



# WIRKUNSVOLLE CYBERDEFENCE

Aus dem Schweizer Cyber Defence Center

NEWS SPORT METEO KULTUR DOK SENDUNGEN A-Z JETZT IM TV JETZT IM RADIO PLAY SRF

SCHWEIZ ABSTIMMUNGEN REGIONAL INTERNATIONAL WIRTSCHAFT PANORAMA MEHR

Wieder globaler Angriff  
**Auch Schweizer Firmen von Cyber-Angriffe betroffen**  
Mehr zu International  
Irak stoppt das Kurden-Referendum

Diensag, 27. Juni 2017, 17:33 Uhr, aktualisiert um 20:44 Uhr

## Cyber-Angriffe legt Admeira lahm

**170 Millionen in den USA betroffen**

Die Werbevermarktungsfirma Admeira ist von der aktuellen Cyber-Angriffe hart getroffen worden. Viele Computersysteme der gemeinsamen Werbeallianz von SRG, Swisscom und Ringier sind ausser Betrieb.

Ein Cyber-Angriff legt weltweit dutzende U  
Auch Schweizer Firmen sollen betroffen se

SWISSSCHAU  
No guarantee that you can recover all assets  
need to do is submit the payment and purcha  
disruption service.  
Please follow the instructions:  
1. Send \$300 worth of Bitcoin to following  
1M7153HmuaTKZ21179mG2a4R8B8M

Zahlreiche Systeme der Werbeplattform Ac  
lahmgelegt. Bild: Manuela Spizzo

## Hackerangriff auf das Verteidigungsdepartement

Die Bundesverwaltung ist erneut Ziel einer Cyber-Angriffe geworden. Nach Angaben des Bundesrats galt der Angriff dem Verteidigungsdepartement.

Spezialisten des Bundes haben im Juli einen Cyber-Angriff «auf einzelne Server» des Verteidigungsdepartements (VBS) «entdeckt und gestoppt». Dies teilte die Bundeskanzlei am Freitag mit. Das Communiqué ist knapp gehalten. Demnach wurde der Angriff «nach einem weitgehend bekannten Muster der Malwarefamilie Turla» verübt. Sicherheitsmassnahmen seien umgehend eingeleitet und eine

Heidi Gmür, Bern  
15.9.2017, 21:47 Uhr

MEISTGELESEN IM RESSORT

**Die Russen erobern den Gotthard**  
Helmut Stalder

DATA ANALYTICS, AI & IOT FOR THE ENTERPRISE  
4 - 5 OCTOBER 2017, EXCEL LONDON

SWIFT Profits Dr...  
Matthew Broersma v. June 12, 2017, 9:41

The SWIFT transfer net expanding security oper  
The international bank t  
third as the group boost  
customer banks.

The shift followed a hack on Bangladesh's central bank in which thieves with \$81 million (£63m) by initiating fraudulent SWIFT transfer messa within the bank's own systems.

### Security concern

The heist and similar attempts led to uncertainty over how well SWIF protected, with the Bank of England ordering a review of the system i year.

In December 2016 SWIFT acknowledged attempted hacks on three unnamed banks but said none had been successful.

A breach is inevitable – Reduce the impact

# Do you spot the attack?



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

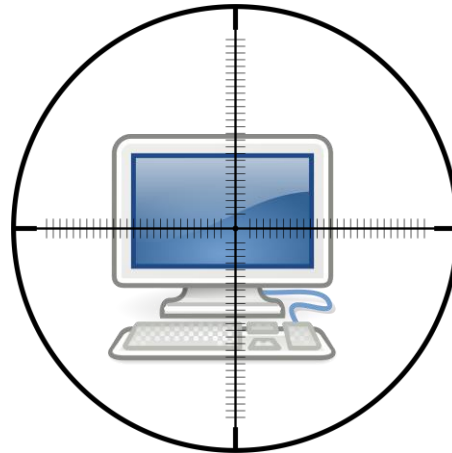
- Errors and Mistakes
- Dynamic Baselineing
- Experience

We focus on what the attacker doesn't know

# Computers in a Breach



Compromised  
Using malware



Compromised  
no malware



Untouched by  
Attacker



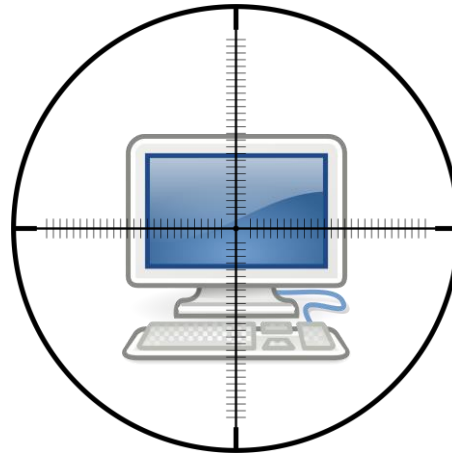
# Computers in a Breach





Compromised  
Using malware

**including rootkits**



Compromised  
no malware



Untouched by  
Attacker

**but full of crap**

Behaviour based



based Detection



What We Do

InfoGuard strives to bring Cyber Defense routines to devices and software **all available information** and **how** he is doing it

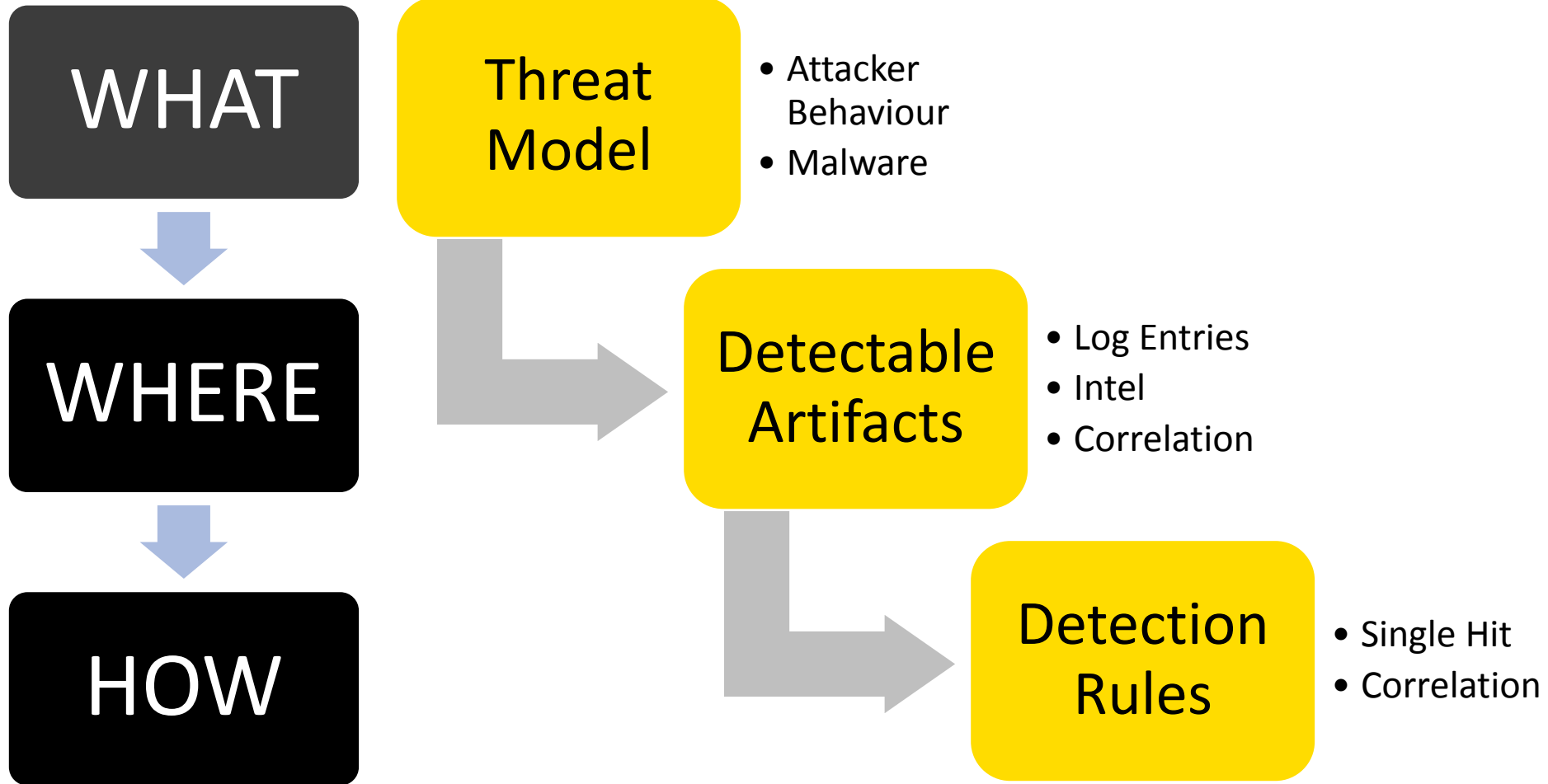
into the daily not only depend on security but on **leveraging** on **what** he is doing

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 flexibility** 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 «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.

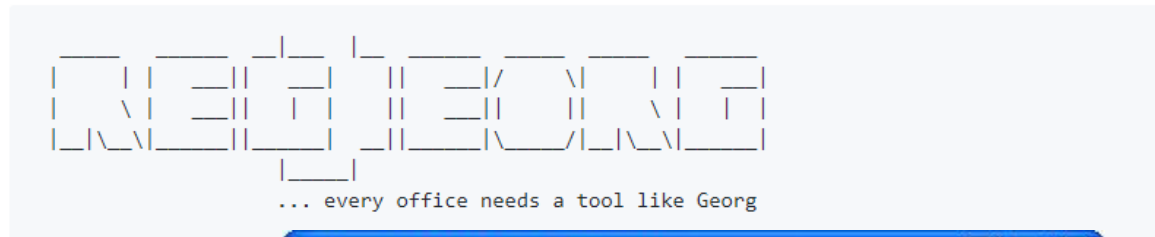
### Technical Sources

- Firewall connection log
- Windows Security Log
- Domaincontroller Logs

### Correlation Rules

- QRadar

## reGeorg



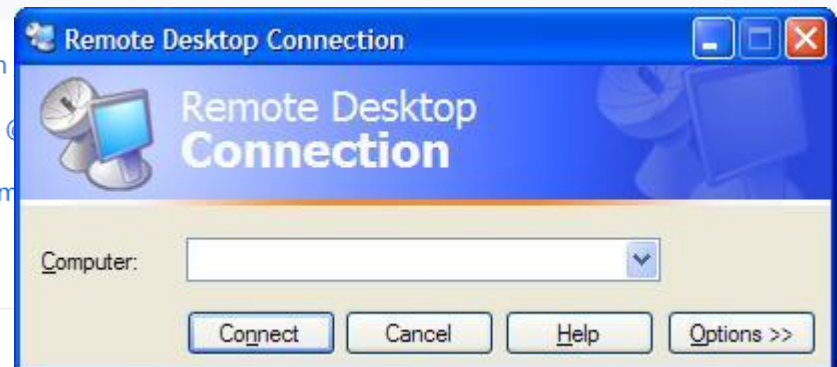
willem@sensepost.com

sam@sensepost.com / C

etienne@sensepost.com

### Version

1.0



**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.

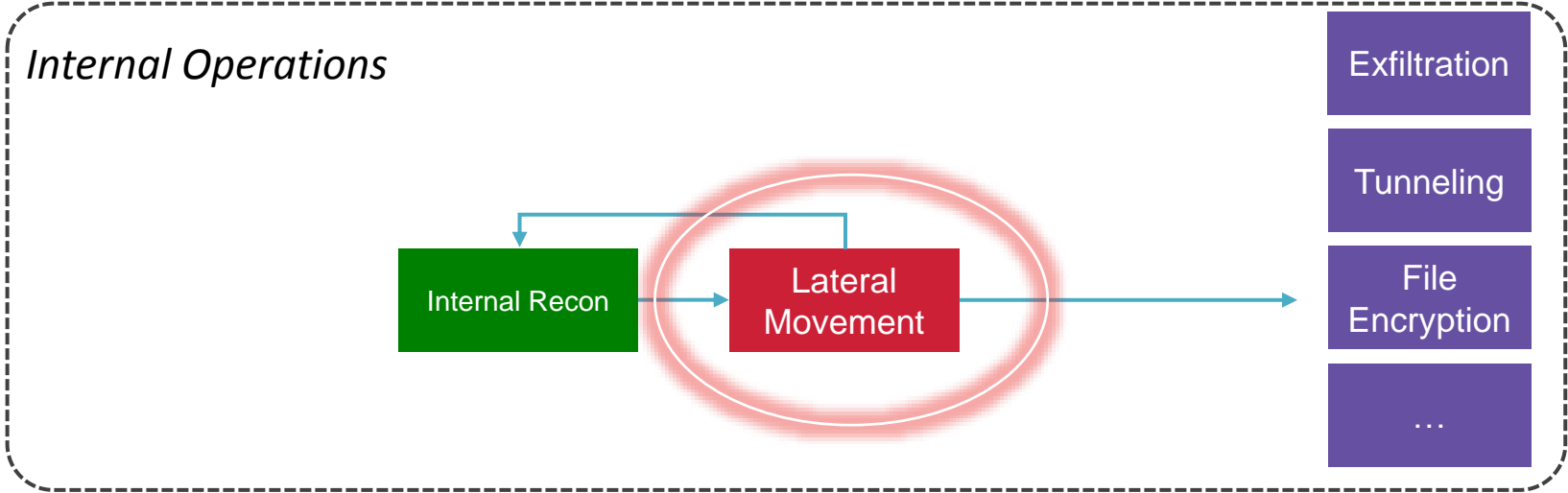
While RDP is frequently used for administrative tasks within most companies, there still is a pattern that lets us differentiate between suspicious and benign connections and connection attempts.

# Sans Kill Chain – Internal Portscan

## Targeted attack



## Opportunistic attack

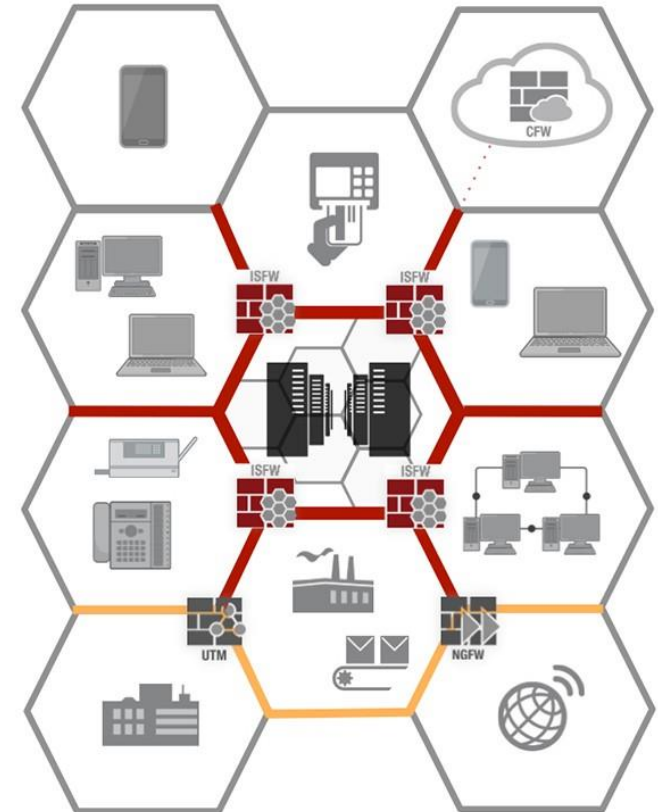


# WHERE?

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 unsuccessful 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

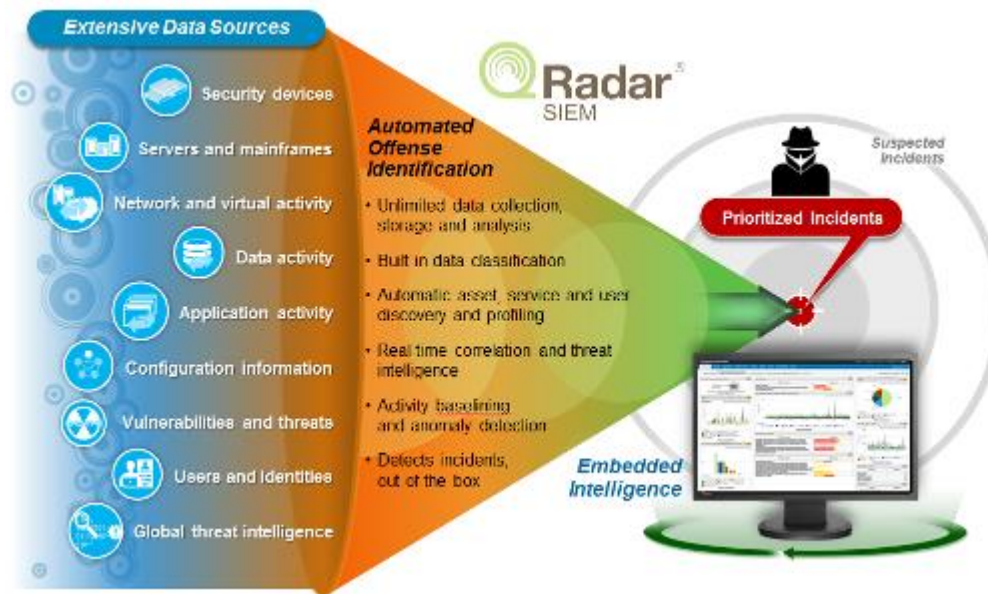




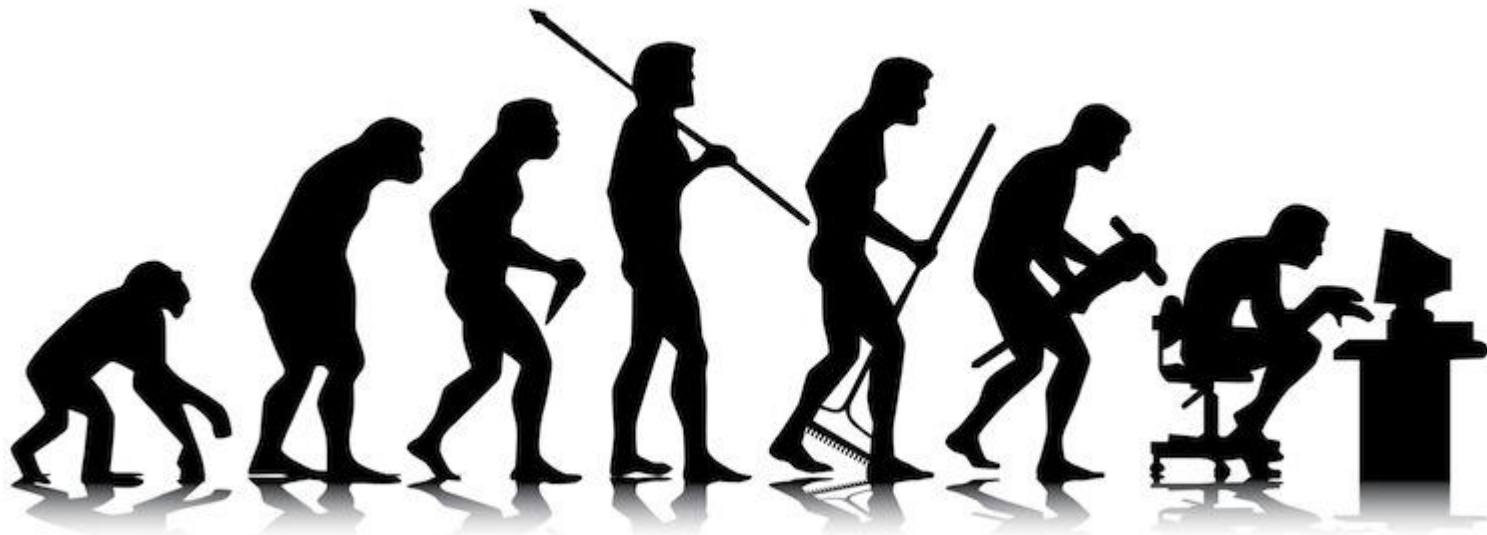
# HOW?

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.



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.**



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

The screenshot displays the InfoGuard Threat Scenario management interface. At the top, there is a navigation bar with options: Threat Scenario, SOP, Threats, Logs & Triggers, ATT&CK Framework, Response, and More. Below this is the InfoGuard logo and a search bar for Threat Scenarios. A notification states "You are now logged in".

The main content area shows a table of threat scenarios. The table has columns for checkboxes, names, categories, scopes, descriptions, response plans, and status. The visible rows are:

Checkbox	Threat Scenario Name	Category	Scope	Description	Response Plan	Status
<input type="checkbox"/>	Ransomware Activity	APT Activity	Global	System infected by Ransomware is detected by its b...	DummyResponse	NO
<input type="checkbox"/>	Malicious Service Detection	APT Activity	Global	Monitored systems will raise alarms when processes...	DummyResponse	desa NO
<input type="checkbox"/>	Production Application launching CMD/PowerShell	APT Activity	Global	Malware is often executed from Microsoft Office fi...	DummyResponse	desa NO
<input type="checkbox"/>	System Event Log Deletion	APT Activity	Global	Event logs are an important source of detecting ma...	DummyResponse	NO
<input type="checkbox"/>	Suspicious Internal Connections	APT Activity	Global	This alert is triggered by connections inside the ...	DummyResponse	NO

Below the table, there are buttons for Edit, Delete, Open in new window, and Export. The page number is 13 of 18.

The detailed view for "Internal Port Scans" is shown below. It includes a search bar and a left-hand navigation menu with options: Owner, Customer, Event Trigger, Threat Scope, Att&ck Technique, Threat Category, and Response Plan. The right-hand details panel shows:

- Connections**
  - Threat Category: APT Activity
  - Threat Scope: Internal Network
  - Response Plan: Default Breach Response
- Details**
  - Idthreatscenario: 19
  - Name: Internal Port Scans
  - Description: A port scan or portscan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself. If firewall or IDS devices detect portscans in the internal network that can be a sign of an attacker driving internal reconnaissance. The source for the portscan needs to be investigated closer.
  - Owner: mafuc