocked from the network.

Knowledge: [REDACTED]

Buttons: Submit, Create Change, Create Problem, Print Preview, Resolve Incident, Save

Malware Incident Response

soc@ren-isac.net via [REDACTED]

to [REDACTED]

Greetings

The following host(s) have been identified as likely compromised with the ZeroAccess Trojan.

| Inc # | description | address | timestamp in UTC | s-prt | dest-addr | d-prt |

| VB8A | ZeroAccess | [REDACTED] | 014-09-11T18:38:01Z | 53769 | 184.176.138.83 | 16465 |

Incident = Required field

Submit Create Change Create Problem Print Preview Resolve Incident Save

Number: INC0153559

Caller: [REDACTED]

Name: [REDACTED]

Location: [REDACTED]

Business Service: Security(Non-Private)

Device: PC

Category: IT Security

Subcategory 1: Malicious code activity

Subcategory 2a: -- None --

Source: Monitoring

Incident state: New

Assignment group: Network

Assigned to: [REDACTED]

Priority: 4 - Low

Urgency: 4 - Low

Opened: 07/25/2013 11:00 PM

Opened by: [REDACTED]

Escalation: Normal

Watch list: [REDACTED]

Problem ID: [REDACTED]

RFC: [REDACTED]

Short description (Viewable to user): [REDACTED]

Description (Viewable to user):

Malware type (if known): ZeroAccess
Date/time identified (if different from incident ticket): 2013-07-23 11:53:35
IP address(es): 10.131.253.44
MAC address(es): [REDACTED]
Domain/hostname: Elle-PC
Building: Natatorium 8
Dept: Kinesiology
Contact person: [REDACTED]
Expected resolution: Reformat/rebuild
elDname/addr of owner, if known: [REDACTED]
Notes: Malicious activity reported by Snort alerts and confirmed with flow data.

Additional Comments (Viewable to user):

Work notes:

Network team, please block 90:4c:e5:47:c5:95 on all networks and send the following email to SIRT-CONTACTS when completed.
Subject: Network Block Notification - Natatorium 8
Body:
The following computer appears to be infected with ZeroAccess, as reported to [REDACTED]. It has been blocked from the network.
Knowledge: [REDACTED]

Submit Create Change Create Problem Print Preview Resolve Incident Save

Notes: Malicious activity reported by Snort alerts and confirmed with flow data.

Additional Comments (Viewable to user):

Work notes:

Network team, please block 90:4c:e5:47:c5:95 on all networks and send the following email to SIRT-CONTACTS when completed.
Subject: Network Block Notification - Natatorium 8
Body:
The following computer appears to be infected with ZeroAccess, as reported to [REDACTED]. It has been blocked from the network.
Knowledge: [REDACTED]

Submit Create Change Create Problem Print Preview Resolve Incident Save

10 minutes/alert

10 minutes/alert
X 15 alerts/day

10 minutes/alert

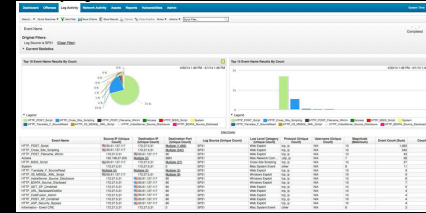
X 15 alerts/day

= over 2 hours/day

Usefulness

Compliance

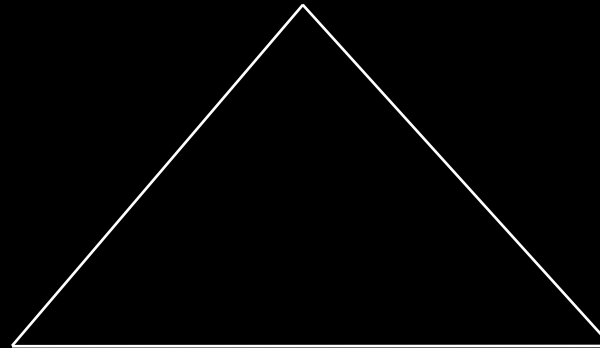
*Software, Skills
(Tools)*



Creativity

Adherence

Analyst

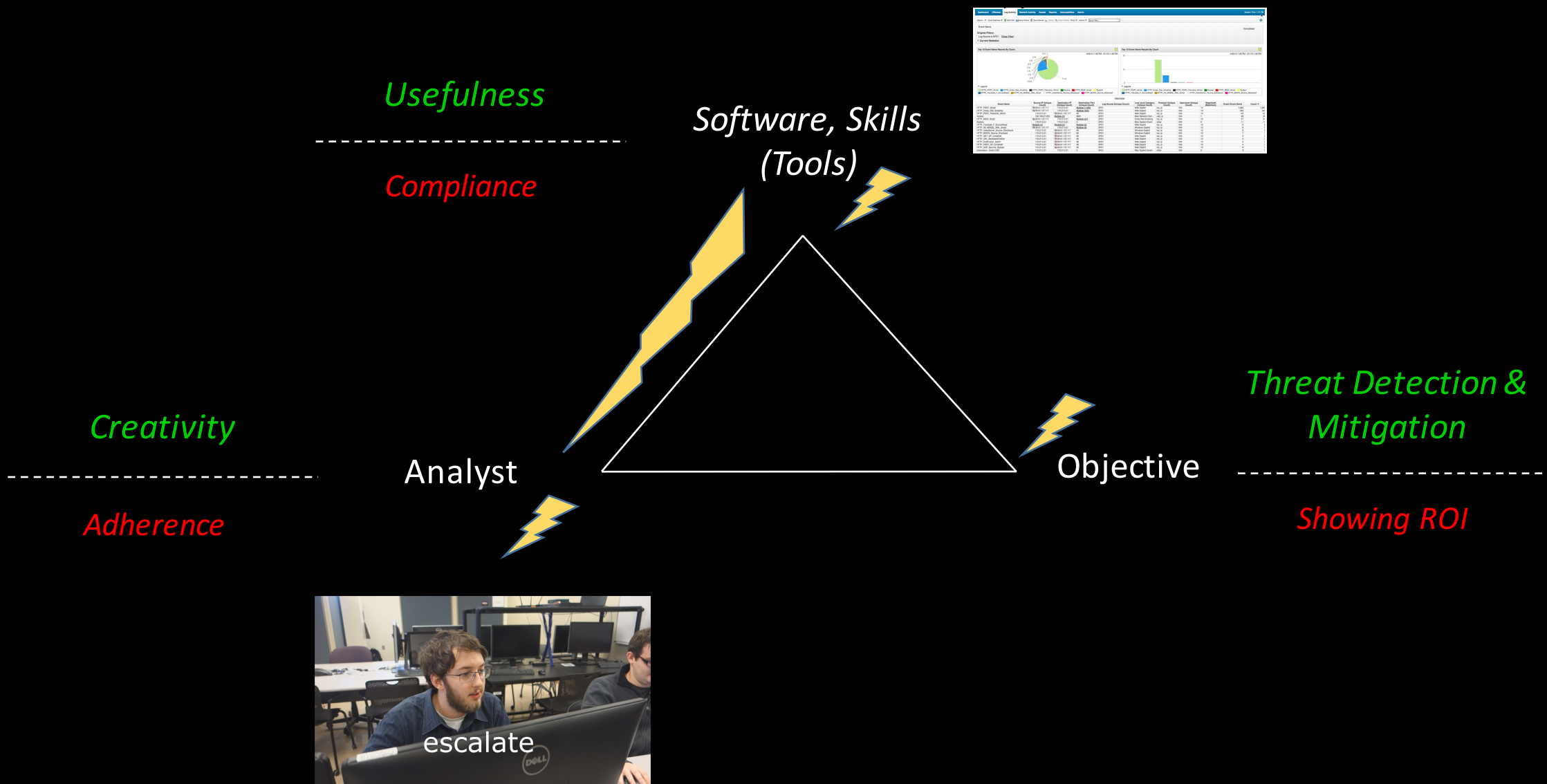


Objective

*Threat Detection &
Mitigation*

Showing ROI





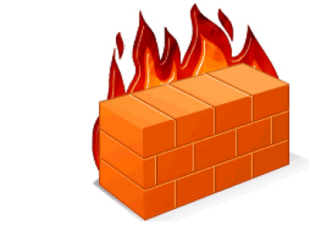
Access point
Logs



ARP Logs



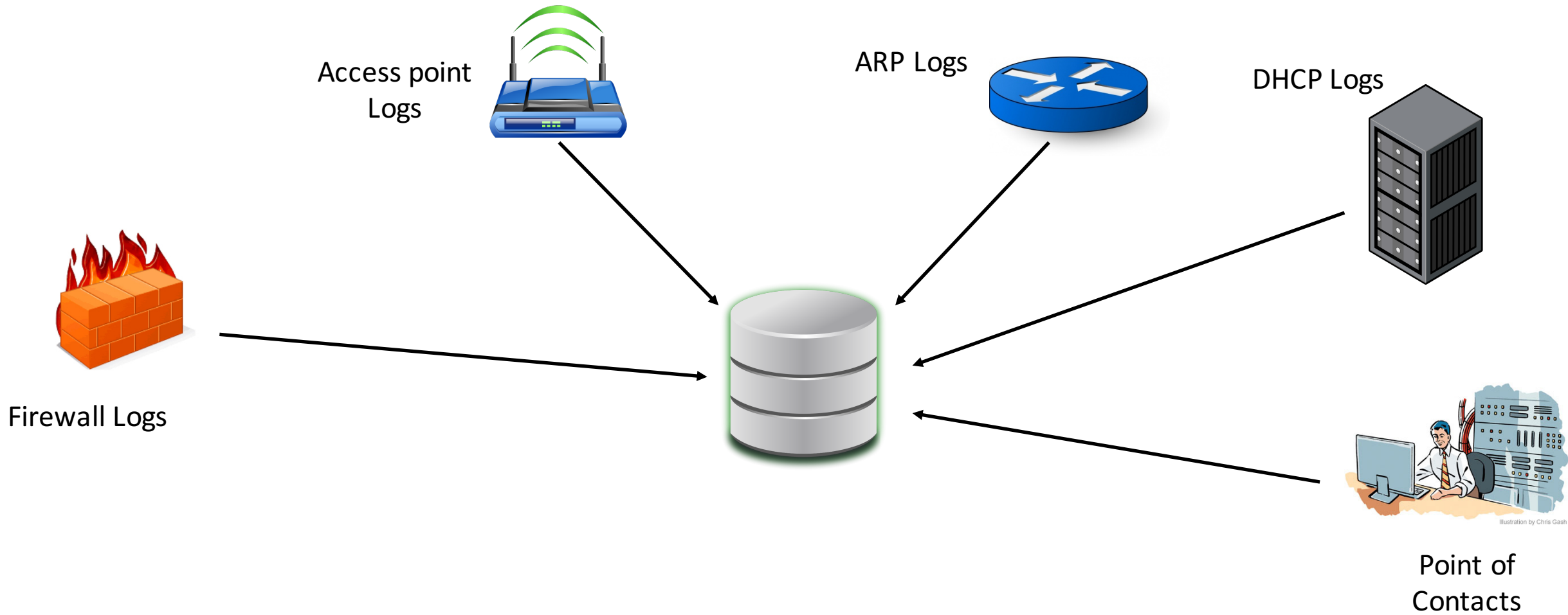
DHCP Logs

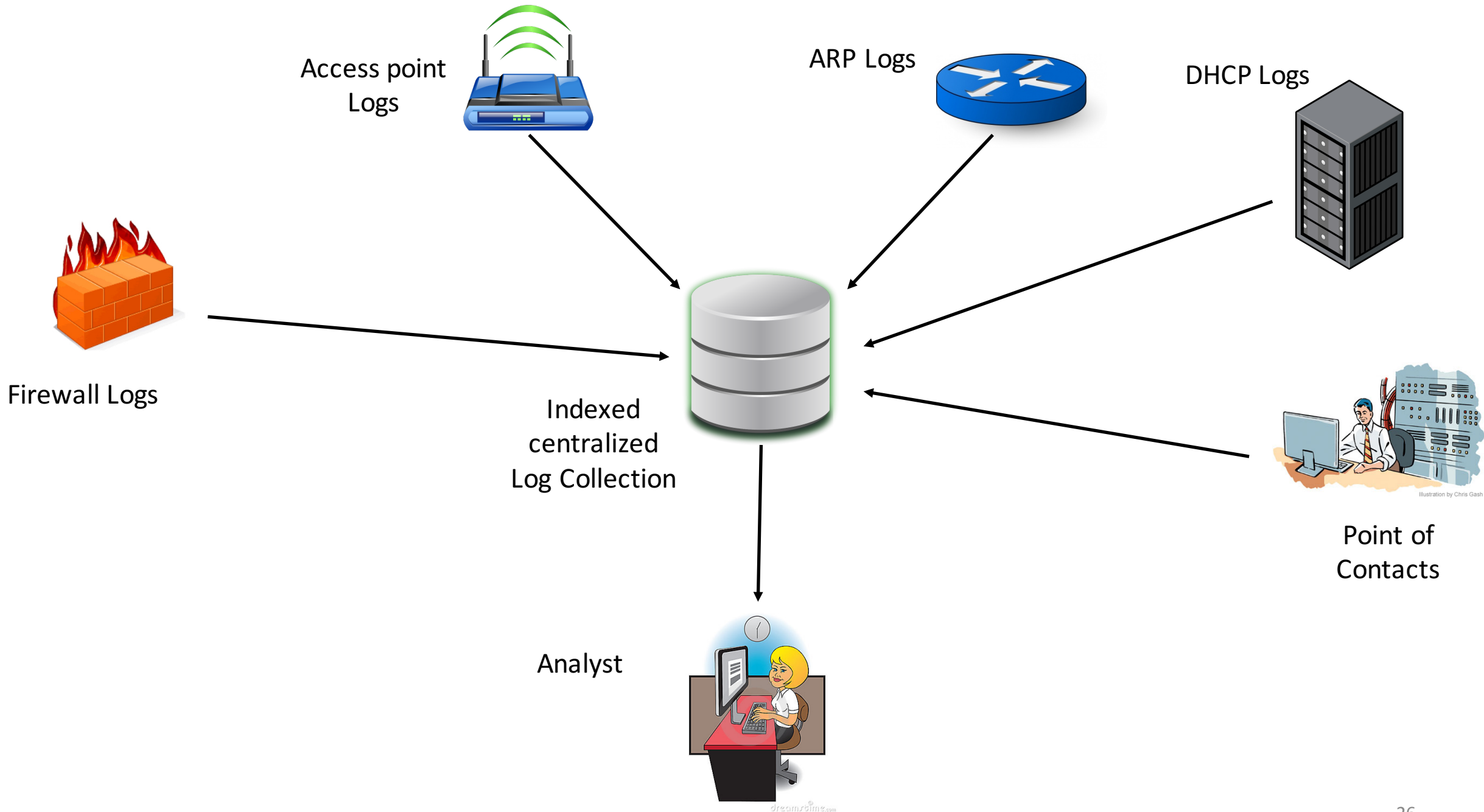


Firewall Logs

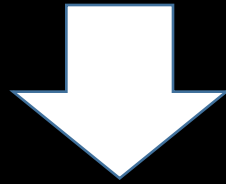


Point of
Contacts



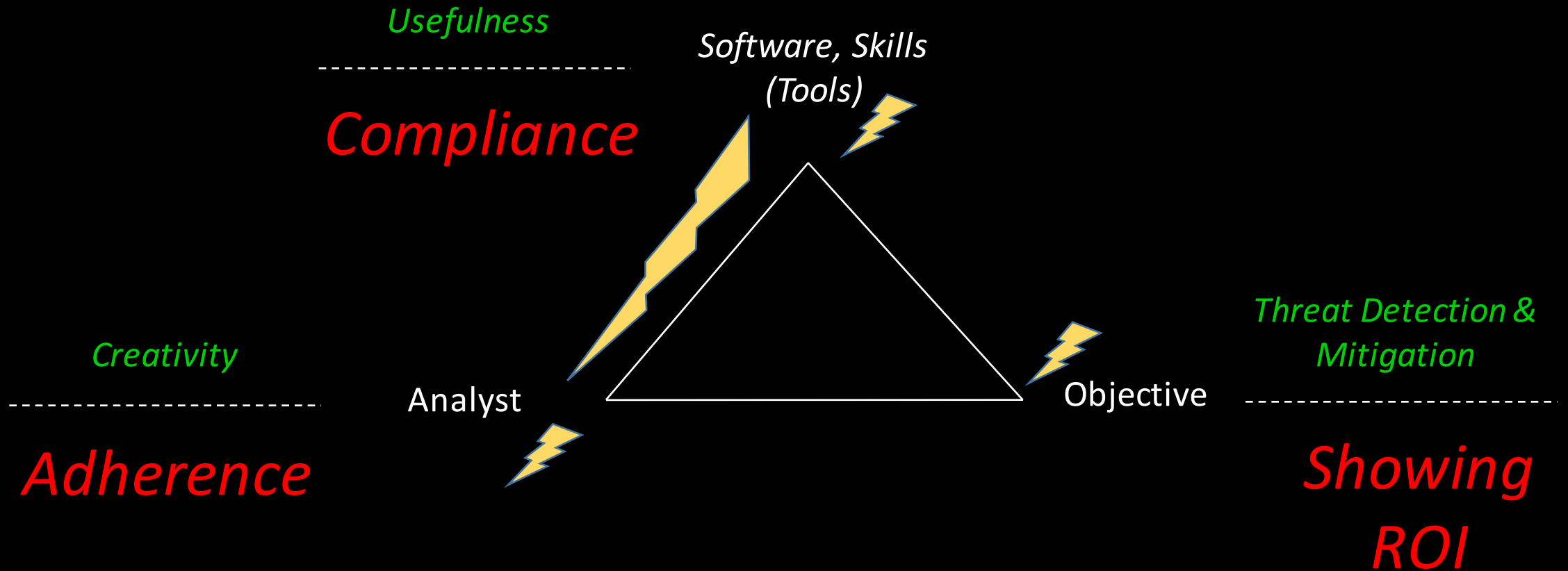


10 minutes / alert

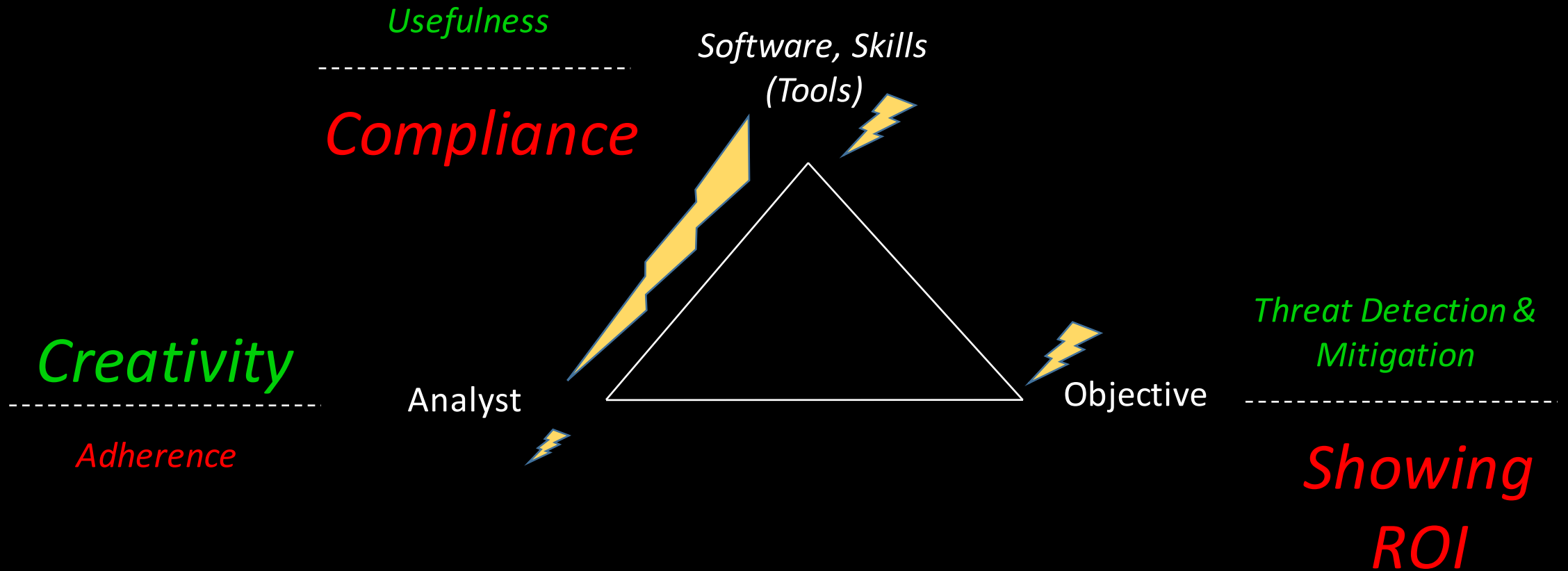


10 secs / alert

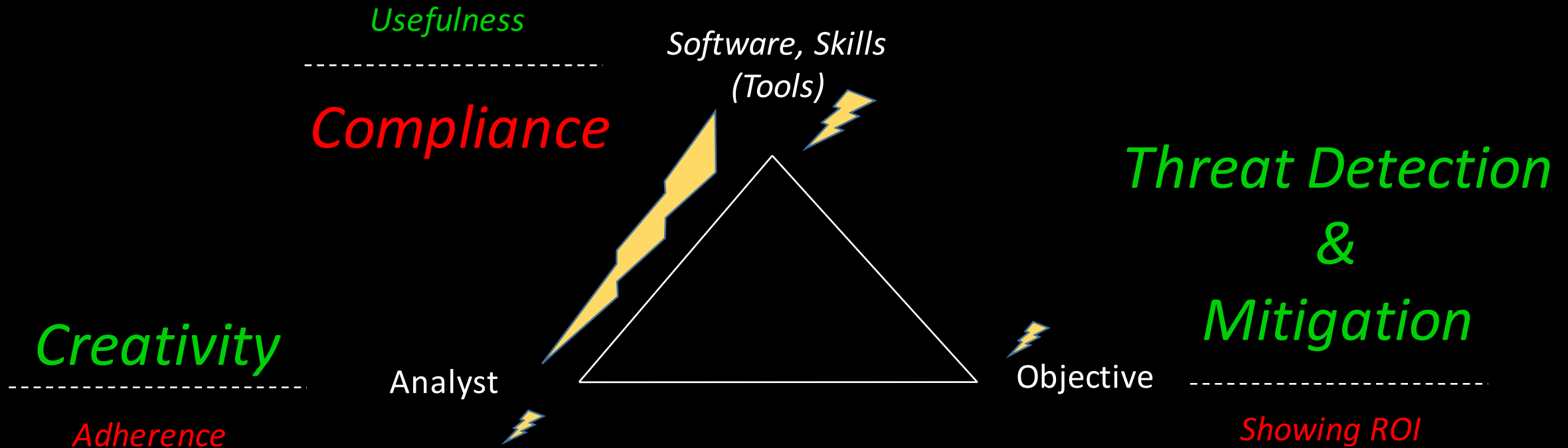
Before ...



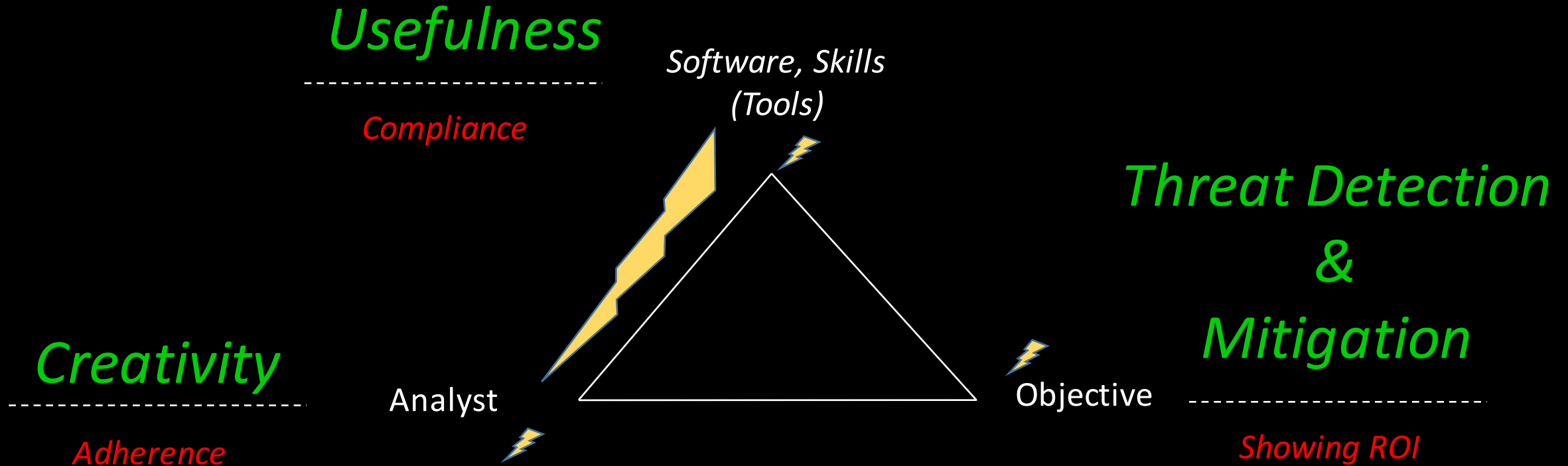
After ...



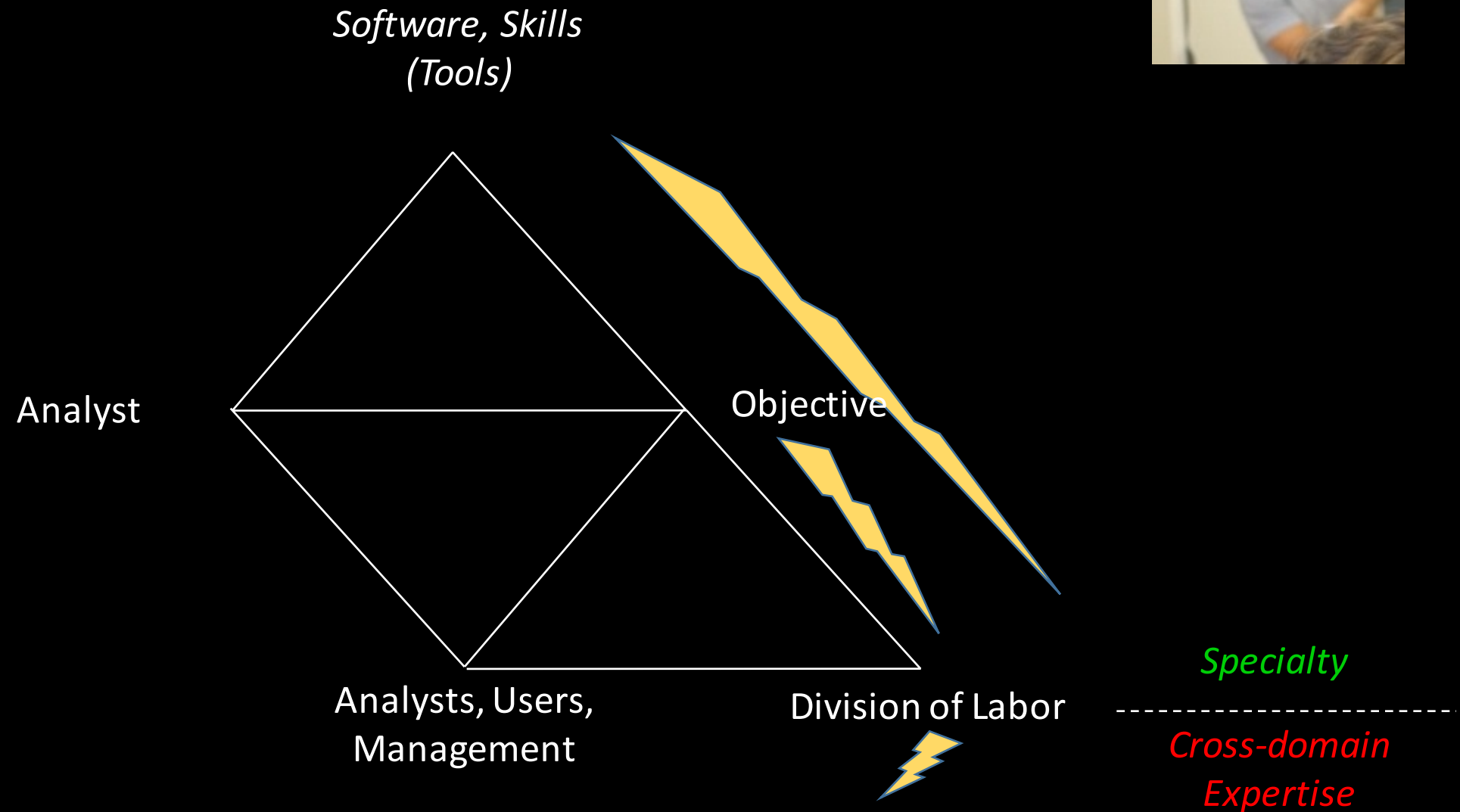
After ...



After ...

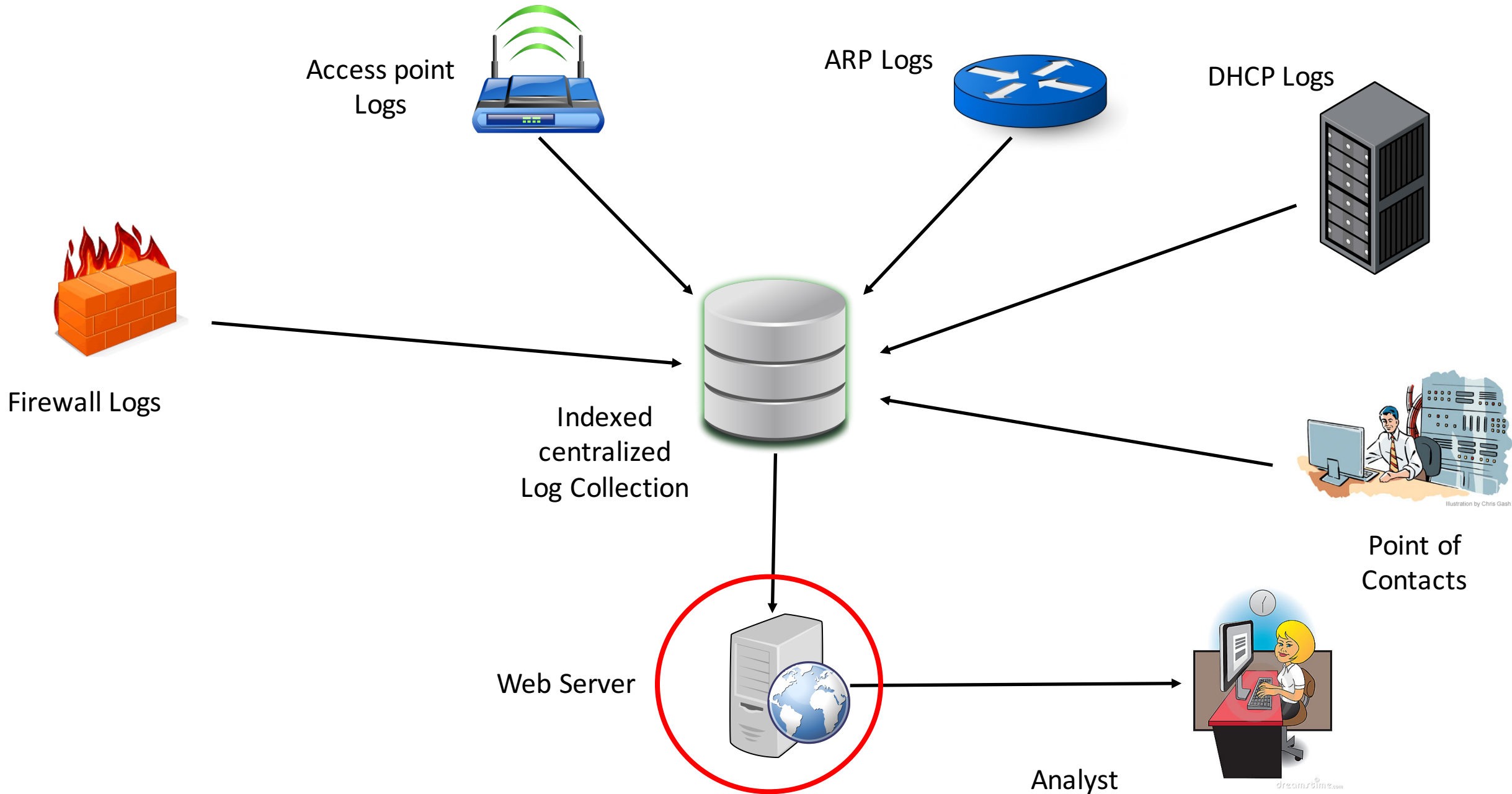


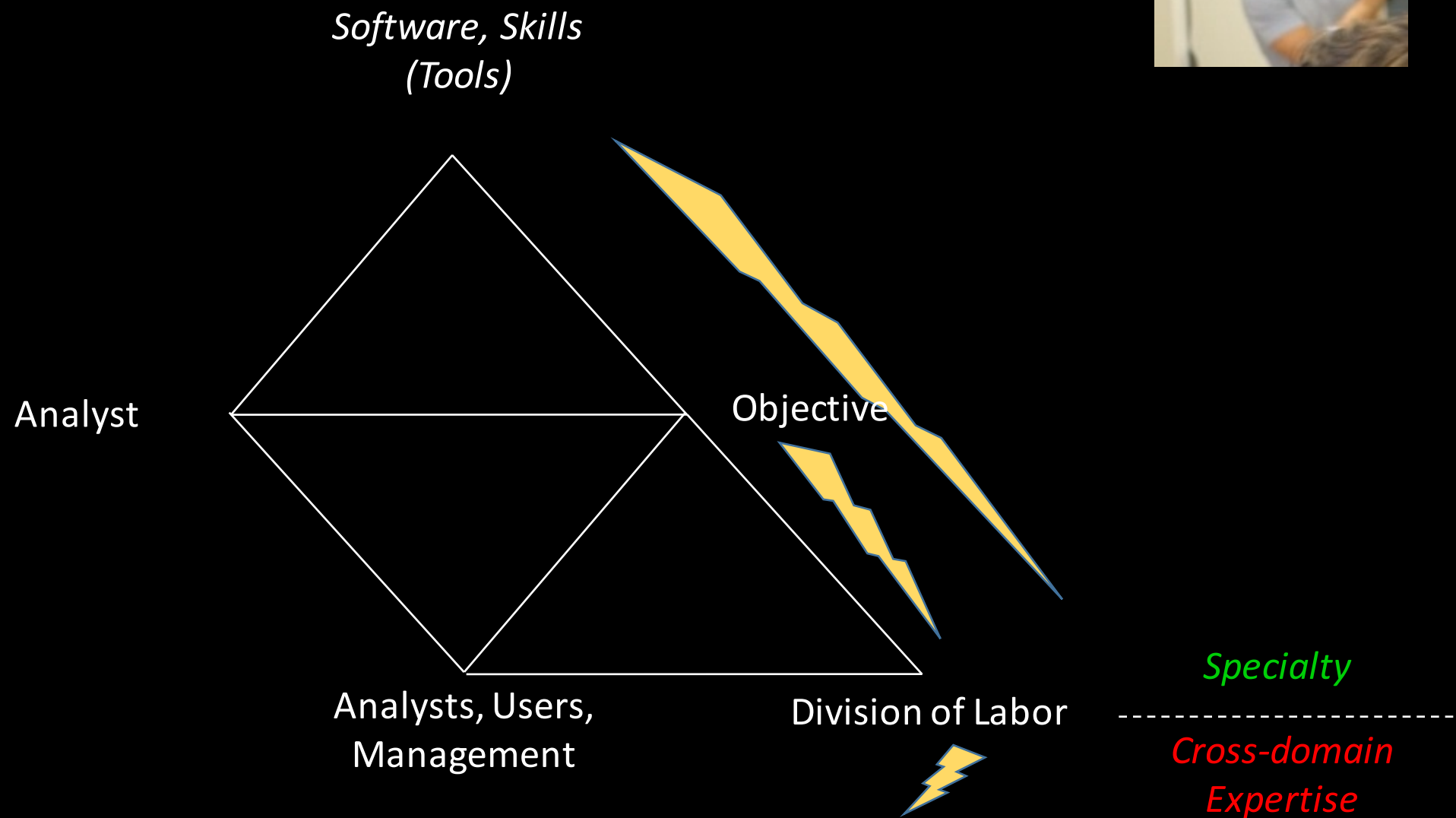
The Saga Continues ...

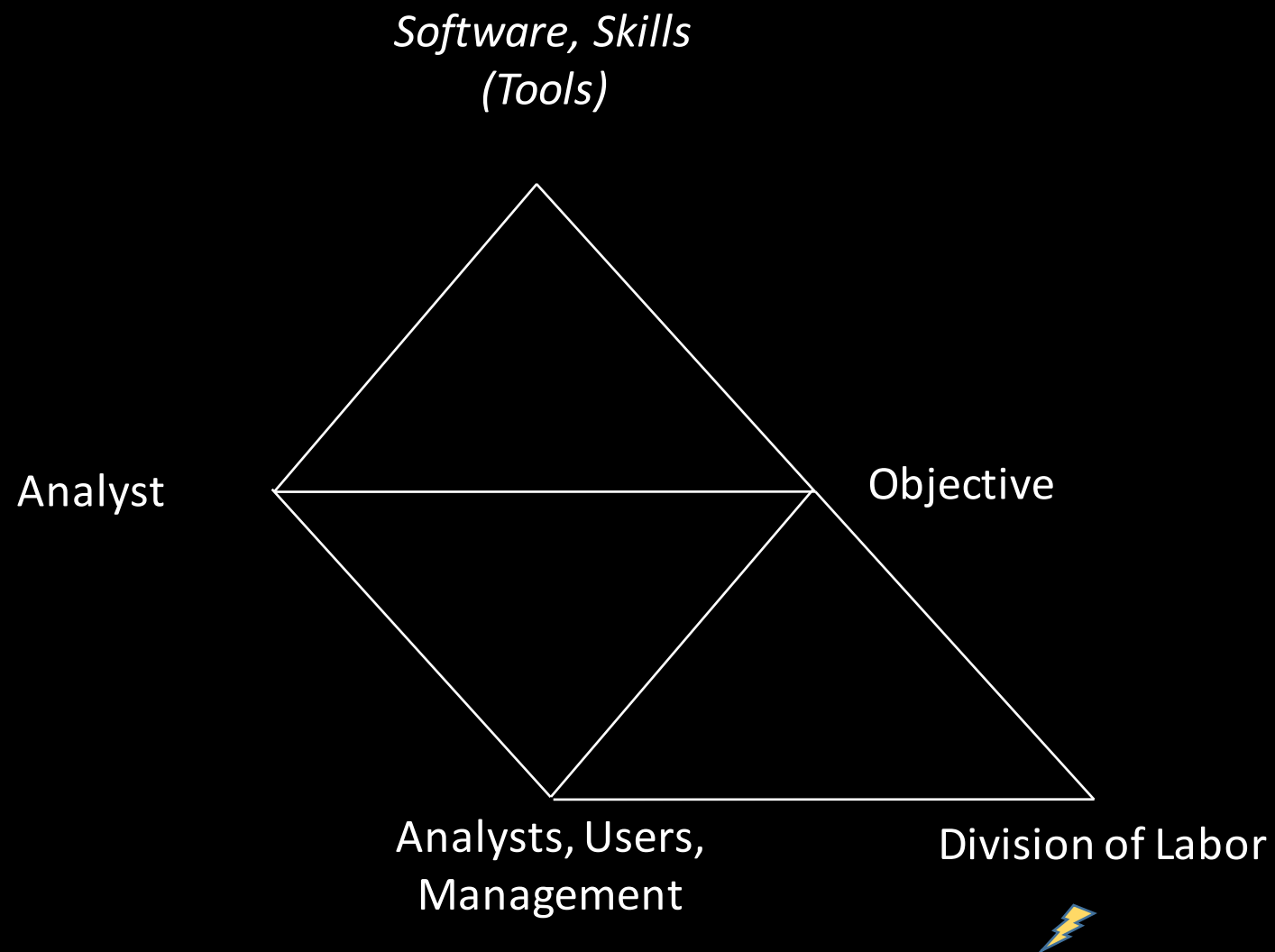


The deployment of our tool
revealed more conflicts!

Conflicts Create Opportunities for Innovation!







Specialty

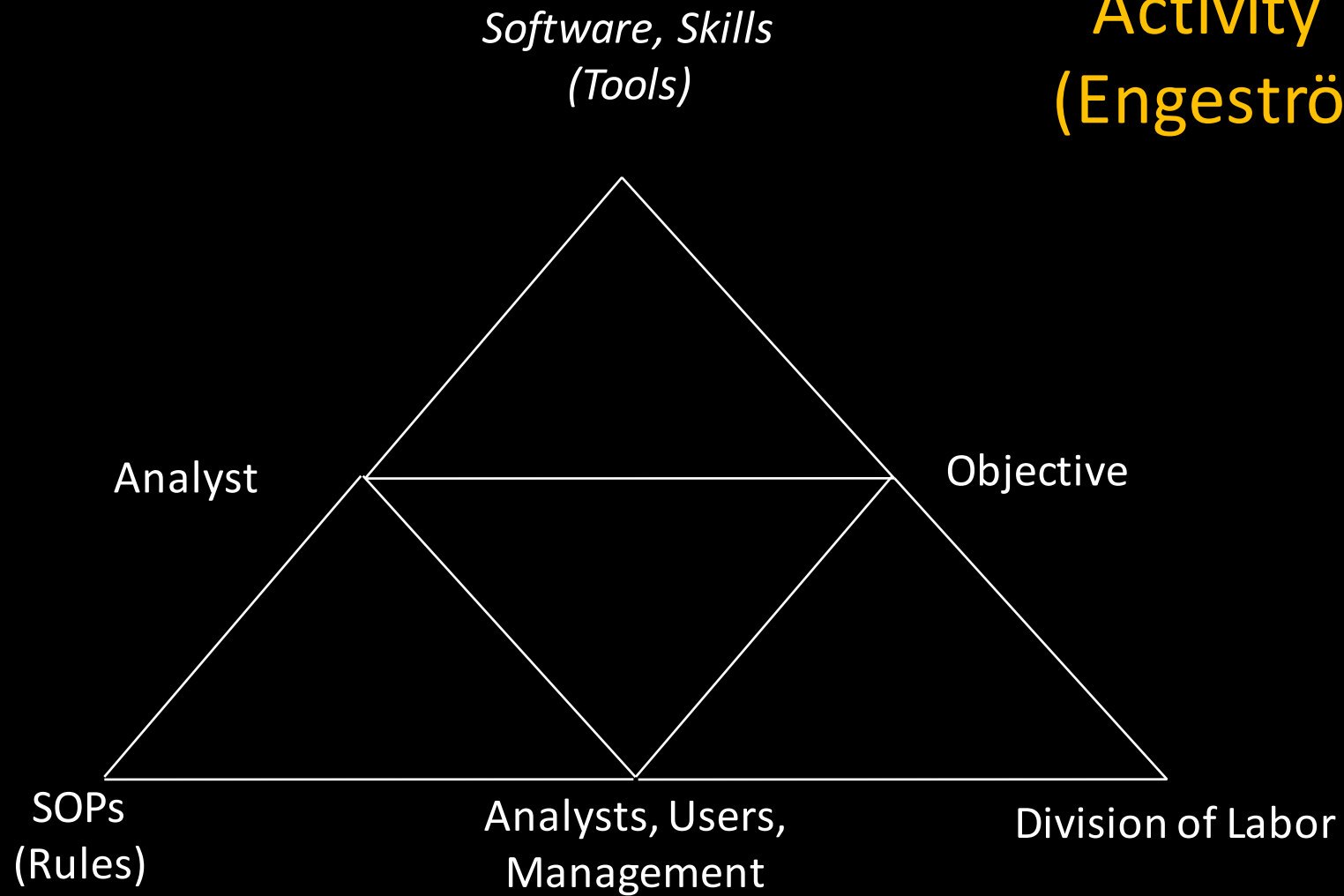
*Cross-domain
Expertise*

A SOC is a dynamic system.

More conflicts will keep arising.

They have to be resolved on a continuous basis.

Activity Theory (Engeström 1987)



These Insights are a result of

- 3.5 years of fieldwork
- At 4 different SOC's
- Involving 4 graduate students and 1 undergraduate student as fieldworkers
- Following systematic data analysis technique
 - Template analysis

A man in a light blue polo shirt stands in the background of an office, pointing his right index finger towards a computer monitor. In the foreground, two men are seated at desks. The man on the left has a beard and glasses, wearing a dark blue button-down shirt. The man on the right wears glasses and a dark grey zip-up jacket. They are both looking towards the monitor being pointed at. The office environment includes multiple computer workstations with monitors, keyboards, and mice. A whiteboard is visible on the right wall, and windows are in the background.

Is that compliant?

Tensions & contradictions are gifts
if we allow ourselves to see them.