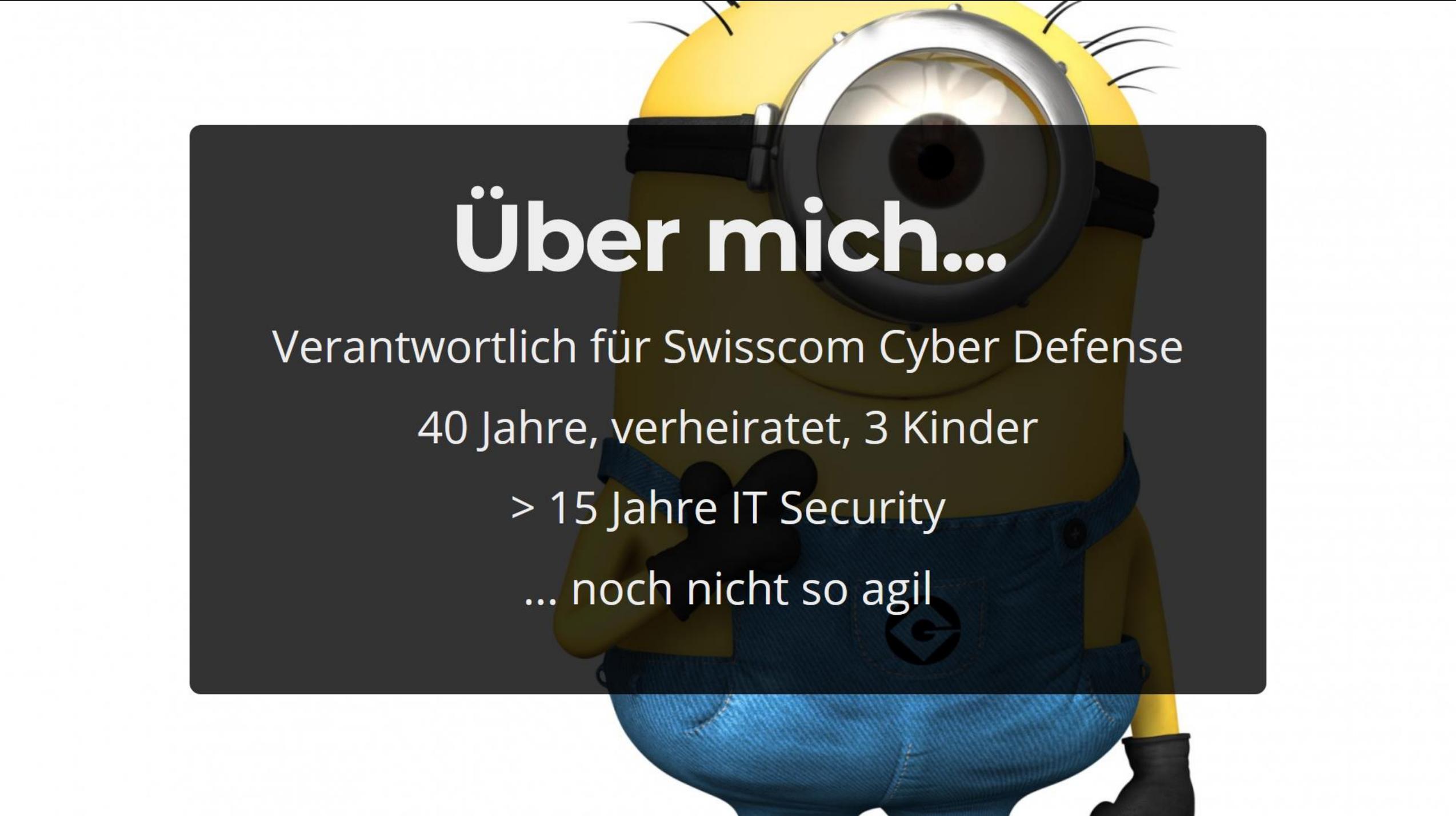


# Cyber Defense @ Swisscom

HERMES 5-Tagung, Bern



# Über mich...

Verantwortlich für Swisscom Cyber Defense

40 Jahre, verheiratet, 3 Kinder

> 15 Jahre IT Security

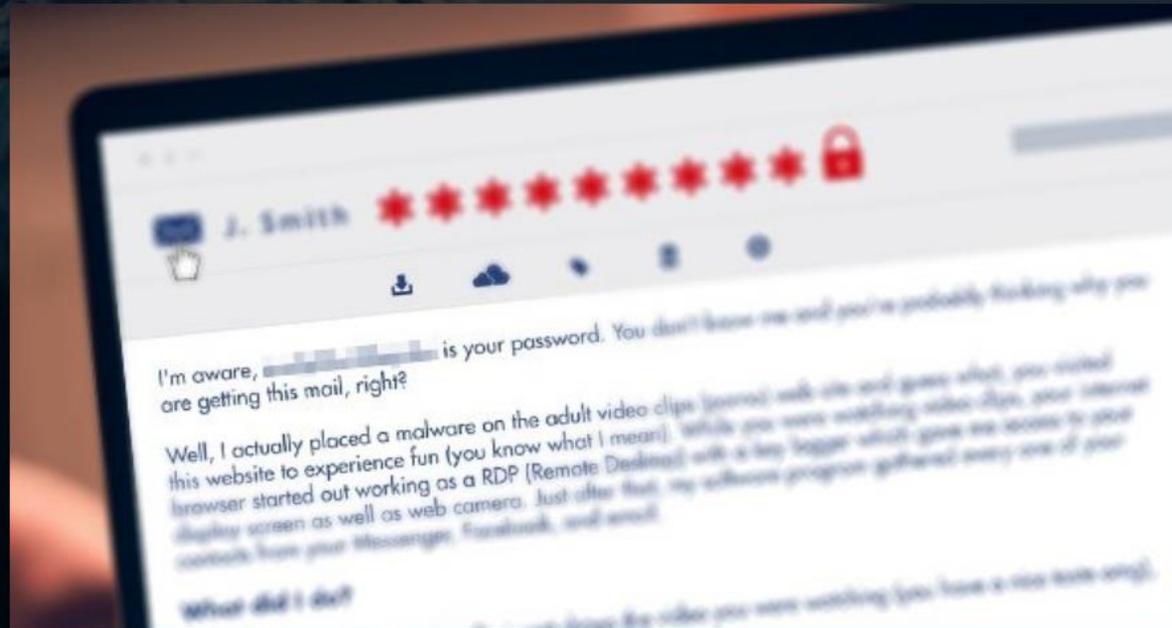
... noch nicht so agil



Was haben ...



Drohnen



## Sextortion



Crypto Mining



... gemeinsam?

A photograph of a large iceberg floating in the ocean. The visible tip of the iceberg is a jagged, snow-capped mountain peak. Below the waterline, the much larger, submerged part of the iceberg is visible, showing a complex, layered structure. The sky is blue with scattered white clouds. The water is a deep blue, and the horizon is visible in the distance.

**Das sind alles (ziemlich)  
neue Bedrohungen!**



Aber auch die Umwelt verändert sich...



**Der Druck effizient  
zu sein, steigt...**

A close-up photograph of a brass aneroid barometer. The device has a white face with a circular scale and various weather-related labels. The scale shows pressure values in hPa, with major markings at 970, 980, 990, 1000, 1010, 1020, 1030, 1040, 1050, and 1060. Weather conditions are labeled around the scale: 'Stormy' (around 970-980 hPa), 'Rain' (around 980-990 hPa), 'Change' (around 1000-1010 hPa), 'Fair' (around 1020-1030 hPa), and 'Very Dry' (around 1050-1060 hPa). The number '31' is visible on the right side of the scale. The brass casing is highly reflective. A semi-transparent dark grey rectangular box is overlaid in the center of the image, containing white text.

**Jeden Monat  
ungefähr...**



20

Sicherheitsvorfälle, die vom CSIRT bearbeitet werden



**3'000**

Phishing Angriffe, die detektiert und blockiert werden



**2'200**

Kundenrechner, die aufgrund einer Infektion mit Malware präventiv in Quarantäne gestellt werden



**2'100'000**

blockierte Angriffsversuche gegen die  
Swisscom Infrastruktur



**2'500**

kontaktierte Kunden aufgrund gehackter  
Accounts

A cheetah is captured in motion, running across a dry, dusty plain. The cheetah's body is low to the ground, and its tail is extended. The background is a blurred, golden-brown landscape. A large, dark, semi-transparent rectangular box is overlaid on the center of the image, containing the text "Agile Incident Response" in white, bold, sans-serif font.

# Agile Incident Response

A cheetah is captured in a full sprint across a dry, dusty plain. The cheetah's body is low to the ground, and its legs are extended in a powerful stride. The background is a vast, open landscape with sparse, dry vegetation. A semi-transparent black rectangular box is overlaid on the center of the image, containing the text "Was braucht es dazu?".

**Was braucht es dazu?**

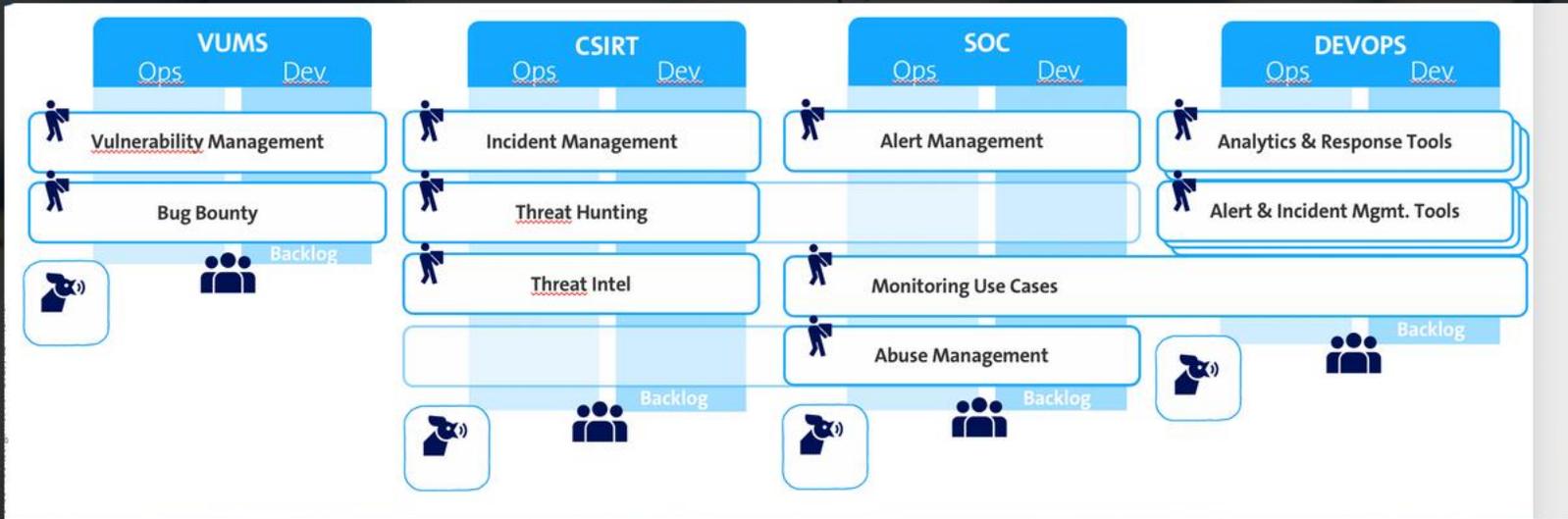


# Eine passende Organisation



The background features a hand-drawn diagram on a glass surface. A central cloud contains several boxes with labels: 'Tenant', 'Service', 'Service (shared)', and 'Tenant'. Below the cloud is a globe with lines connecting it to the cloud. To the left, a box contains the number '21'. To the right, a box contains three vertical bars and a dot. Arrows and other lines connect these elements, suggesting a flow or relationship between different components of an organization.

# "Agile" Organisationsformen



A hand-drawn diagram on a glass wall, featuring a central cloud shape containing several boxes with labels: 'Tenant', 'Service', 'Service (shared)', 'Tenant', and 'External Service'. Below the cloud is a globe icon. To the left, a box contains the number '21'. To the right, a box contains three vertical bars and a dot. The background shows a blurred office interior with people.

Eine "agile" Kultur



z.B. "Fail Fast" Kultur



The image shows a JIRA Kanban board for 'CSIRT Security Incidents'. The board is titled 'Kanban board' and has a 'Board' dropdown menu. It features several columns representing different stages of the incident response process: New, Investigation, Containment, Eradication, Recovery, Resolved, and Closed. The board is populated with several issues, including 'SIM-379', 'SIM-421', 'SIM-414', 'SIM-373', 'SIM-200', and 'SIM-388'. The issues are organized into swimlanes based on their priority: 'P0 - Crisis (Blocker) 1 issue', 'P1 - Critical (Critical) 1 issue', and 'P2 - High (Major) 5 issues'. The board also includes a 'QUICK FILTERS' section with options like 'Hide Test', 'Hide Sub-Tasks', 'Only My Incidents', and 'Recently Updated'. The background of the image is a wooden workbench with various tools like a saw, pliers, a brush, a hammer, and a screwdriver.

Steuerung mit agilen Tools

New chat Search

Swisscom

ROOMS

- Group Security
- Group Security - Manage...
- GSE-CYD
- GSE-CYD-CIC**
- [Redacted]
- CSIRT | Coordination
- CSIRT | Intel Operations
- CSIRT | Forensics
- CSIRT | Communication
- CSIRT | Threat Hunting
- + Create a room

**GSE-CYD-CIC**  
KW07: IM: Stefan (Mo-Di), Claudio (Mi-Fr) IH: Pool (https://c...swisscom.com...)

Thursday February 7, 2019

Splunk-Seclog · Feb-7 01:32

**Sysmon Daily Stats**  
seclog.swisscom.com

1335 binaries first seen. 31 with 1 VT positive, 11 with 2-5 VT positives, 6 with >5 VT positives. Max VT positive score is 41

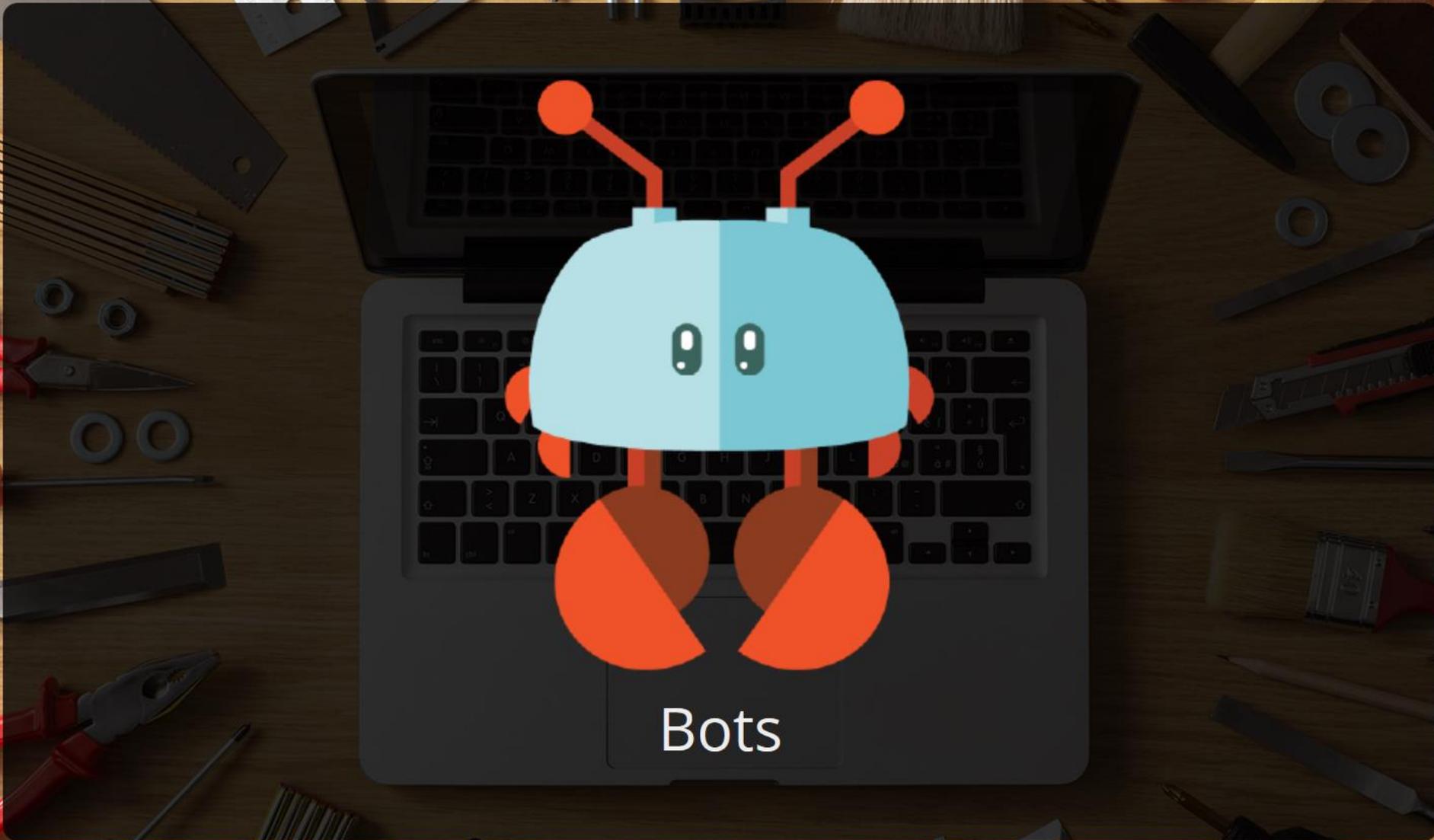
Hunkeler Andreas, GSE-CYD · Feb-7 11:27  
lpassive [Redacted]

SA-PF000 CSIRT, GSE-MON · Feb-7 11:27

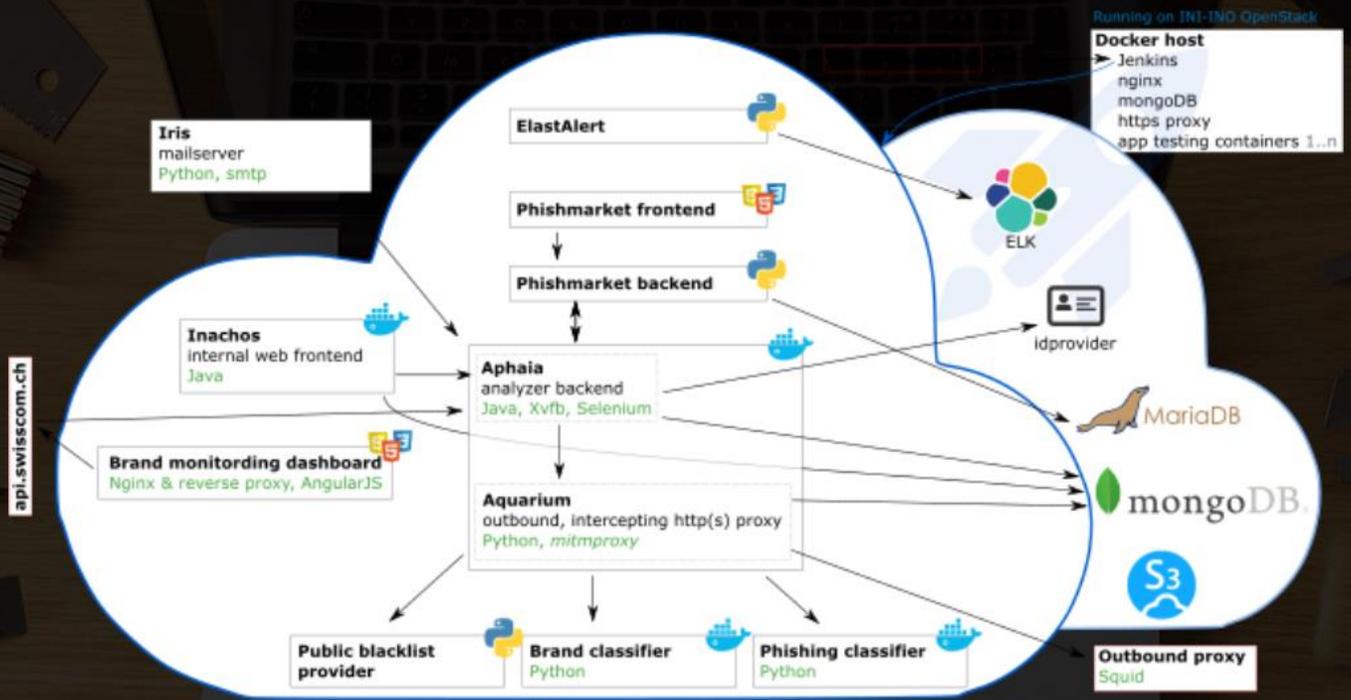
3.	2016-09-06 22:00:00	2019-02-07 09:00:00	48	[Redacted]	[Redacted]
4.	2016-12-21 12:51:38	2019-02-07 01:00:50	108	[Redacted]	ns3.hostpoint.ch
5.	2016-12-21 12:51:38	2019-02-07 01:00:50	108	[Redacted]	ns.hostpoint.ch
6.	2016-12-21 12:51:38	2019-02-07 01:00:50	108	[Redacted]	ns2.hostpoint.ch
7.	2017-07-12 09:24:18	2018-09-09 18:09:14	13	[Redacted]	10 mx1.mail.hostpoint.ch

[Show more](#)

ChatOps



Bots



# Machine Learning



# Klare Prozesse

## Procedure

Offizielle Version ist hier abgelegt: <https://collaboration.swisscom.com/confidential/isms-sc/Documents/Forms/AllItems.aspx?RootFolder=%2Fconfidential%2Fisms-sc%2FDocuments%2F09%2E%20Pro>

 Incident Manager	 Incident Responder/ S/R Owner	 Incident Responder/ S/R Owner	 Incident Responder/ S/R Owner	 Incident Manager
 <p style="text-align: center;"><b>Identification and Assessment</b></p> <p style="text-align: center;">15-60 min</p>	 <p style="text-align: center;"><b>Containment</b></p>	 <p style="text-align: center;"><b>Eradication</b></p>	 <p style="text-align: center;"><b>Recovery</b></p>	 <p style="text-align: center;"><b>Lessons Learned</b></p> <p style="text-align: center;">1-8h</p>
<ul style="list-style-type: none"> <li>• Infos über Incident auswerten</li> <li>• IR definieren</li> <li>• Initiales Meeting</li> <li>• Incident charakterisieren</li> <li>• Vor Ort Team nötig?</li> <li>• Ticket erstellen</li> <li>• Kommunikation</li> </ul>	<ul style="list-style-type: none"> <li>• Beweissicherung</li> <li>• Massnahmen einleiten um das Problem einzudämmen</li> </ul>	<ul style="list-style-type: none"> <li>• Ursache des Problems finden</li> <li>• Behebung des Problems</li> <li>• Verbesserung des Schutzes</li> <li>• Vergleichbare Probleme identifizieren</li> </ul>	<ul style="list-style-type: none"> <li>• Wiederherstellung</li> <li>• Validierung</li> <li>• Überwachung</li> </ul>	<ul style="list-style-type: none"> <li>• Debriefing</li> <li>• Dokumentation</li> <li>• Anwenden der Korrektur-Massnahmen</li> </ul>
<p style="text-align: center;">  6f                        2w                        6h                 </p>	<p style="text-align: center;">  6g                 </p>	<p style="text-align: center;">  6g                 </p>	<p style="text-align: center;">  6g                 </p>	<p style="text-align: center;">  2c                 </p>
<p><b>Roles:</b></p> <ul style="list-style-type: none"> <li>Incident Responder <b>R</b></li> <li>Incident Manager <b>A</b></li> <li>Security Delivery <b>S</b></li> <li>S/R Owner <b>C</b></li> <li>OIM, SecOff, CSO <b>I</b></li> </ul>	<p><b>Roles:</b></p> <ul style="list-style-type: none"> <li>IncRes, S/R Owner <b>R</b></li> <li>Incident Manager <b>A</b></li> <li>Security Delivery <b>S</b></li> <li>- <b>C</b></li> <li>OIM, SecOff, CSO <b>I</b></li> </ul>	<p><b>Roles:</b></p> <ul style="list-style-type: none"> <li>Incident Responder <b>R</b></li> <li>Incident Manager <b>A</b></li> <li>Security Delivery <b>S</b></li> <li>S/R Owner <b>C</b></li> <li>- <b>I</b></li> </ul>	<p><b>Roles:</b></p> <ul style="list-style-type: none"> <li>Incident Responder <b>R</b></li> <li>Incident Manager <b>A</b></li> <li>Security Delivery <b>S</b></li> <li>S/R Owner <b>C</b></li> <li>- <b>I</b></li> </ul>	<p><b>Roles:</b></p> <ul style="list-style-type: none"> <li>Incident Manager <b>R</b></li> <li>Incident Manager <b>A</b></li> <li>IncRes, S/R Owner <b>S</b></li> <li>- <b>C</b></li> <li>OIM, CSO, SecOff <b>I</b></li> </ul>

# Prozeduren & Prozesse

# Checklists

---

- AAA - Common Sub-Workflows
  - Subworkflow - Activate corresponding IPS rule
  - Subworkflow - Analyze forensic evidence
  - Subworkflow - Block access to external malicious resources
  - Subworkflow - Block compromised accounts
  - Subworkflow - Close Incident
  - Subworkflow - Communication
  - Subworkflow - Forensic evidence collection
  - Subworkflow - Handover to Crisis organization
  - Subworkflow - Handover to Major Incident Management
  - Subworkflow - High Incident
  - Subworkflow - Isolate affected resources from the network
  - Subworkflow - Lessons Learned
  - Subworkflow - Prioritize Incident
  - Subworkflow - Setup custom monitoring
  - Subworkflow - Start Incident
- Checkliste Incident Handling
- Compromised Accounts
- D1 - Unauthorized Access
- D2 - Denial of Service
- D3 - Vulnerabilities



... aber es gibt auch spezielle Fälle ...

A dramatic image of a nuclear mushroom cloud rising from a city. The cloud is massive, with a dark, dense stem rising from the city and a large, billowing, white and grey top. The city below is densely packed with buildings, and the sky is a hazy, golden-brown color, suggesting a sunset or sunrise. The overall tone is ominous and catastrophic.

# "DER" Datendiebstahl

A large, dark, billowing mushroom cloud from a nuclear explosion rises from a cityscape. The cloud is composed of thick, dark grey and black smoke and debris, with a lighter, more turbulent top section. The city below is densely packed with buildings, and the sky is a hazy, yellowish-brown color, suggesting a post-apocalyptic or war-torn environment.

**800'000**

gestohlene Kundendatensätze

# Swisscom-Leck: «Fahrlässig, wie die Daten gesichert waren»

Bei den gestohlenen 800'000 Kundendaten handle es sich um sensible Informationen, kritisiert der Zürcher Datenschützer die Swisscom.

07.02.2018

## Feedback

Tragen Sie mit

[Hinweisen](#) zu diesem

Artikel bei oder melden

Sie uns [Fehler](#).

Unbekannte haben sich im Herbst 2017 missbräuchlich die Kontaktangaben von rund 800'000 Swisscom-Kunden verschafft. Sie hatten dafür die Zugriffsrechte eines Vertriebspartners des Telekomriesen entwendet. Die verschärft nun die Sicherheitsmassnahmen.

Betroffen sind laut [Swisscom](#) Name, Adresse, Telefonnummer und Geburtsdatum, wie es in einer Mitteilung vom Mittwoch heisst. Es handle sich also grösstenteils um Kontaktdaten, die öffentlich oder über Adresshändler verfügbar seien.

## «Unklar, was mit den Daten passiert»

Der Eidgenössische Datenschutz- und

## Artikel zum Thema

### Swisscom verdient 1,57 Milliarden und baut 700 Stellen ab



Die Swisscom musste 2017 einen Gewinnrückgang hinnehmen. 684 Stellen wurden abgebaut. Bis Ende Jahr sollen 700

A large, billowing mushroom cloud of nuclear fallout rises from a cityscape, symbolizing a catastrophic event. The cloud is dark and dense at the base, transitioning to a lighter, more textured top. The city below is a dense grid of buildings, with a body of water visible in the distance under a hazy, yellowish sky.

**Was gab es alles zu  
organisieren?**



Sofortmassnahmen / Eindämmung

A large, billowing mushroom cloud of nuclear fallout rises from a cityscape. The cloud is composed of dark, dense smoke at the base, transitioning to lighter, more dispersed particles as it ascends. The city below is a dense grid of buildings, with a body of water visible in the distance. The sky is a hazy, yellowish-brown color, suggesting a post-apocalyptic or war-torn environment.

Analyse / Beschaffen von Daten

A large, billowing mushroom cloud of nuclear fallout rises from a cityscape, symbolizing a catastrophic event. The cloud is dark and dense at the base, transitioning to a lighter, more textured top. The city below is a dense grid of buildings, with a body of water visible in the distance under a hazy, yellowish sky.

Information Kunden, Behörden und Medien  
vorbereiten

A large, billowing mushroom cloud of nuclear fallout rises from a cityscape. The cloud is composed of thick, dark grey and brown smoke and debris, with a lighter, more turbulent top section. The city below is densely packed with buildings, and the sky is a hazy, yellowish-brown color, suggesting a sunset or sunrise. A dark, semi-transparent rectangular box is overlaid on the middle of the cloud, containing white text.

Zusätzliche Schutzmassnahmen definieren  
und umsetzen

A large, billowing mushroom cloud of nuclear fallout rises from a cityscape. The cloud is composed of dark, dense smoke at the base, transitioning to lighter, more dispersed clouds at the top. The city below is densely packed with buildings, and the sky is a hazy, yellowish-brown color, suggesting a post-apocalyptic or disaster scenario.

# Rechtliche Massnahmen



uvm...

A large, dark, billowing mushroom cloud from a nuclear explosion rises from a cityscape. The cloud has a thick, dark stem and a large, billowing, grey and white top. The city below is densely packed with buildings, and the sky is a hazy, yellowish-brown color. The overall scene is one of destruction and devastation.

# Organisation in Form einer Taskforce

A large, billowing mushroom cloud of nuclear fallout rises from a cityscape. The cloud is composed of dark, dense smoke at the base, transitioning to lighter, more textured clouds as it ascends. The city below is densely packed with buildings, and the sky is a hazy, yellowish-brown color, suggesting a post-apocalyptic or war-torn environment.

Warum?

A large, dark, billowing mushroom cloud from a nuclear explosion rises from a cityscape. The city below is densely packed with buildings, and the sky is filled with a hazy, yellowish light, suggesting a sunset or sunrise. The mushroom cloud is the central focus, with its stem rising from the city and its large, rounded top spreading out in the sky.

Grössere Flexibilität  
Übergreifende Zusammenarbeit  
Vertraulichkeit  
Tempo  
"Standards" passen einfach nicht

A large, billowing mushroom cloud of nuclear fallout rises from a cityscape. The cloud is composed of dark, dense smoke at the base, transitioning to lighter, more dispersed particles at the top. The city below is densely packed with buildings, and the sky is a hazy, yellowish-brown color, suggesting a sunset or sunrise. A dark, semi-transparent rectangular box is overlaid on the middle of the cloud, containing white text.

Aber... aufbauend auf etablierten Elementen

A large, dark, billowing mushroom cloud from a nuclear explosion rises from a cityscape. The city below is filled with smoke and debris, and the sky is a hazy, yellowish-brown. A dark, semi-transparent rectangular box is overlaid on the center of the cloud, containing white text.

Steuerung mit Kanban

ChatOps

...

A comic book illustration of Superman flying through a sky filled with white and yellow clouds. He is wearing his iconic blue suit with a red cape and a yellow 'S' on his chest. His right arm is extended forward, and his left arm is bent at the elbow. The background is a deep blue sky with scattered white clouds.

# Fazit

Agile Methoden ("doing agile") helfen, aber nicht in jeder Situation...

Wichtiger ist ein agiles Mindset! ("being agile")



Vielen Dank!