Effective Methods to Detect Current Security Threats

Taking your IT security to the next level, you have to consider a paradigm shift.

*In the past* companies mostly invested resources to try to avoid security violations. *Nowadays* you have to face the inevitable: a security breach can’t be fully prevented.

You need to detect it as fast as possible to be able to stop the breach in its early stages. A multi-layer defense strategy is needed to detect attacks and secure your company with a combination of various sensors to improve transparency. Based on our experience managing Security Monitoring for various Swiss companies terreActive we will share insights with you how to tackle this.
Effective Methods to Detect Current Security Threats

Enrico Petrov
Director Managed Security Services
terreActive

October 21st, 2015
Overview Current Threats.
Security Threat Detection.

Trojan Horse
Advanced Persistent Threats (APTs)
Denial of Service
Malware
Compromised Accounts

Vulnerable Applications
Data Leakage
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.

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

“Many organizations recognize only after 6-9 months that they have been compromised”
Dr. Eric Cole “Advanced Persistent Threat”
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

<table>
<thead>
<tr>
<th>Concept</th>
<th>Identify targets, define priorities and strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect</td>
<td>Systematically collect evidence of security relevant events</td>
</tr>
<tr>
<td>Analyse</td>
<td>Normalize security events, define key metrics, apply correlation and base-lining</td>
</tr>
<tr>
<td>Report</td>
<td></td>
</tr>
<tr>
<td>Review</td>
<td></td>
</tr>
</tbody>
</table>

#### Security Monitoring Cycle

- **Detect**: Detect incidents, policy violations and anomalies
- **React**: Incident Handling, Mitigation, Escalation
- **Collect**: Systematically collect evidence of security relevant events
- **Analyse**: Normalize security events, define key metrics, apply correlation and base-lining
- **Report**: Mgt. Summary, Compliance, Security Status, Tracking
- **Review**: Test / Assessment, Gap analysis, Tuning
- **Concept**: Identify targets, define priorities and strategies
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
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»

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 Certificate]

Dridex

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
Organization and processes to make it work.

Security Threat Detection: Methodology

1. Collect vitals
2. Apply advanced diagnostics
3. Consult the expert
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)
Thank you!