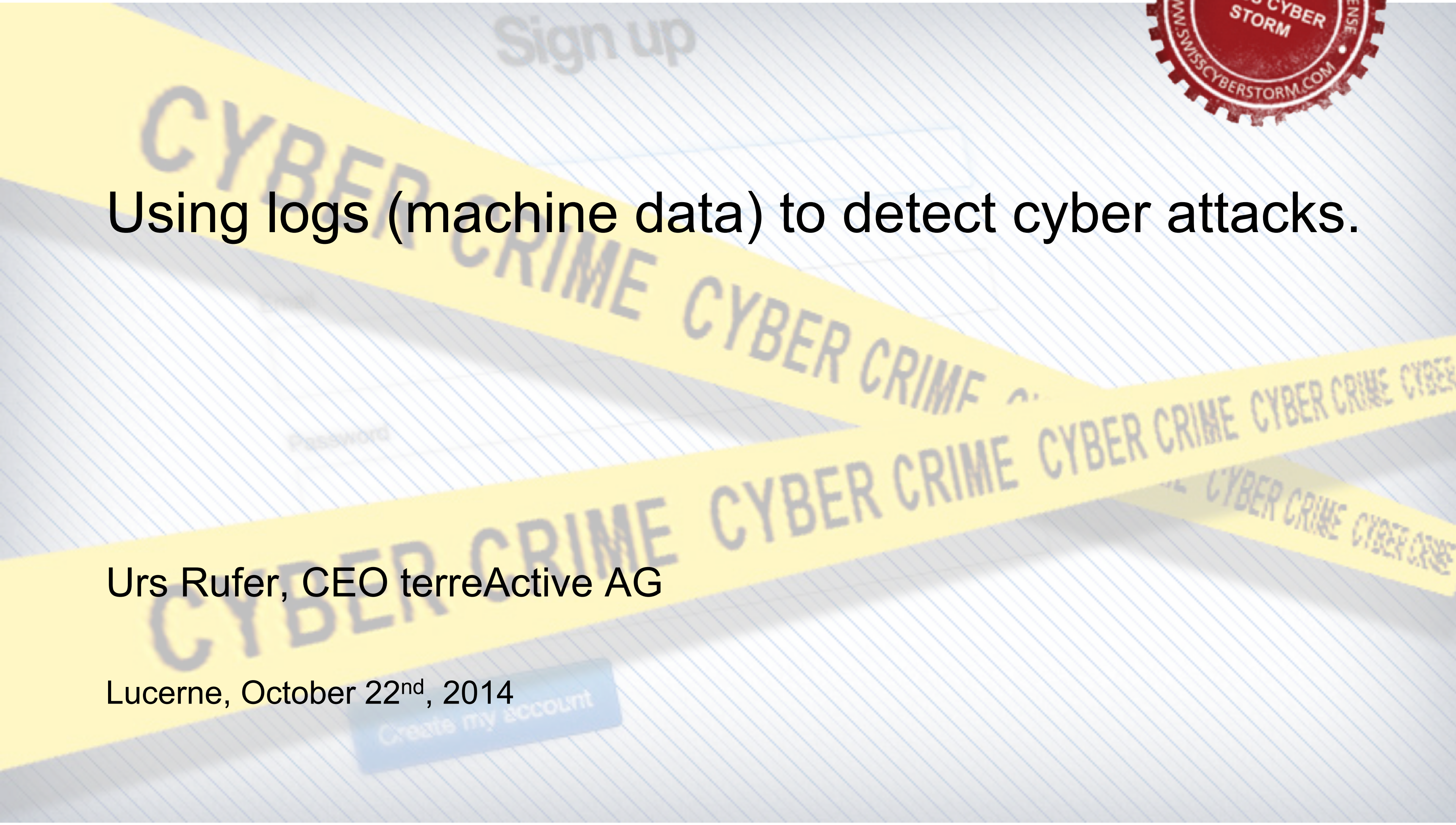
CYBER ATTACKS AND DEFENSE
SWISS CYBER STORM
WWW.SWISSCYBERSTORM.COM



Using logs (machine data) to detect cyber attacks.

Urs Rufer, CEO terreActive AG

Lucerne, October 22nd, 2014

Swiss Cyber Storm 5.
Agenda.

- About terreActive.
- Prevention not possible?
- Monitoring / Detection strategies.
- Money saved: real world examples.
- Conclusion / Summary.

terreActive AG.
About us.

Positioning

- IT security consulting and operation (MSS) as core competency
- Trusted partner for comprehensive and sustainable IT security solutions

Facts

- Founded in April 1996 - over 18 years of competency in IT security
- Swiss company
- 40 employees (30 engineers) in Aarau

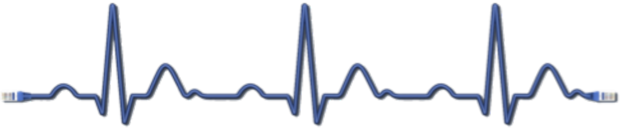
Profile

- Independent and solution-oriented
- Services in IT security lifecycle
- MSS since 1997 – share of turnover approx 2/3

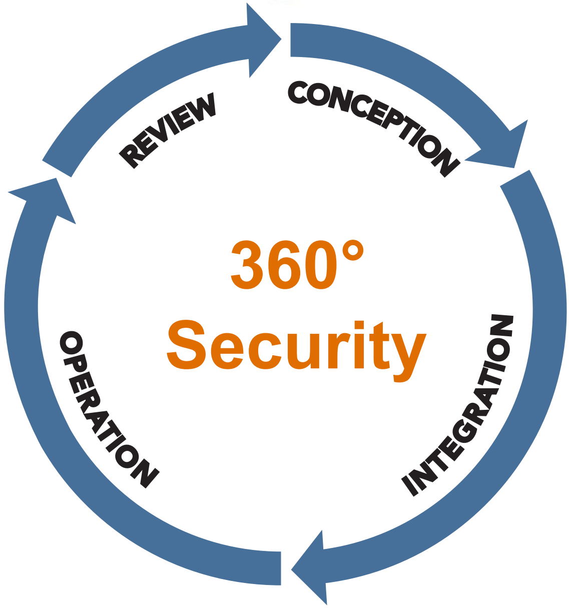
Customers

- Financial institutions (30%)
- Administration and organisations (30%)
- Telecom and IT service providers (20%)
- Industry and health services / Pharmaceuticals (20%)

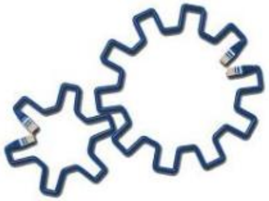
terreActive AG.
Our business segments.



Consulting



Operation



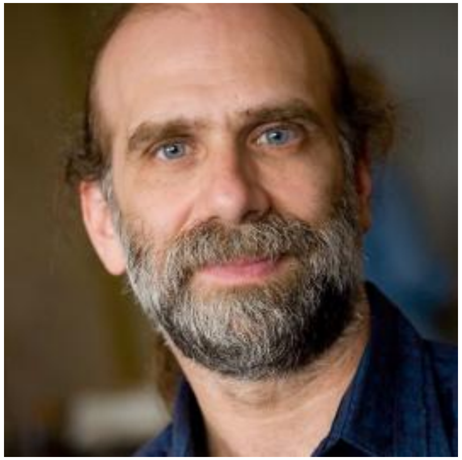
Integration

Development

tac
.ch

Swiss Cyber Storm 5.

Prevention not possible?



«You can’t defend.

You can’t prevent.

The only thing you can do is detect and respond.»

© by Bruce Schneier

Bruce Schneier is an American cryptographer, computer security and privacy specialist, and writer. He is the author of several books on general security topics, computer security and cryptography.

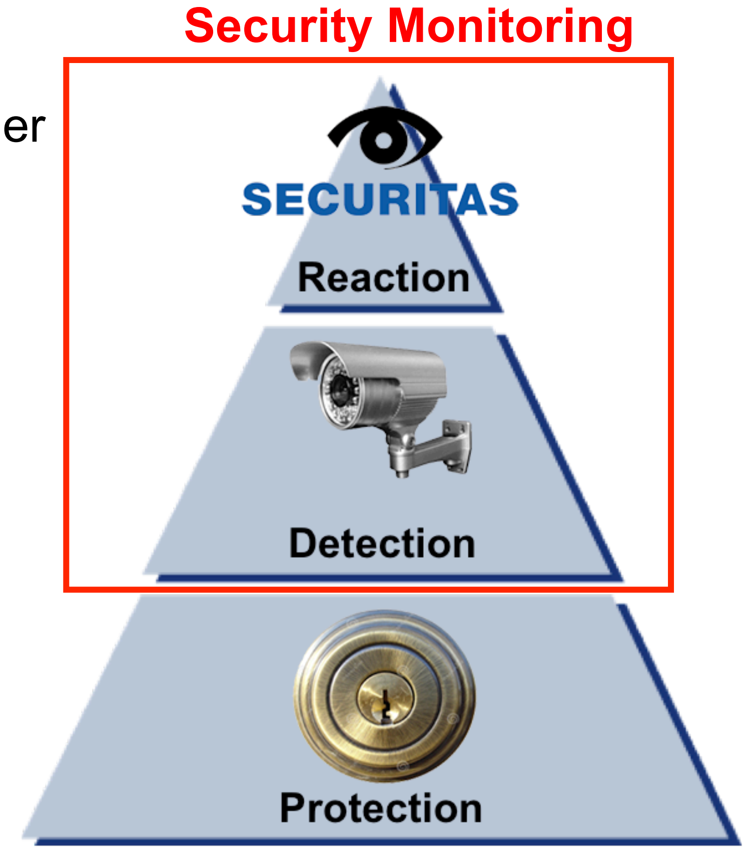
Swiss Cyber Storm 5.

Monitoring / Detection definition.

Information Security Monitoring is the process involving **collection**, **analysis**, and **escalation** of indications and warnings in order to detect, track and respond to **security threats**.

Security threats include attacks, intrusions, policy violations, data leakage, software vulnerabilities, denial of service.

Security Monitoring as continuous Risk-Assessment

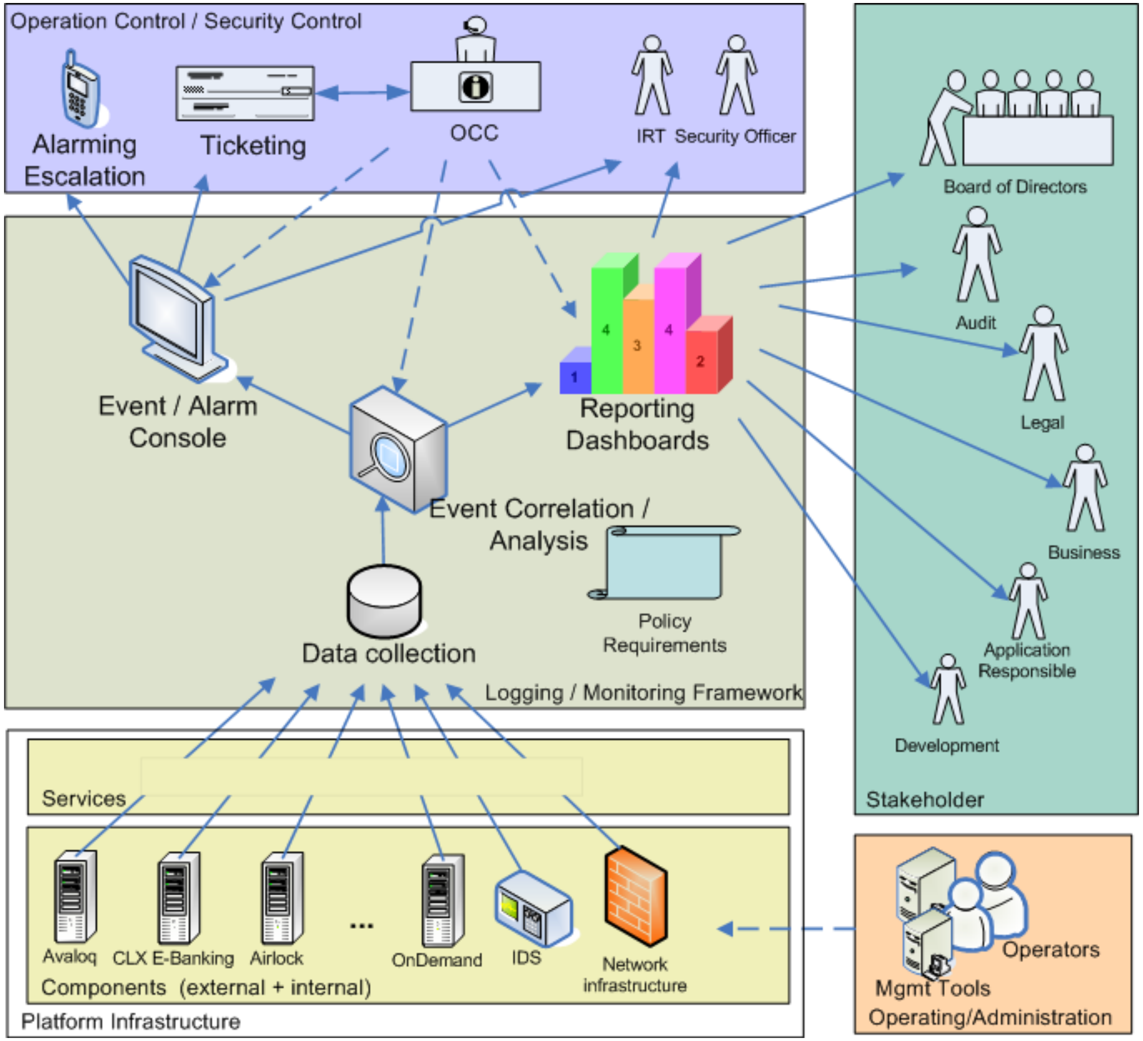


Security Architecture

Swiss Cyber Storm 5.
Monitoring / Detection strategies.

Monitoring Blueprint

- Alarming / Reaction
- Searching / Reporting
- Event correletion / analysis
- Data collection and processing
- Data sources



Swiss Cyber Storm 5.
Monitoring / Detection strategies.

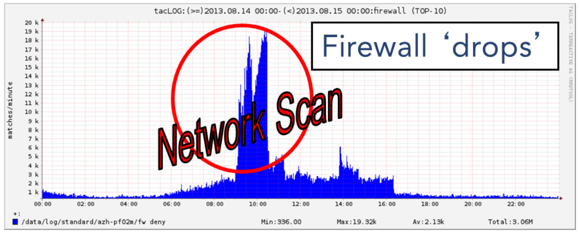
Data Sources Types

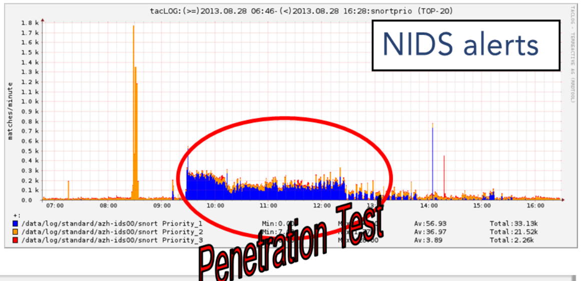
Pattern Matching

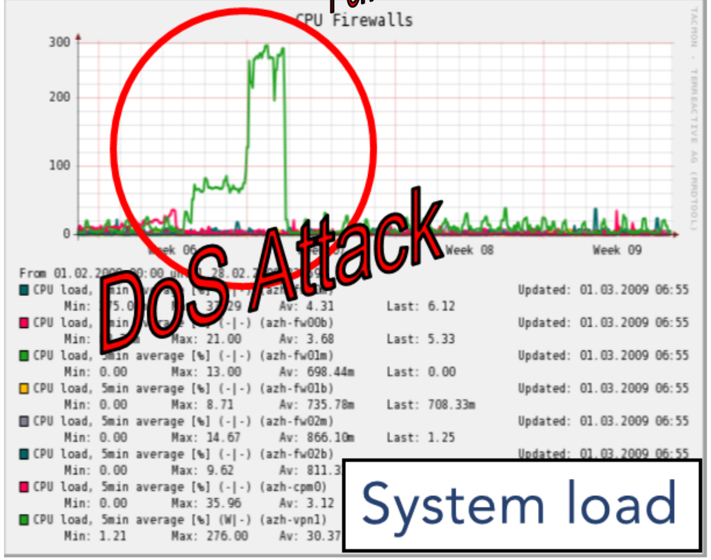
- Firewall
- Network IDS
- Web Application Firewall / Reverse Proxy
- Application Logs

Performance

- Bits/s
- Logs/s
- CPU load







Swiss Cyber Storm 5.

Data loss: the facts!

Company / Application

- Online Web-Shop

Attack

- Software exploit in web application which resulted in data leakage

Detection approach

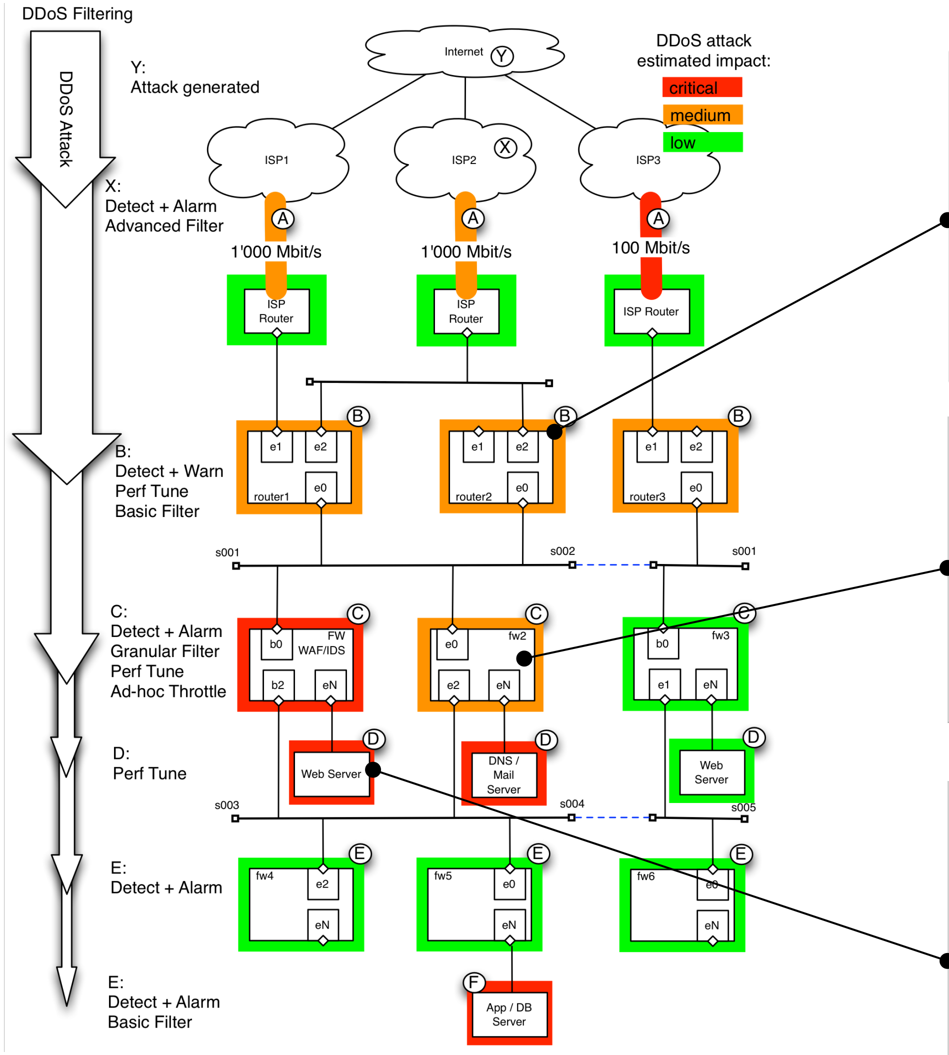
- Various automatic alarms triggered: Network load, NIDS, IDS and app logs

Mitigation

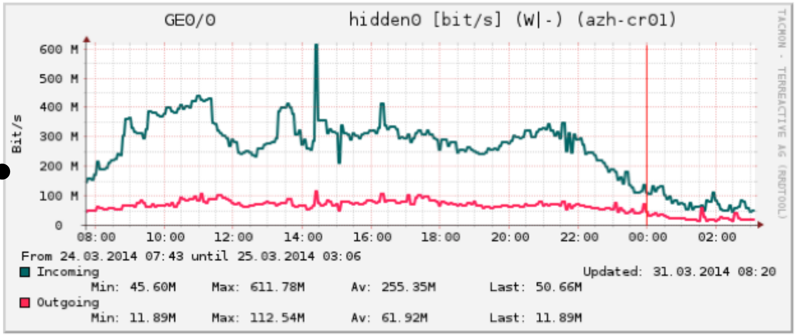
- Inform Web-/DB-Operator
- Shutdown the system
- Possibly too late

Swiss Cyber Storm 5.

Data loss: technical details.



Traffic Internet Link

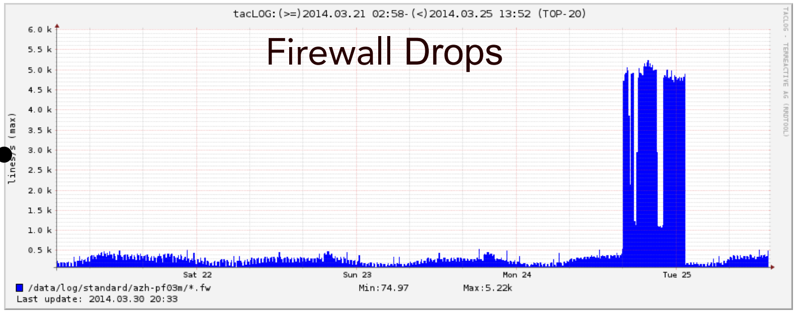


From 24.03.2014 07:43 until 25.03.2014 03:06

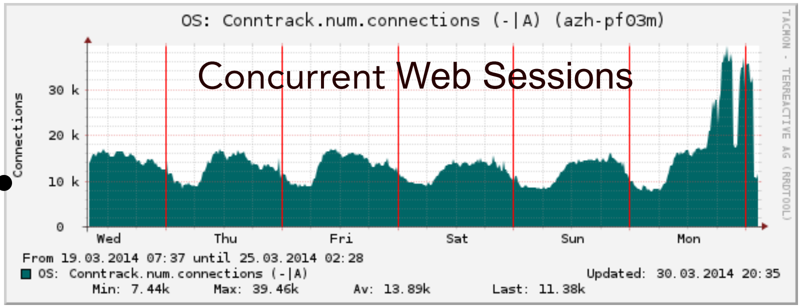
Updated: 31.03.2014 08:20

🟩 Incoming
Min: 45.60M Max: 611.78M Av: 255.35M Last: 50.66M

🟥 Outgoing
Min: 11.89M Max: 112.54M Av: 61.92M Last: 11.89M



🟦 /data/log/standard/azh-pf03m/*.fw Min:74.97 Max:5.22k
Last update: 2014.03.30 20:33



From 19.03.2014 07:37 until 25.03.2014 02:28

Updated: 30.03.2014 20:35

🟩 OS: Conntrack.num.connections (-|A)
Min: 7.44k Max: 39.46k Av: 13.89k Last: 11.38k

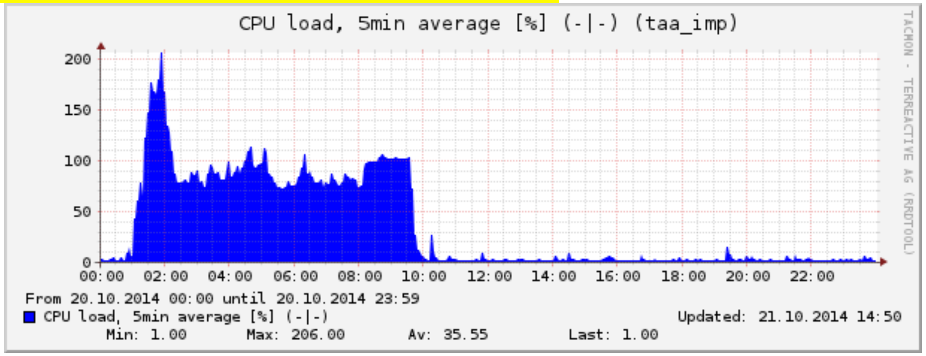
Swiss Cyber Storm 5.

Data loss: technical details.

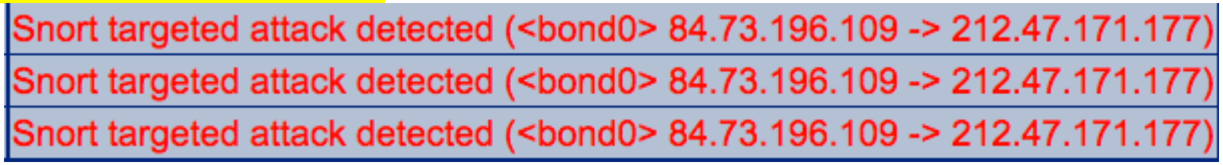
Web Application Errors

```
91.121.202.95 - - [04/Aug/2014:23:31:50
+0000] "GET /DigitalScribe/stuworkdisplay
.php?ID=-1)%20UNION 20ALL20SELECT
200x4f70656e5641532d53514c2d496e6a
656374696f6e2d54657374,2,3,4,5,6,7,8,
9,10,11%23 HTTP/1.1" 200 27 "-" ”
Mozilla/5.0 (X11; Linux; rv:17.0) Gecko
/17.0 Firefox/17.0"
```

System Overload (CPU/Network)

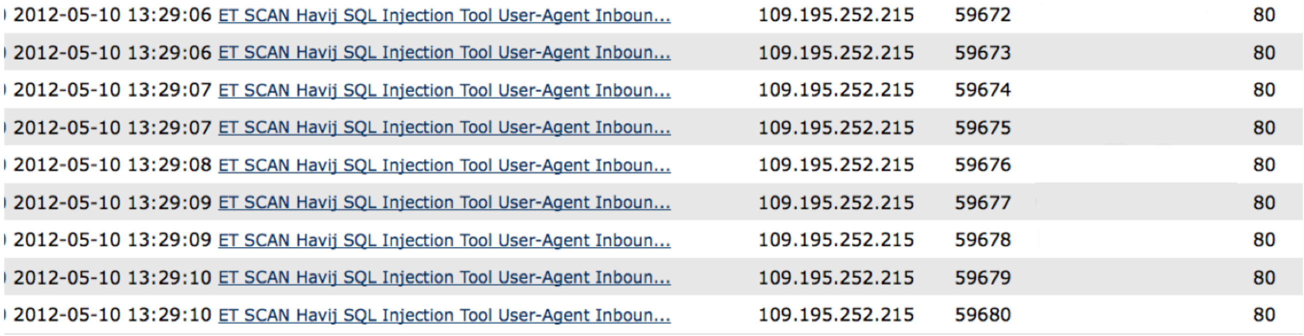


NIDS Generic Alerts



```
Snort targeted attack detected (<bond0> 84.73.196.109 -> 212.47.171.177)
Snort targeted attack detected (<bond0> 84.73.196.109 -> 212.47.171.177)
Snort targeted attack detected (<bond0> 84.73.196.109 -> 212.47.171.177)
```

IDS Specific Alerts



2012-05-10 13:29:06	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59672	80
2012-05-10 13:29:06	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59673	80
2012-05-10 13:29:07	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59674	80
2012-05-10 13:29:07	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59675	80
2012-05-10 13:29:08	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59676	80
2012-05-10 13:29:09	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59677	80
2012-05-10 13:29:09	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59678	80
2012-05-10 13:29:10	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59679	80
2012-05-10 13:29:10	ET SCAN Havij SQL Injection Tool User-Agent Inboun...	109.195.252.215	59680	80

Swiss Cyber Storm 5.
Money saved: the facts!

Company / Application

- Globally active private bank
- Web-Banking

Attack

- Malware: Men-in-the-browser / Trojan

Detection approach

- Unusual behaviour in WAF logs as part of daily log check detected
- Manual analysis of attack
- Report / search for defined pattern developed

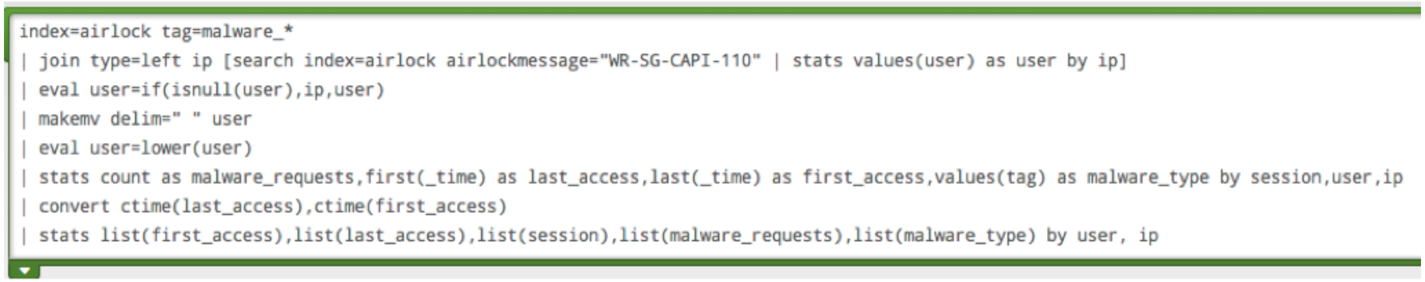
Mitigation

- Identify accounts
- Block / cancel payments
- Money saved in this case: ca. 200k CHF!

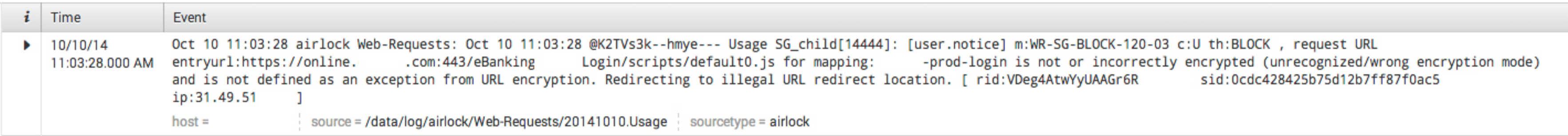
Swiss Cyber Storm 5.

Money saved: technical details!

Search

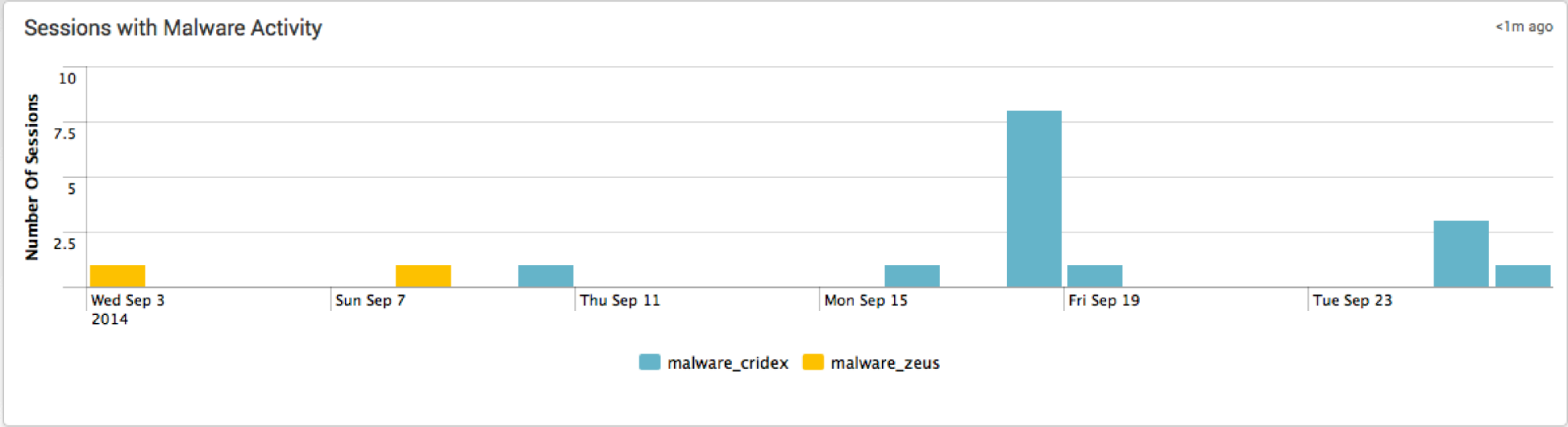


```
index=airlock tag=malware_*
| join type=left ip [search index=airlock airlockmessage="WR-SG-CAPI-110" | stats values(user) as user by ip]
| eval user=if(isnull(user),ip,user)
| makemv delim=" " user
| eval user=lower(user)
| stats count as malware_requests,first(_time) as last_access,last(_time) as first_access,values(tag) as malware_type by session,user,ip
| convert ctime(last_access),ctime(first_access)
| stats list(first_access),list(last_access),list(session),list(malware_requests),list(malware_type) by user, ip
```



i	Time	Event
▶	10/10/14 11:03:28.000 AM	Oct 10 11:03:28 airlock Web-Requests: Oct 10 11:03:28 @K2TVs3k--hmye--- Usage SG_child[14444]: [user.notice] m:WR-SG-BLOCK-120-03 c:U th:BLOCK , request URL entryurl:https://online. .com:443/eBanking Login/scripts/default0.js for mapping: -prod-login is not or incorrectly encrypted (unrecognized/wrong encryption mode) and is not defined as an exception from URL encryption. Redirecting to illegal URL redirect location. [rid:VDeg4AtwYyUAAGr6R sid:0cdc428425b75d12b7ff87f0ac5 ip:31.49.51] host = ⁞ source = /data/log/airlock/Web-Requests/20141010.Usage ⁞ sourcetype = airlock

Report



Swiss Cyber Storm 5.

Summary.

Monitoring / Detection lessons learned

- Logs and other machine data can be very valuable
- Detection works well in a «clean» infrastructure
- Combine automated alerting and manual (human) analysis for best results
- Establish a dedicated Security Operations Center in bigger organisations
- Start with your core applications (e.g. e-Banking) and expand with the experience
- Don’t forget: «listen to your logs»

Swiss Cyber Storm 5.
Conclusion.

Good detection based on automatic alerting and manual analysis makes prevention possible and can save money before it’s too late!

«You can’t FULLY defend.
You can’t FULLY prevent.
A GOOD thing TO do is detect and respond.»

Thank you for your attention!
We safeguard your success!

terreActive AG
Kasinostrasse 30
CH-5001 Aarau
sales@terreActive.ch