Effective Methods to Detect Current Security Threats

Enrico Petrov
Director Managed Security Services
terreActive

October 21st , 2015

terreActive Background.

About us.

Facts

- 20 years experience in IT-security
- Swiss company with 45 employees

Profile

- Trusted partner for comprehensive and sustainable IT-security solutions
- Strong focus on Security Monitoring Independent and solution-oriented
- Services in the IT-security-lifecycle
- Pioneer for MSS Managed Security Services (60% of company revenues)

terreActive Background.

Who trust us - our customers.

Aargauische Kantonalbank
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
ad cubum
SWISS EXCELLENCE KWC ARMATUREN
CSS Versicherung
Basler Kantonalbank fair banking
abraxas
aspectra hosting your future
ifolor.
CONCORDIA
Schwyzer Kantonalbank
KANTON AARGAU
jobs.ch
SULZER
INSELSPITAL
Luzerner Kantonalbank
Basel-Stadt
Fleurop-Interflora
aspo
Kantonsspital St.Gallen
CREDIT SUISSE
STADT AARAU
SBB CFF FFS
rivella
Helsana
Swiss Re
Stadt Zürich Organisation und Informatik
swisscom
SGS
Kantonsspital Graubünden
Julius Bär
SWISS POST
TNT SWISS POST
STADT BADEN
EPI Schweizerisches Epilepsie-Zentrum
dreyfus
VRSG Vertrauen verbindet.
Wüest & Partner
rega
Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF
Staatssekretariat für Wirtschaft SECO

Overview Current Threats.

Security Threat Detection.

Trojan Horse

Vulnerable Applications

Advanced Persistent Threats (APTs)

Denial of Service

Data Leakage

Malware

Compromised Accounts

Overview Current Threats.

Security Threat Detection.

Spending in Information Security continues to grow (8% in 2014).

Gartner

Cyber attacks are within the top 5 risks in terms of likelihood.

WEF: 2014 Global Risk Report

The number of reported security incidents has grown 66% year-over-year since 2013.

PWC: The Global State of Information Security® Survey 2015

Number of organizations reporting cybersecurity incidents with costs exceeding 20 Mio increased by 92% since 2013.

PWC: The Global State of Information Security® Survey 2015

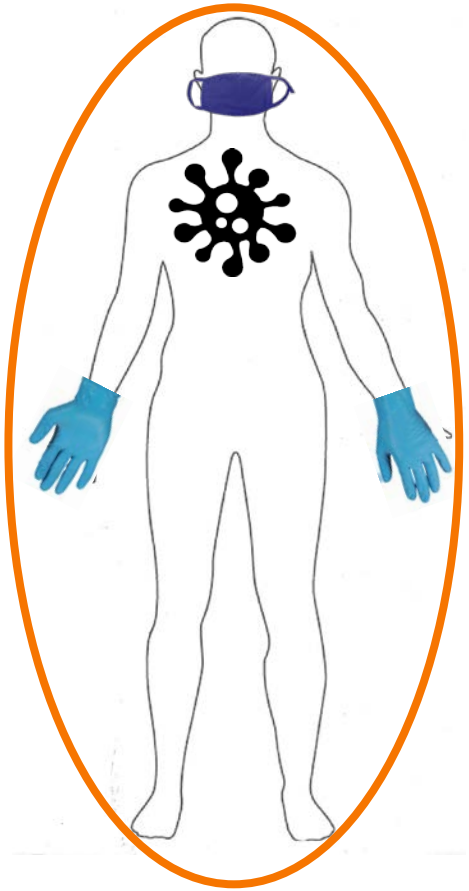
“Many organizations recognize only after 6-9 months that they have been compromised”

Dr. Eric Cole “Advanced Persistent Threat”

Overview Current Threats.

Security Threat Detection.

Security ≠ absolute protection:
→ Incident *will* happen, no matter what protection is in place



Security threats are like a bad disease:

→ It can stay hidden and grow
→ Can cause serious damage
→ Can be hard to get rid of

Solution:

- Border protection?
- Better: strong **Immune System**

→ IT Security Monitoring

IT Security Monitoring

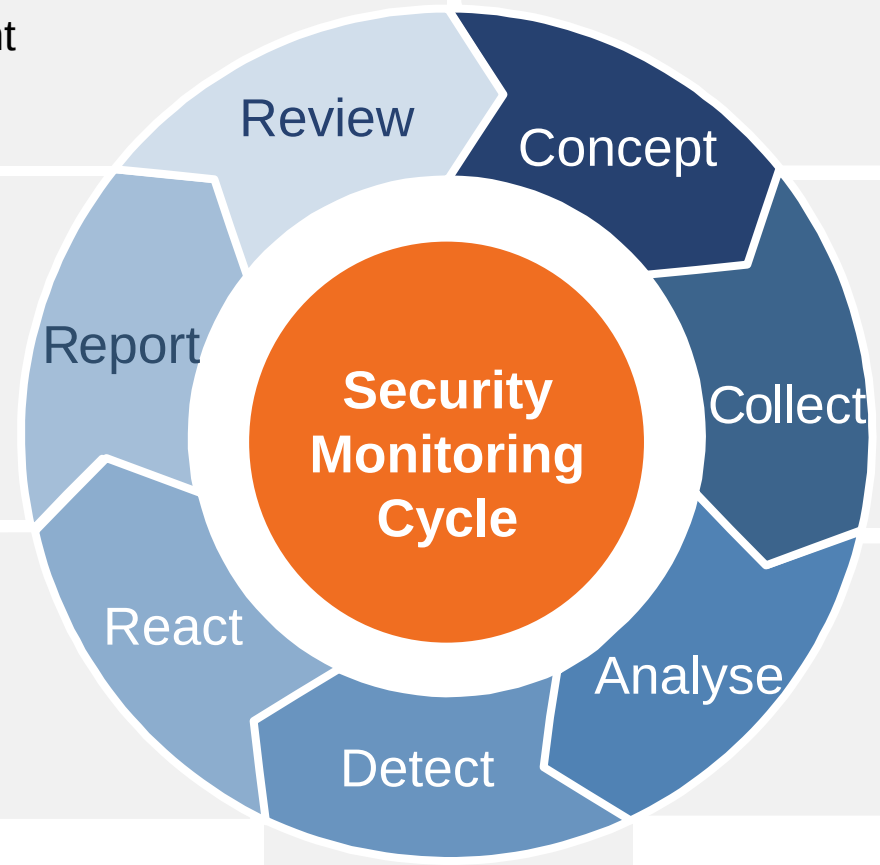
"It's not a just tools, or processes: it's a discipline providing assurance on the capability of an organization in **continuously** and **efficiently** detect and respond to disruptive information security events"

Works like the human body 'Immune System':

- Differentiated
- Sophisticated detection
- Works from the inside
- Learning
- Adaptive
- Always-on

Tools and Methods.

Security Threat Detection: IT Security Monitoring



Test / Assessment
Gap analysis
Tuning

Identify targets, define priorities and strategies

Mgt. Summary
Compliance
Security Status
Tracking

Systematically collect evidence of security relevant events

Incident Handling
Mitigation
Escalation

Normalize security events, define key metrics, apply correlation and base-lining

Detect incidents, policy violations and anomalies

Details and Examples.

Security Threat Detection: «Collect»

Log messages

Security logs: Firewall, VPN, Remote Access, Mail/Web Gateways

→ Protocol **ALL** connections entering / leaving corporate network
- not only the denies … (*"Accepted connections are bad"*)

→ Break encryption and collect logs from SSL reverse proxy, SSL intercept Web surfing, Transfer Gateways (*"Encryption is bad"*)

Application logs: Web, Application Server

Intrusion detection: Network-IDS, Host-IDS, Anti Virus, Anti Malware

Details and Examples.

Security Threat Detection: «Collect»

Log messages

Audit logs: DBs, AAA, DLP, Privileged Access Log / Sessions

→ Trust your administrators … but *“no blind trust → full action logging”*

Log DNS requests / responses on internal network

→ Malware needs to “call-home”

Details and Examples.

Security Threat Detection: «Collect»

Monitoring data

System and network monitoring information (availability, performance, system load for host, gateways and network links)

Real-time and trend traffic statistics (e.g. bit/s, packets/s)

Application monitoring (end-to-end performance, fingerprint)

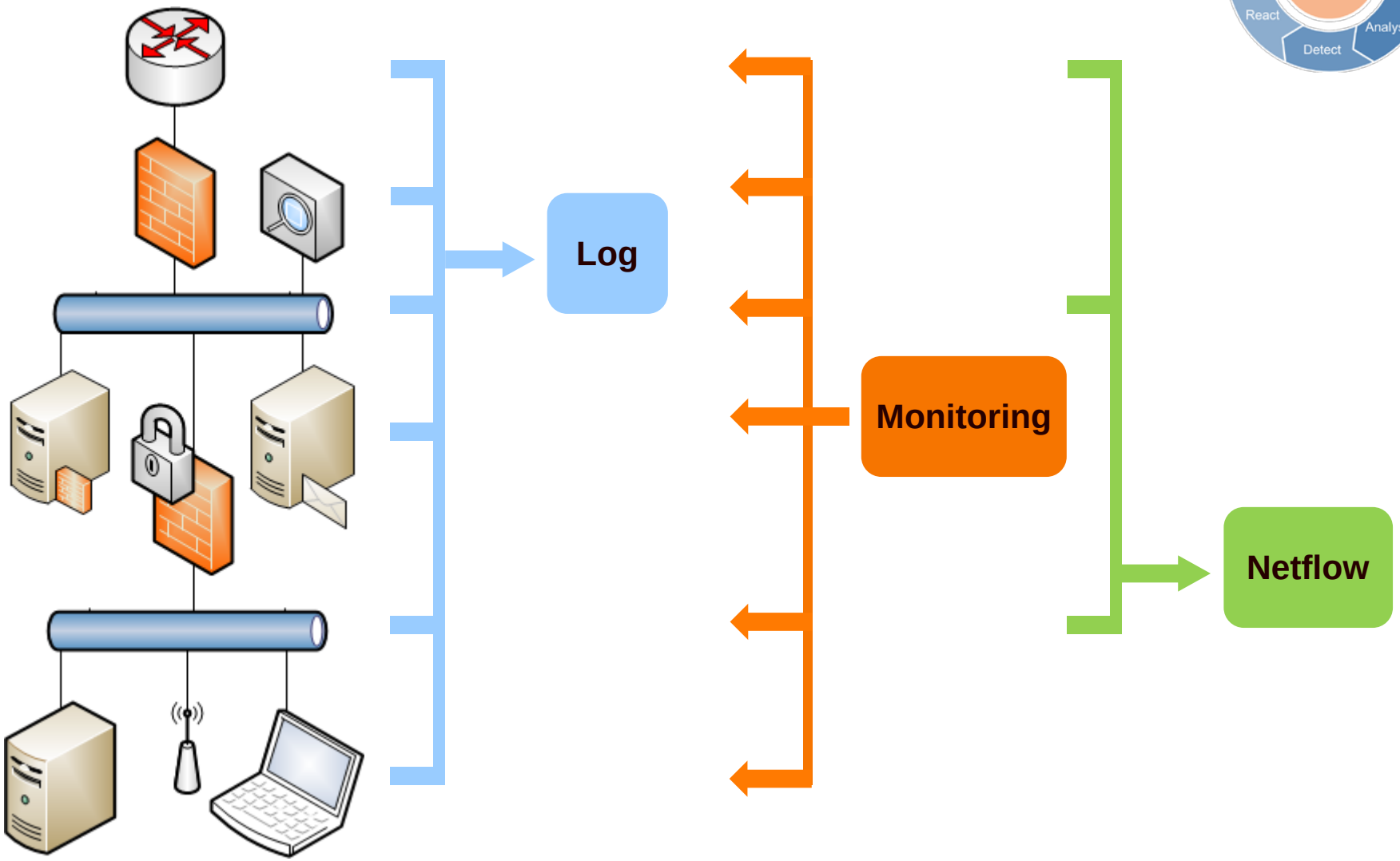
Netflow data

Application ‘flow streams’ at network layer

Break down by protocol / hosts / duration / transfer rates and volume

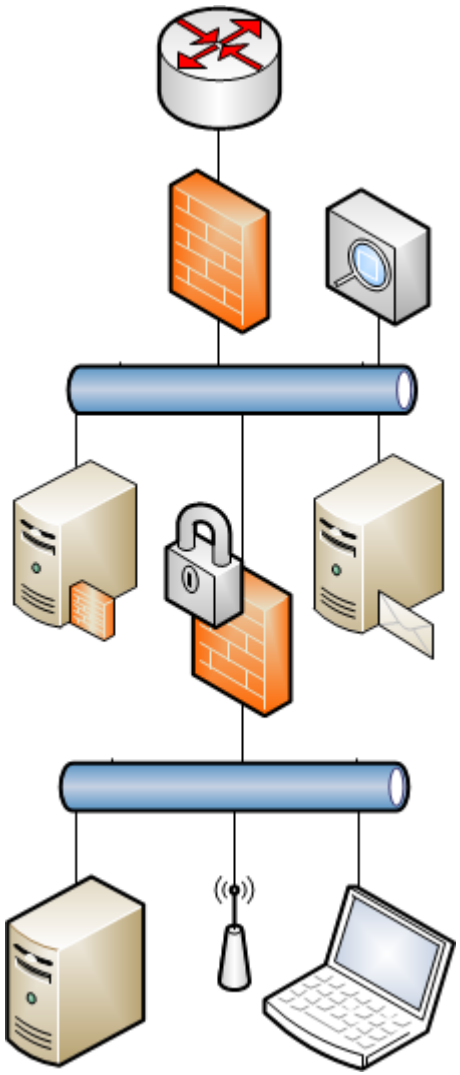
Details and Examples.

Security Threat Detection: «Collect»



Details and Examples.

Security Threat Detection: «Collect»



Log **Monitoring** **Netflow**

Collect & store on central dedicated system

→ Read-only, cannot be tampered with
→ Role based access control
(operator, security analyst, CISO)

Enable long retention time

→ Forensics, trend analysis (“learn from the past”)

Make collected data available online

→ Live search
→ Visual statistics

Enable dashboards

→ Aggregation key metrics, drilldown

Details and Examples.

Security Threat Detection: «Analyse»

Analyse data (sample)

"The enemy is outside", *"the enemy is inside"*:

→ assume a security breach has already happened
→ *focus on outbound accepted/denied connections*
(that's where often malware covert channels lie)

Keep an eye on long lasting connections (they are invisible …)

Check reputation scoring of accessed external IP / domains:

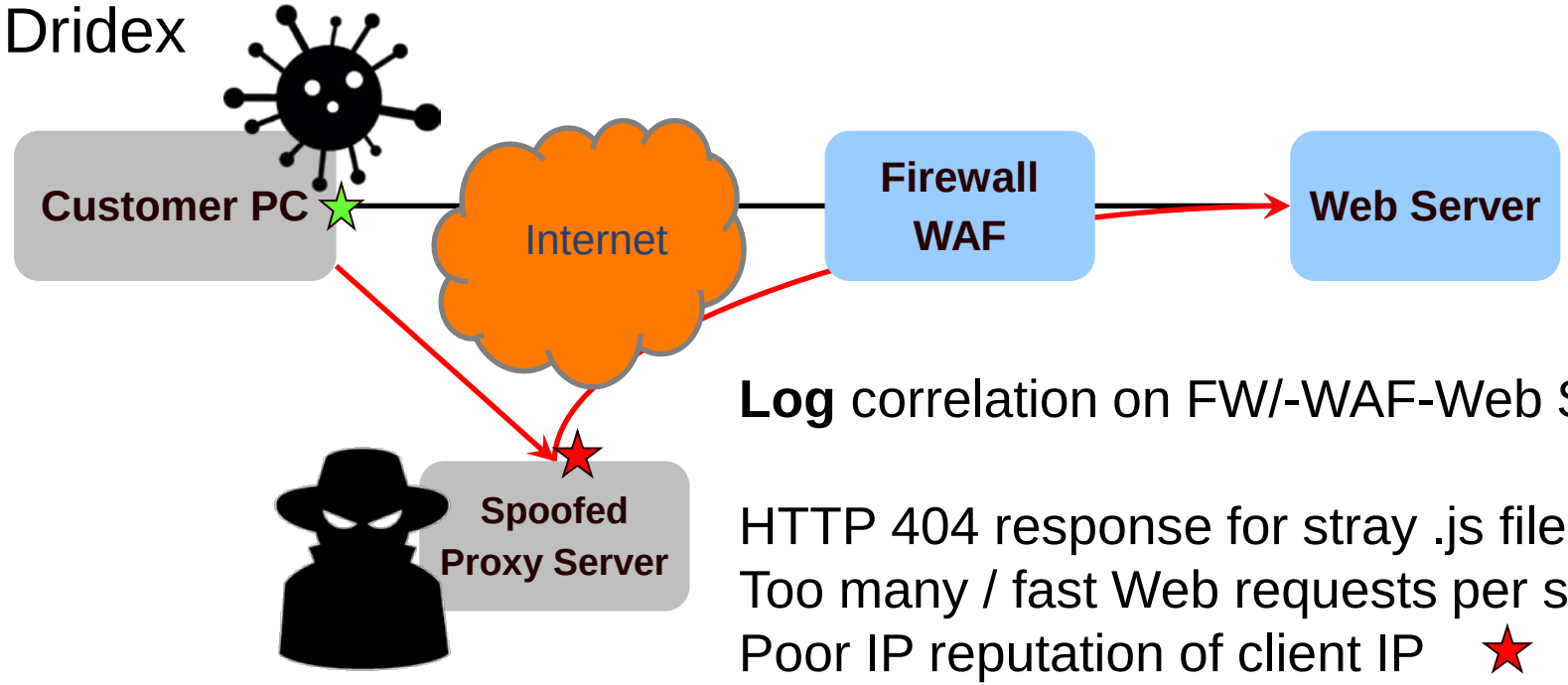
→ periodically fetch IP blacklists (e.g. www.abuse.ch, MELANI, ..)
→ match them against relevant logs

Details and Examples.

Security Threat Detection: «Detect»

Scenario: Malware on Bank/eShop client's PC

[DNS spoofing, JScript injection, fake CA Certiticate]



Log correlation on FW/-WAF-Web Server:

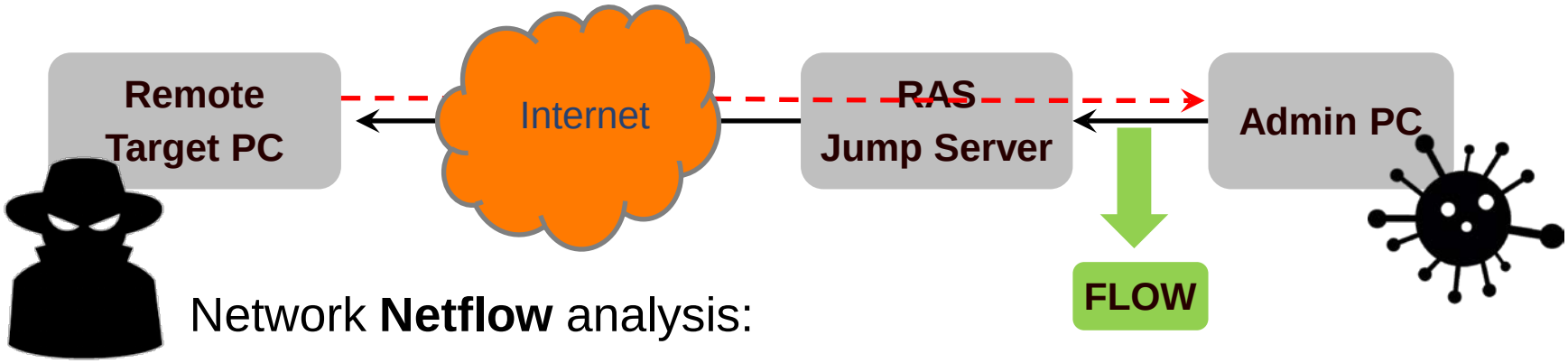
HTTP 404 response for stray .js files
Too many / fast Web requests per session
Poor IP reputation of client IP ★
Geo IP distance between logins ★★

Steal credential / CC info
Unauthorized transactions

Details and Examples.

Security Threat Detection: «Detect»

Scenario: Covert (reverse) tunnel



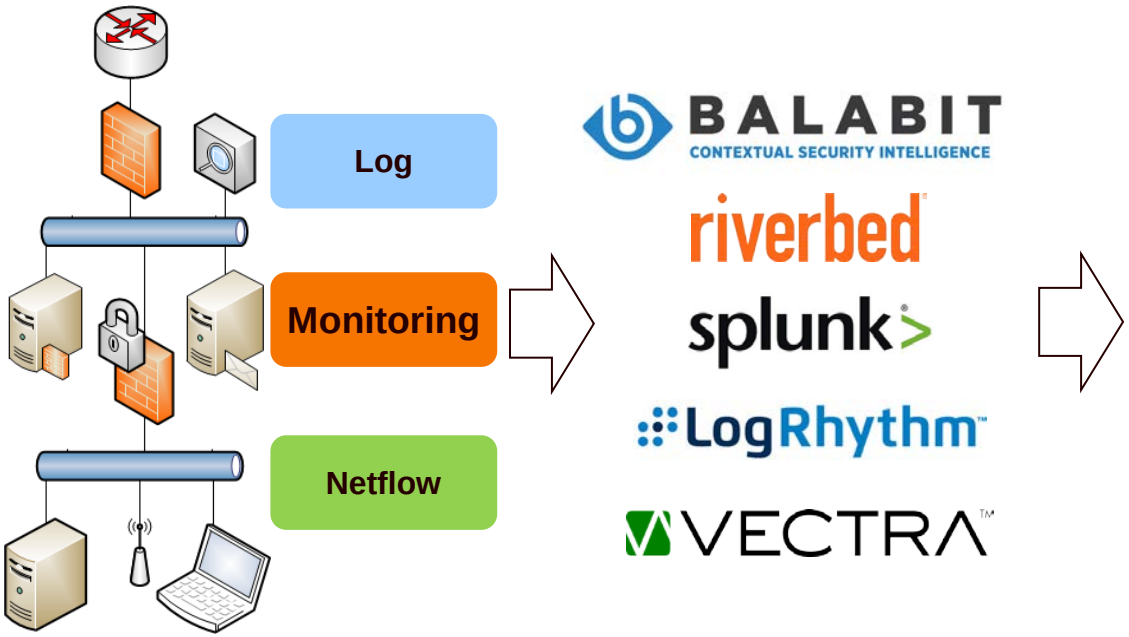
Network **Netflow** analysis:

Long lasting SSH connection via Jump Host bypassing enforced idle / absolute timeouts

Row	Start Time ↑	End Time	Duration	Protocol	Client	Client Port	Server	Server Port
1	Oct 5, 2015 9:56:44 AM	Oct 15, 2015 6:05:18 PM	1 week 3 days	tcp	dru	44390	jot2	22
2	Oct 14, 2015 1:13:10 PM	Oct 15, 2015 6:04:24 PM	1 day 4 hours	tcp	lco	49502	wsa1-back	3128
3	Oct 15, 2015 8:22:15 AM	Oct 15, 2015 6:06:21 PM	9 hours 44 minutes	tcp	roman	55963	wsa1-back	3128
4	Oct 15, 2015 8:22:17 AM	Oct 15, 2015 6:05:18 PM	9 hours 43 minutes	tcp	roman	55981	wsa1-back	3128

Organization and processes to make it work.

Security Threat Detection: Methodology



1. Collect vitals
2. Apply advanced diagnostics
3. Consult the expert

Thank you!

terreActive AG
Kasinostrasse 30
5001 Aarau
Switzerland

www.security.ch

info@terreActive.ch