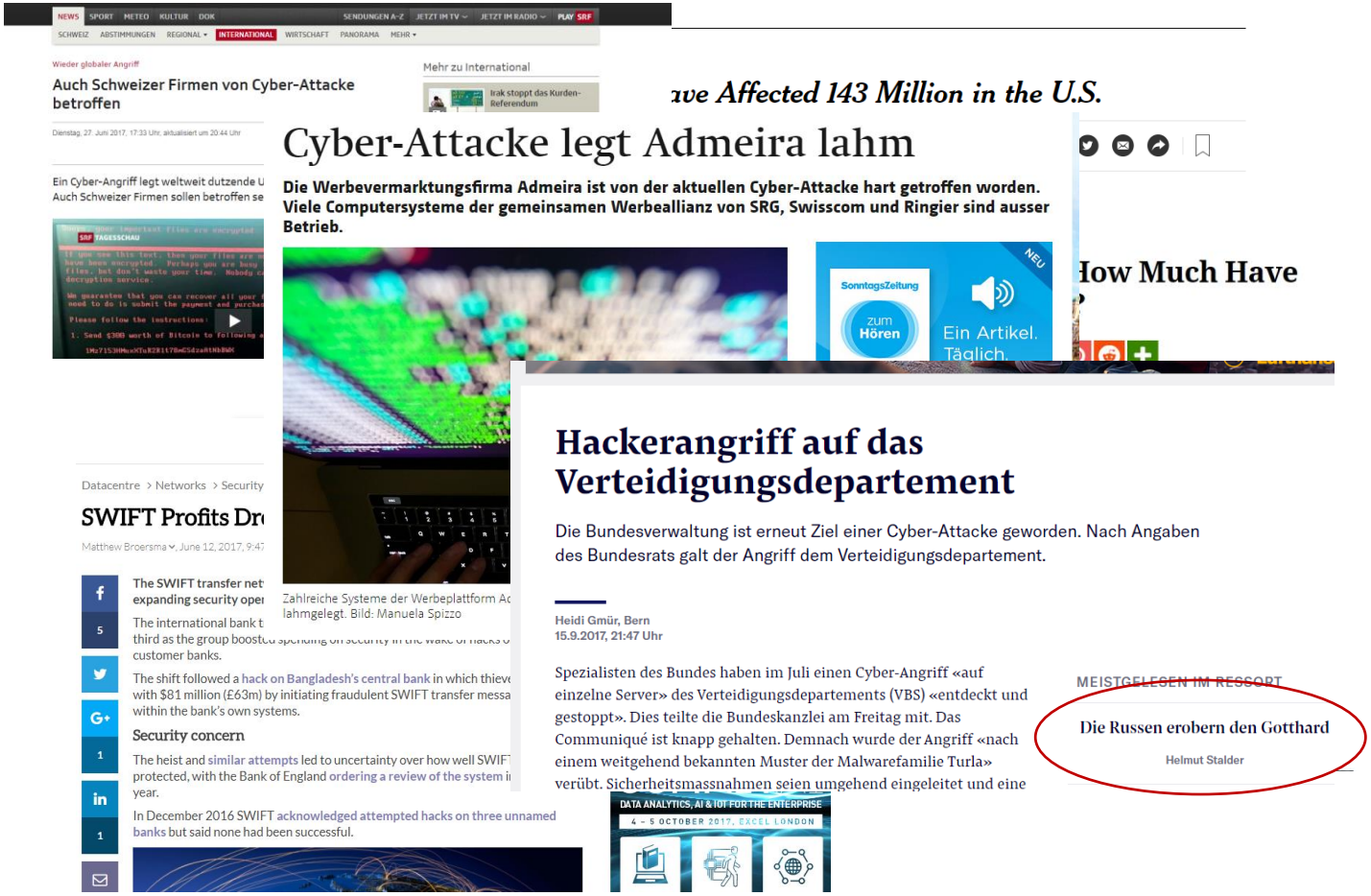
InfoGuard
SWISS CYBER SECURITY

WIRKUNSVOLLE CYBERDEFENCE

Aus dem Schweizer Cyber Defence Center

Switzerland
~~US Firms~~ under Attack

InfoGuard
SWISS CYBER SECURITY



A breach is inevitable – Reduce the impact

Do you spot the attack?

InfoGuard
SWISS CYBER SECURITY

We bring Incident Response strategies, methods and experience into the daily CDC routine

Most strategies ONLY focus on what the attacker knows

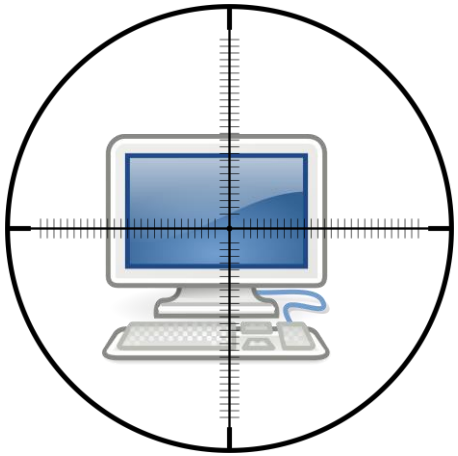
- Specific Malware
- Command & Control
- Delivery

We focus on what the attacker doesn't know

- Errors and Mistakes
- Dynamic Baselining
- Experience

Computers in a Breach

Compromised
Using malware



Compromised
no malware

Untouched by
Attacker

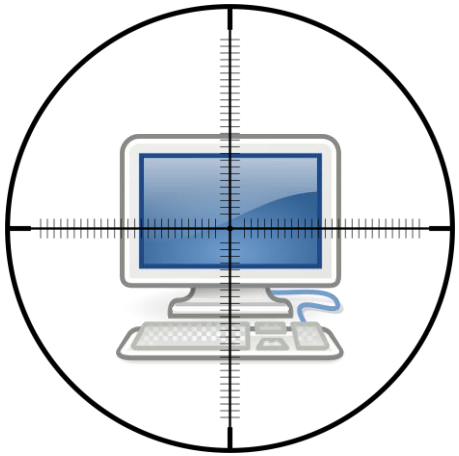
Computers in a Breach

InfoGuard
SWISS CYBER SECURITY

Computers in a Breach

Compromised
Using malware

including rootkits



Compromised
no malware

Untouched by
Attacker

but full of crap

Use Case Strategy

InfoGuard
SWISS CYBER SECURITY

Behaviour based ased Detection

InfoGuard strives to b into the daily Cyber Defense routin only depend on security devices and software t on leveraging all available informati on what he is doing and how he is doing i

Use Case Developement

InfoGuard
SWISS CYBER SECURITY

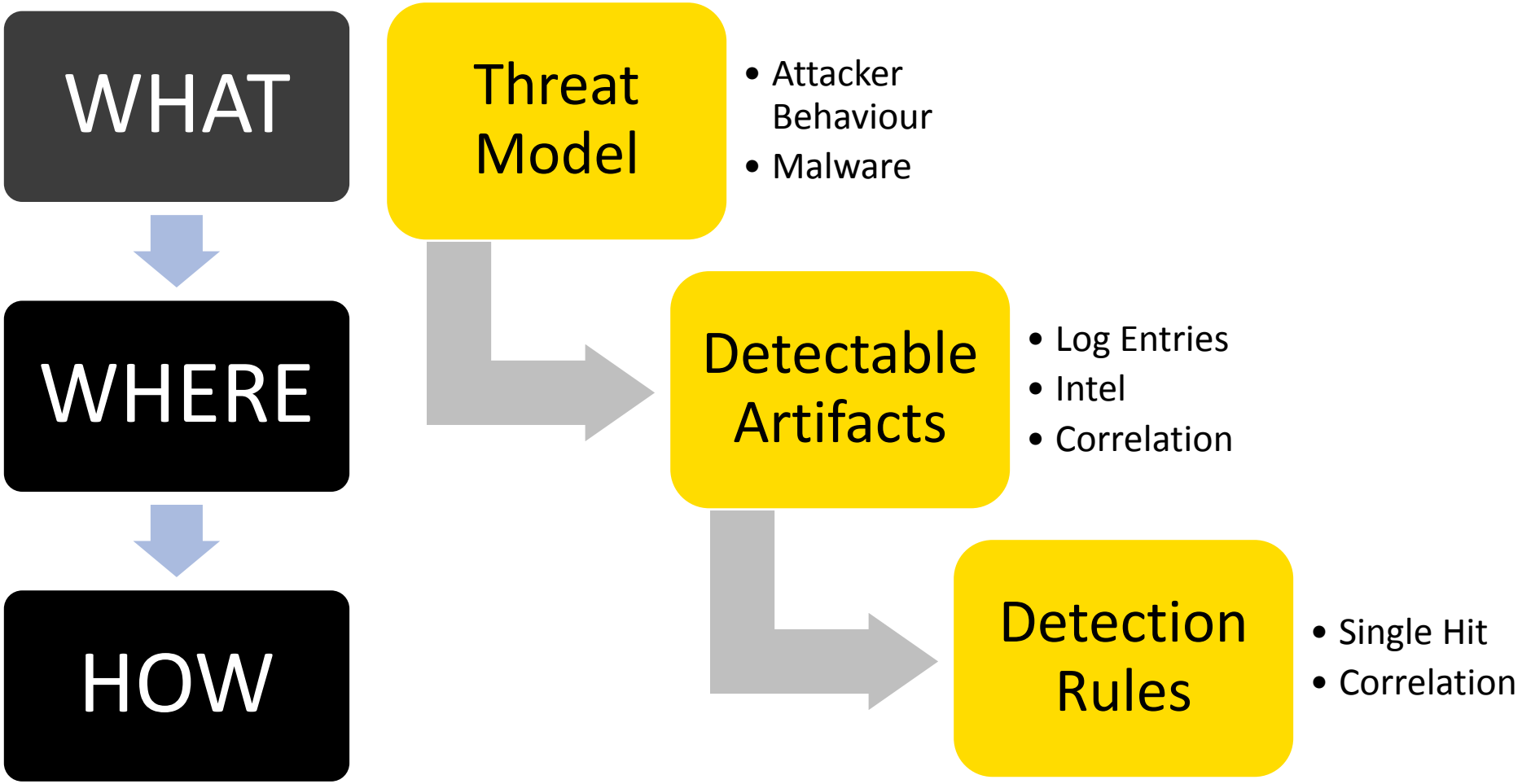
InfoGuard designs Use Cases based on Threat Models. We don't start our design by asking *«What CAN we see»* but with the question *«What do we WANT to see»*

This approach ensures high flexbility in how we detect attacks and particularly emerging threats.

For InfoGuard Use Cases are the units we sell, the underlying detection mechanisms evolves constantly.

Use Case Developement

InfoGuard
SWISS CYBER SECURITY



Showcase - Detection

Use Case «Lateral movement using RDP»

High Level Description

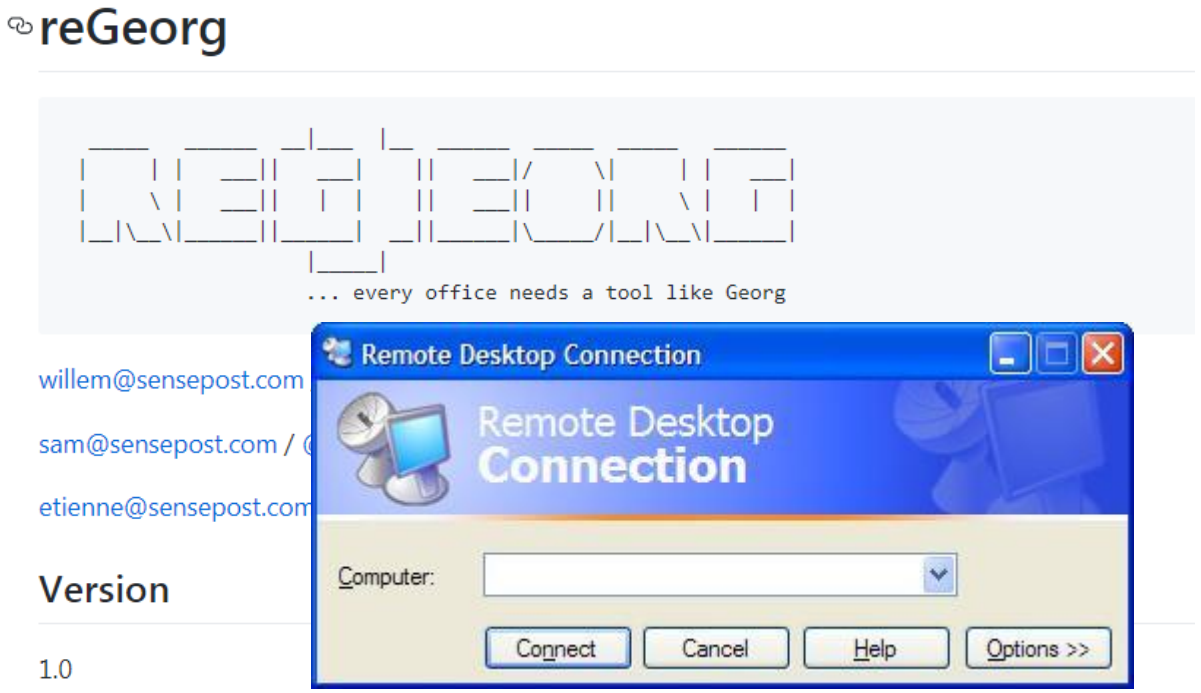
This Threat Scenario detects unusual RDP connections and connection attempts based on source and target as well as on account.

Technical Sources

- Firewall connection log
- Windows Security Log
- Domaincontroller Logs

Correlation Rules

- QRadar



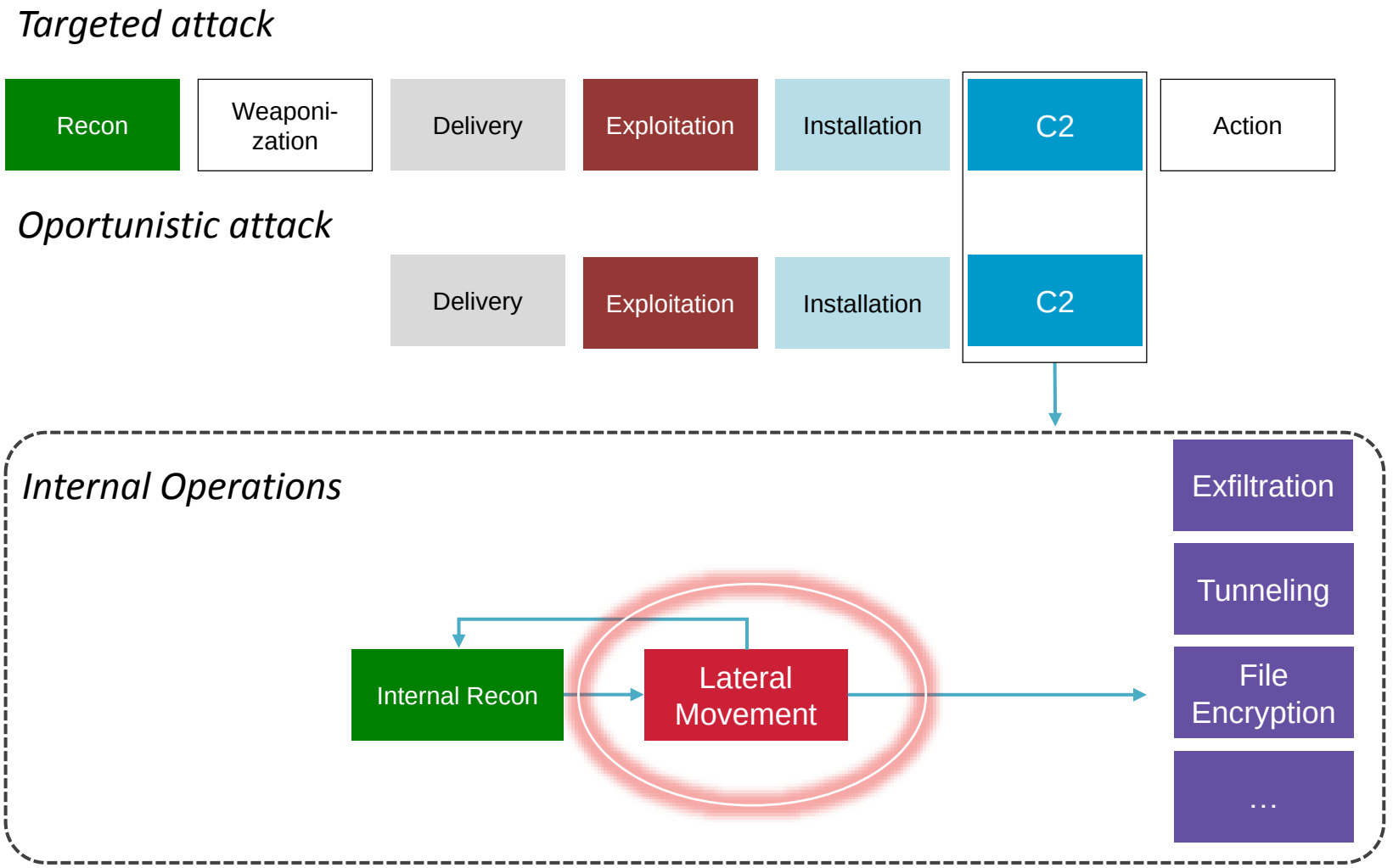
WHAT?

Remote Desktop Protocol (**RDP**) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software. (Wikipedia)

RDP connections use TCP Port 3389 and need the user to log on prior to establishing the session.

While RDP is frequently used for administrative tasks within most companies, there still is a pattern that lets us differentiate between suspicious and benign connections and connection attempts.

Sans Kill Chain – Internal Portscan

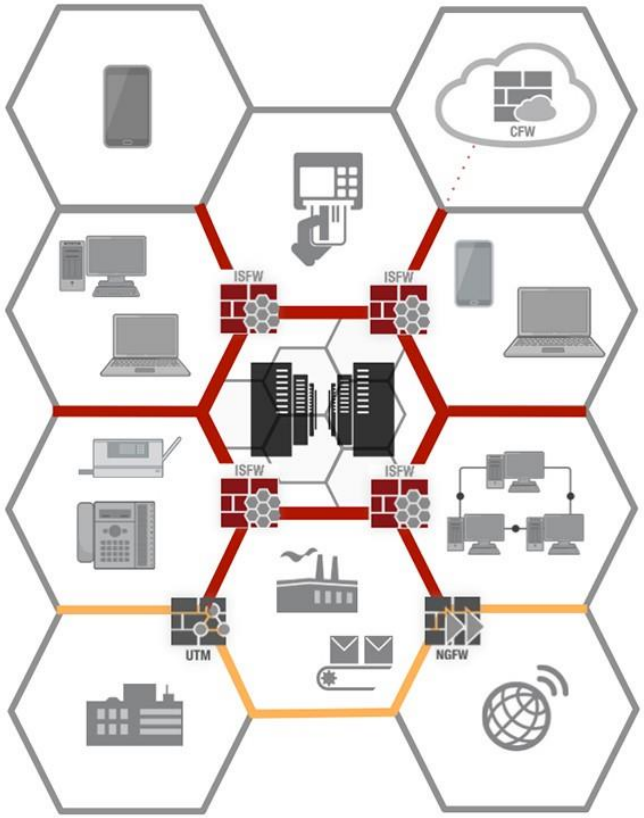


WHERE?

A port scan is a network based and a host based scenario. Connections and unsuccessful connection attempts will be logged by the firewall.

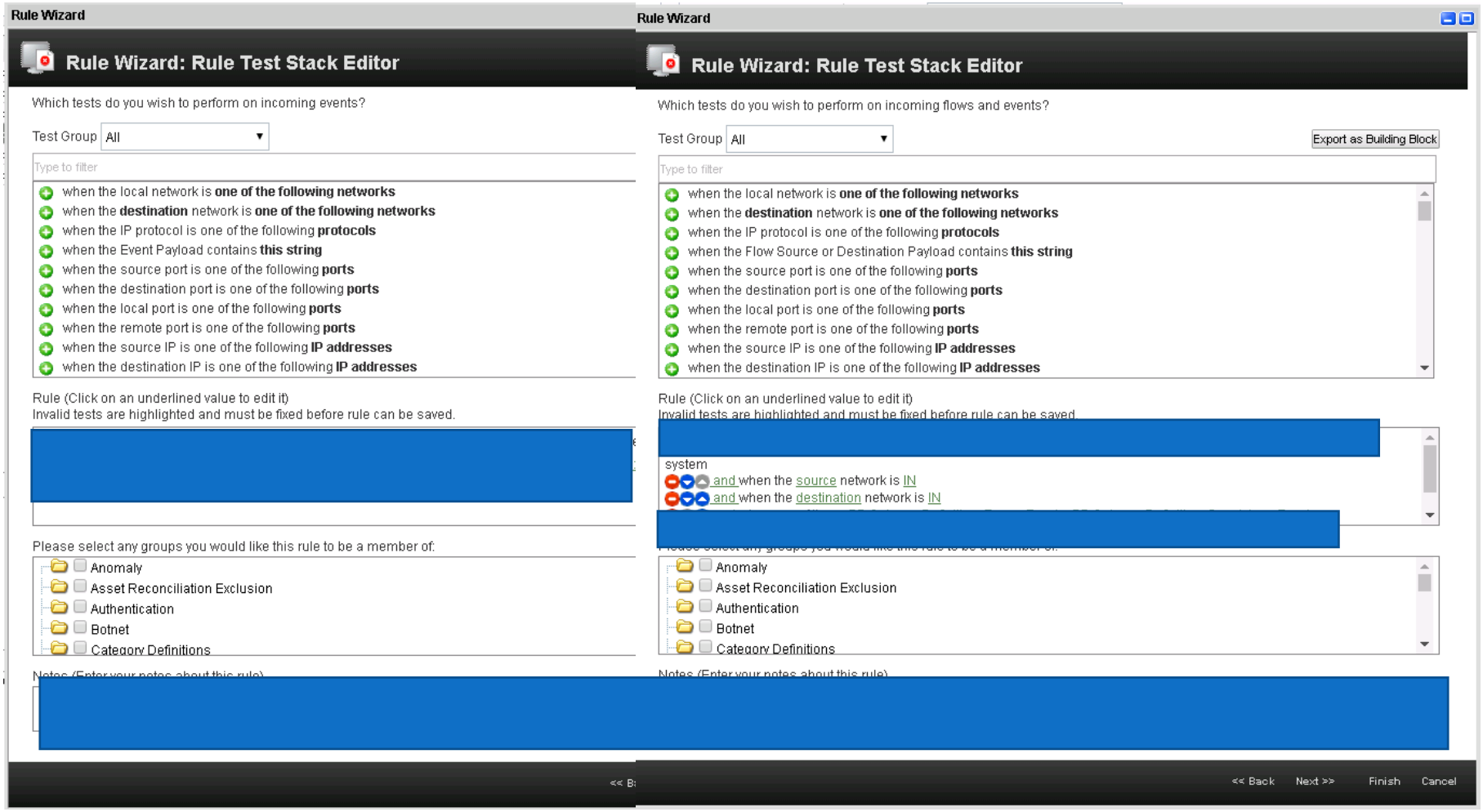
The Windows Security Log stores successful and unsuccessfull logon attempts as well as established RDP sessions. Those can be correlated to identify suspicious behaviour.

If the RDP logon is based on domain credentials, the user will be authenticated on the domain controller which will also store successful and unsuccessful logon attempts.



	Firewall Deny	igchd1-ffwE01	1	Jul 7, 2017, 1:46:56 PM	Firewall Deny
	Firewall Deny	igchd1-ffwE01	1	Jul 7, 2017, 1:46:56 PM	Firewall Deny
	Firewall Deny	igchd2-ffwE01	1	Jul 7, 2017, 1:46:56 PM	Firewall Deny
	Firewall Deny	igchd2-ffwE01	1	Jul 7, 2017, 1:46:56 PM	Firewall Deny
	Firewall Deny	igchd2-ffwE01	1	Jul 7, 2017, 1:46:56 PM	Firewall Deny

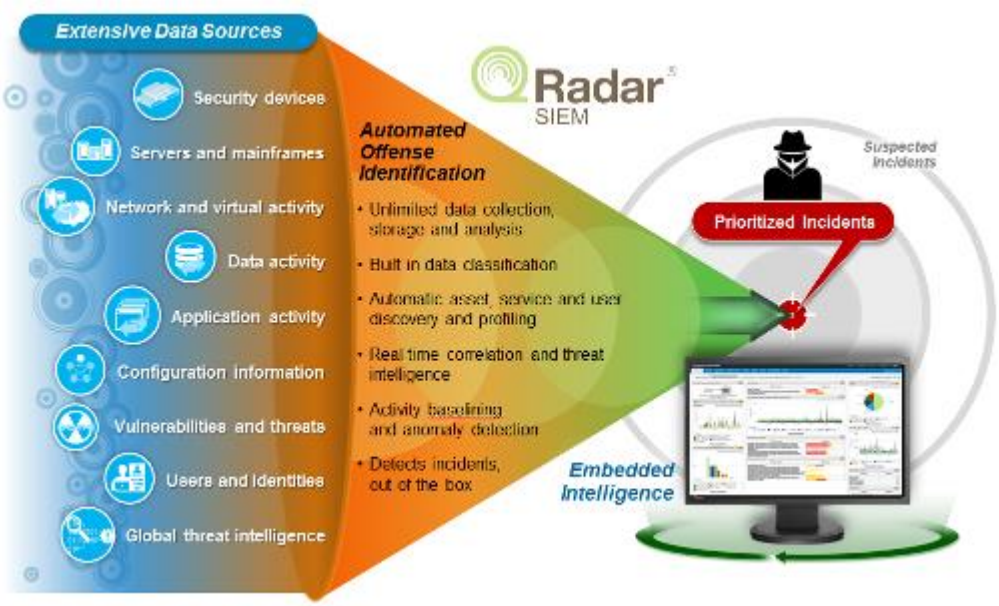
HOW?


Rule Wizard
Rule Wizard: Rule Test Stack Editor
Which tests do you wish to perform on incoming events?
Test Group All
Type to filter
when the local network is one of the following networks
when the destination network is one of the following networks
when the IP protocol is one of the following protocols
when the Event Payload contains this string
when the source port is one of the following ports
when the destination port is one of the following ports
when the local port is one of the following ports
when the remote port is one of the following ports
when the source IP is one of the following IP addresses
when the destination IP is one of the following IP addresses
Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.
Please select any groups you would like this rule to be a member of:
Anomaly
Asset Reconciliation Exclusion
Authentication
Botnet
Category Definitions
Notes (Enter your notes about this rule)
Rule Wizard
Rule Wizard: Rule Test Stack Editor
Which tests do you wish to perform on incoming flows and events?
Test Group All
Export as Building Block
Type to filter
when the local network is one of the following networks
when the destination network is one of the following networks
when the IP protocol is one of the following protocols
when the Flow Source or Destination Payload contains this string
when the source port is one of the following ports
when the destination port is one of the following ports
when the local port is one of the following ports
when the remote port is one of the following ports
when the source IP is one of the following IP addresses
when the destination IP is one of the following IP addresses
Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.
system
and when the source network is IN
and when the destination network is IN
Please select any groups you would like this rule to be a member of:
Anomaly
Asset Reconciliation Exclusion
Authentication
Botnet
Category Definitions
Notes (Enter your notes about this rule)
<< Back
Next >>
Finish
Cancel

HOW?

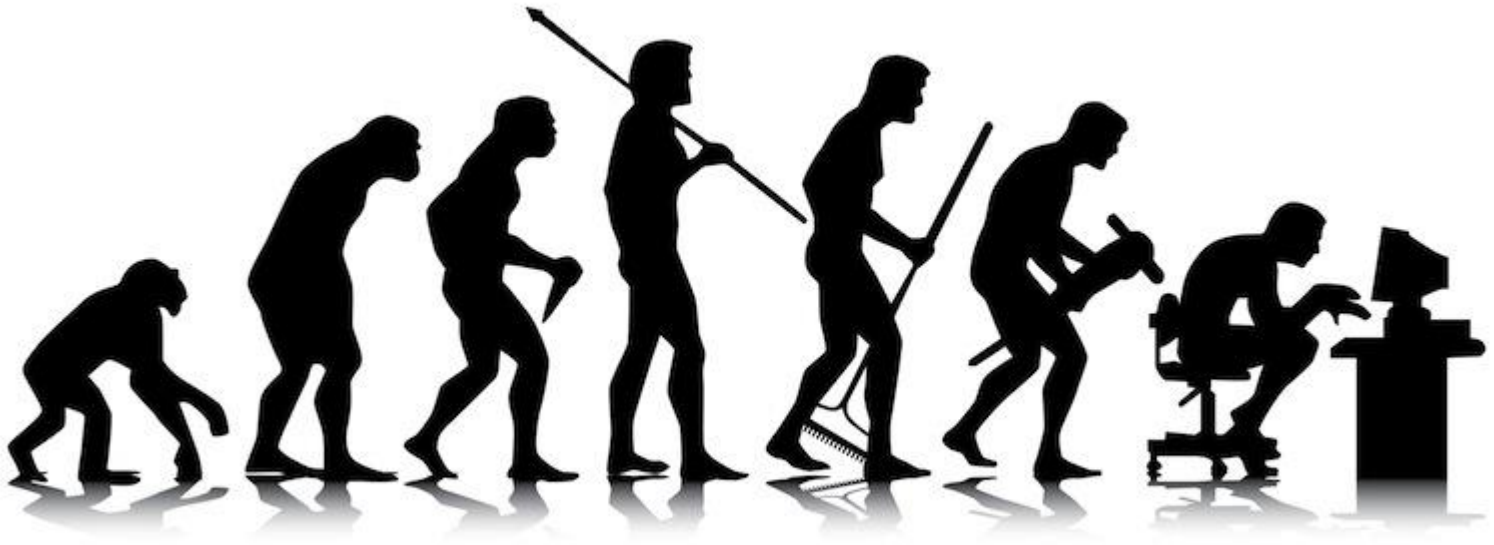
InfoGuard uses QRadar as centralized SIEM solution. Rules in QRadar ultimately fire alerts, analysts triage those and react in an appropriate predefined way.

Besides log correlation in InfoGuard also leverages comprehensive Threat Intelligence to identify malicious behaviour.



Use Case Evolution

The typical threats behind a Use Case don’t simply cease to exist. As detection mechanisms mature, we onboard additional logsources and event triggers (rules) to existing use cases to stay on top of the game.



Use Case Management

InfoGuard uses a custom database to track Use Cases throughout their lifecycle. This ensures transparency of our technical approach to identify and hunt evil.