the open Net

sine qua non

Vulnerability Risk management for everyone

arkenoi@gmail.com

ENOG12

the open Net

- mobilize technical Internet community
- provide technical expertise
- talk to other stakeholders

Why bother

Risk Management is the essence and purpose of all Information Security activities

Everything you do for Information Security is some kind of risk management!

Who cares?

- 60% of respondents stated company executives are only “somewhat” to “not at all” informed about the risk posed to their business from today’s security threats

(NopSec 2016 Outlook: Vulnerability Risk Management and Remediation Trends)

What is risk management

- GRC: Governance, Risk management and Compliance

- Stage 0: ad hoc
- Stage 1: missing! (a lot of bad stuff happens just here)
- Stage 2: compliance driven (things that cannot be ignored)

Nature of risk management gap

- Cultural (“It is compliance driven stuff, we do not care, we have business to do”)
- Financial (“Only wealthy companies can afford this”)
- Technological (“We have no resources to waste on your complicated toys”)

Measurement: Quantitative?

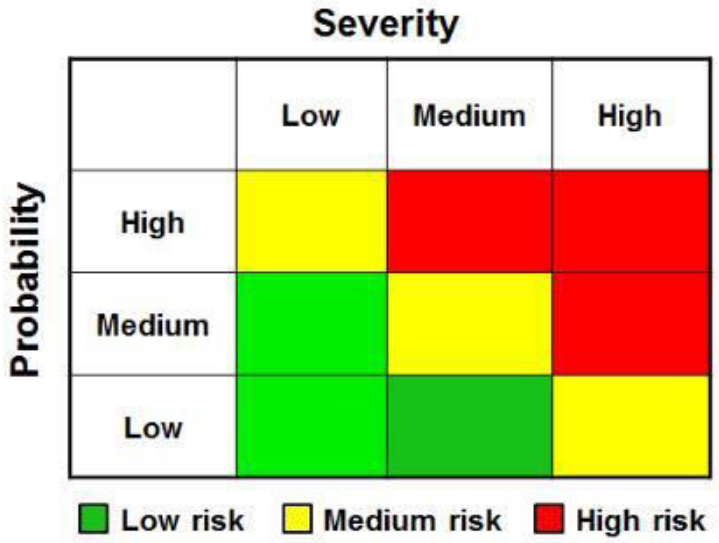
Risk = Impact ($) * Probability

Both variables are mostly unknown, yet estimated. The formula might get complicated if you add more variables (means, motive, controls, whatever)

Reliability of data sources is questionable, yet if you present *any* numbers rather than *none* it looks more convincing

Measurement: Qualitative?

- Better for decision making
- You may or may not have real quantitative data as input



Google deeper: Cox's risk matrix theorem

Threat Intelligence

"What's happening out there"? Understanding risk through external context.

Not just about 0-days and IoCs for IPS/SIEM

Both APT-like actors and opportunistic attackers matter

Network operators as natural data source for threat intel

Huge coverage

Already having tools (IDS, traffic analysis, DPI, DNS request data, etc)

Managed security services for customers

Creating effective collaboration

How should joint CERT work?

Anything is always better than nothing.

Coordinate, aggregate, analyse and share.

Distributed tasks are easier.

Three functions of joint CERT

1. CC: coordinate effort and promote information exchange (here we start!)
2. CSIRT: incident investigation, response and tactical analysis (easier!)
3. SOC: realtime and retrospective event processing (harder!)

Let’s get practical

Why vulnerability management?

Most of the breaches involve vulnerability of some kind

Manageable and measurable (involves less social context, as we know machines are easy and humans are hard)

Vulnerability Management

- Stage 0: none

- Stage 0.5: [a]periodic scans, huge vulnerabilities lists, panic and depression (significant human effort is required in this struggle)

- Stage 1: continuous vulnerability management and first attempts to prioritise on the fly (here VM vendors jump in and ask for big $$)

- Stage 2: more or less futile attempt to bring both variables into the risk equation (RM vendors jump in and ask for even more $$)

Why pay premium price

Because it is obviously valuable. And there is (or at least seems to be) no alternative.

51% of organizations are suffering from data overload (and I think many more either have massively incomplete data or do not admit their difficulties)
24% do not know how to prioritize
22% use CVSS and maybe some internal data
21% do manual correlation with threat intel
31% use commercial tools

(NopSec 2016 Outlook: Vulnerability Risk Management and Remediation Trends)

Notable players (VM)

Nessus one of best yet cheapest security scanners, but continuous vulnerability management (SecurityCenter) is expensive. Risk management capabilities are limited.

A nice try to integrate threat intelligence and advanced asset management into vulnerability scanning, again, big $$

As authors of Metasploit, the penetraion testing tool, Rapid7 is notable for highly practical approach to vulnerability management.

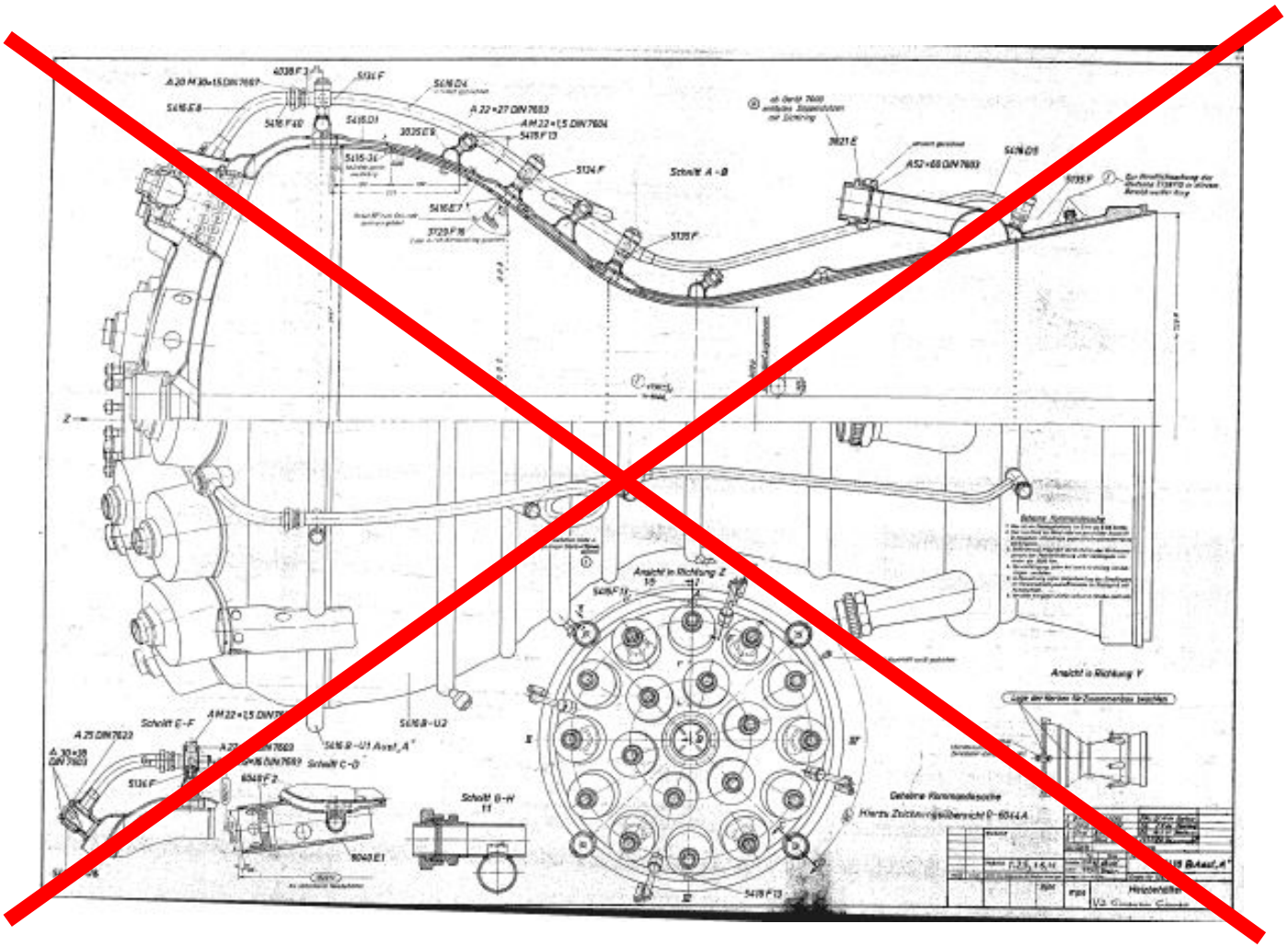
Notable players (RM)

An Israeli start-up, first (known to me) attempt to break vendor lock-in for the vulnerability risk management. Has connectors to multiple scanners. Starts with $30K or so.

If you are not from Russia, you probably never heard about this one. It's a shame because the capabilities are impressive.

GRC vendors without specific focus on VM (like RSA etc) are not listed here for obvious reason.

Industry's Dirty Little Secret



As easy as that

- “Continuous vulnerability management” requires a database backend, vulnerability scanner connectors and a few reporting tools. And it is already here (Seccubus project, developed by Schuberg Philis)
- “Vulnerability risk management” requires (surprisingly) an asset management tool with good heuristics to assist evaluation (think hostnames, software inventory, LDAP lookups etc), a method to integrate environmental factors (firewall configuration, protective tools,..), possible **threat intelligence data** and vulnerability assessment as is.
- (if you are interested in risk assessment methodology per se, refer to Open Group’s FAIR (*), it simple)

(*) Factor Analysis of Information Risk

How to evaluate vulnerability

Like hackers (well, or pentesters ;-) do!

- The only things you need to know are:
- Is this vulnerability exploitable in *your configuration*?
- Is there a pre-built exploit *for your system* available?
- What is the *real* impact?
-
- If you know that, you get part of the equation solved. The other parts are the asset value, protection countermeasures and you chances to be attacked.

A real life example

- Winshock (MS14-066) vulnerability

- Unauthenticated RCE in Windows SChannel code
- “Exploits are available”, given top priority by all vulnerability scanners
- Maximum posible CVSS score of 10.0
- Actually no RCE exploits in the wild, just DoS!

Simply put

Traditional vulnerability scanning software scares you into thinking you have an immediate and imminent threat and you should concentrate your efforts on fixing that. While there actually could be **more important things** for you to do, because the cost and complexity of the attack is much higher than was implied!

Enter Vulners

A search engine for exploits and security bulletins, contains 60+K exploits to date

Non-profit and free to use

But, wait

- Vulners exploit search is for humans
- No formal definition exists for exploit capabilities
- Time to fix that!

Enter ECDML and EACVSS

- Exploit Capability Definition Markup Language – describe exploit properties via CVE, CPE and supplementary information (CCE, common configuration enumeration is dead, sorry)
- EACVSS – Exploit Adjusted CVSS – evaluate real exploit capability

Sorry for non-readable text ;-)

```
<exploit>
<configuration>
<cpe-lang:logical-test operator="OR" negate="false">
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_8.1:-:-:~-~-~-~x64~"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_8.1:-:-:~-~-~-~x86~"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:-:gold"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:r2:-:~-~datacenter~~~
"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:r2:-:~-~essentials~~~
"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:r2:-:~-~standard~~~~"/
>
</cpe-lang:logical-test>
</configuration>
<eacvss>
  <cvssv2:base-score>8.5</cvssv2:base-score>
  <cvssv2:access-vector>NETWORK</cvssv2:access-vector>
  <cvssv2:access-complexity>LOW</cvssv2:access-complexity>
  <cvssv2:authentication>NONE</cvssv2:authentication>
  <cvssv2:confidentiality-impact>PARTIAL</cvssv2:confidentiality-impact>
  <cvssv2:integrity-impact>NONE</cvssv2:integrity-impact>
  <cvssv2:availability-impact>COMPLETE</cvssv2:availability-impact>
  <cvssv3:base-score>8.2</cvssv3:base-score>
  <configuration-constraints>DEFAULT</configuration-constraints>
  <availability>PUBLIC</availability>
  <malware>false</malware>
  <worms>false</worms>
</eacvss>
<exploit_frameworks>metasploit</exploit_frameworks>
<exploit-quality>NORMAL</exploit-quality>
<metasploit_module_path>auxiliary/scanner/http/ms15_034_http_sys_memory_dump.rb</metasploit_module_path>
<publication_date>15-Apr-2015</publication_date>
<last_updated>15-Apr-2015</last_updated>
</exploit>
```

Back to risk analysis and FAIR methodology

Loss Event Frequency (LEF) is the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.

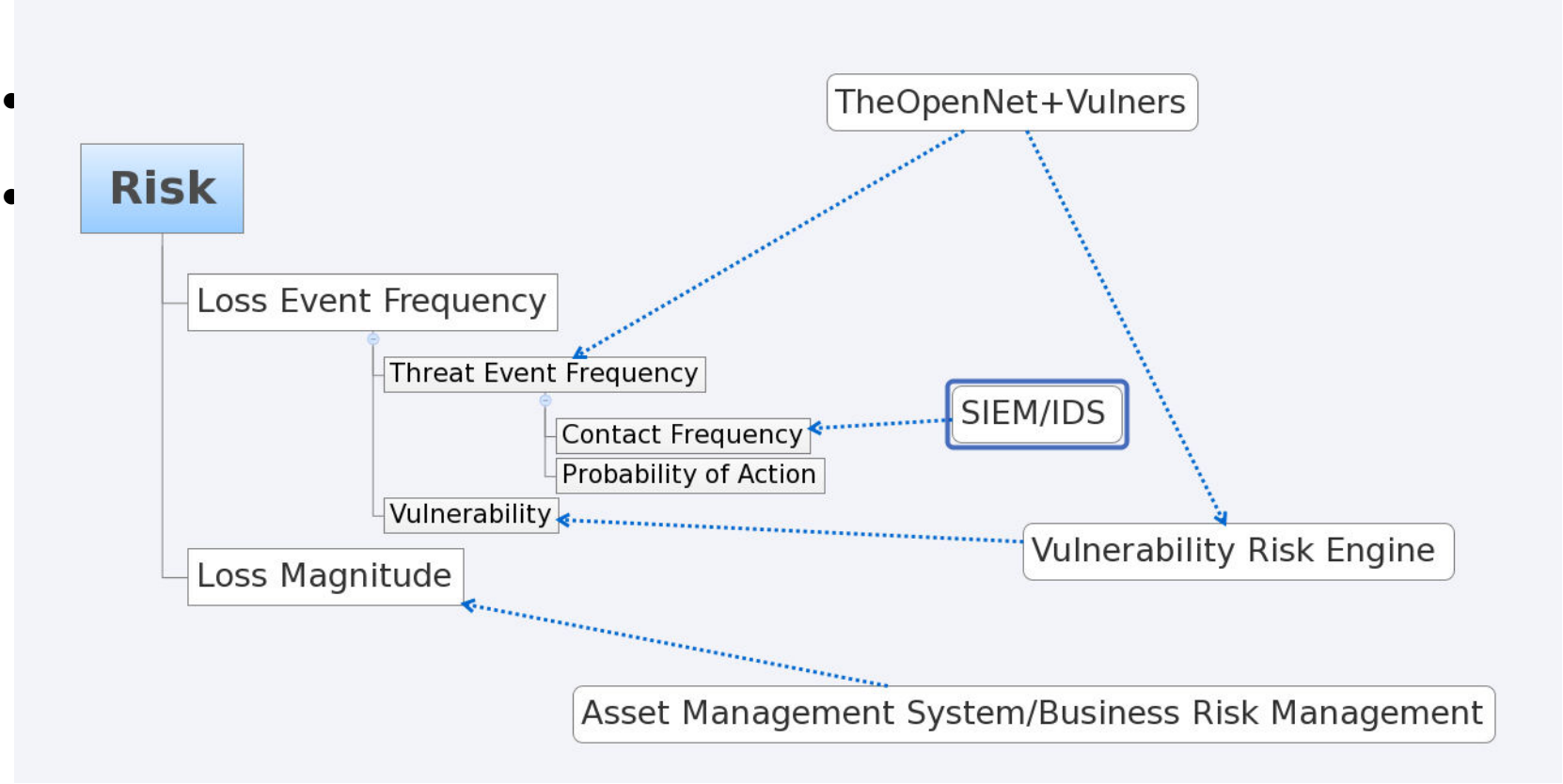
In order for a loss event to occur, a threat agent has to act upon an asset, such that loss results. This leads us to our next two factors: Threat Event Frequency (TEF) and Vulnerability (Vuln).

Figure 3: Loss Event Frequency (LEF)

What's next

- Augment risk intelligence with Threat Event Frequency
- Implement (mostly) automated risk assessments using FAIR methodology
- That's where joint CERT could provide extremely valuable information!

Dreams ;-)



How state of the art risk analysis should work

Not covered here

- Advanced vulnerability management issues like detecting and avoiding vulnerability scan gaps, “scannerless” data collection ,etc etc
- Seccubus implementation and deployment details (ask me if you want to discuss any of those later)
- FAIR methodology in depth
- Privacy issues for threat intel
- Threat intel information exchange formats

Useful links

- http://theopennet.ru
- https://www.vulners.com
- https://www.seccubus.com

Thank you!
Questions?