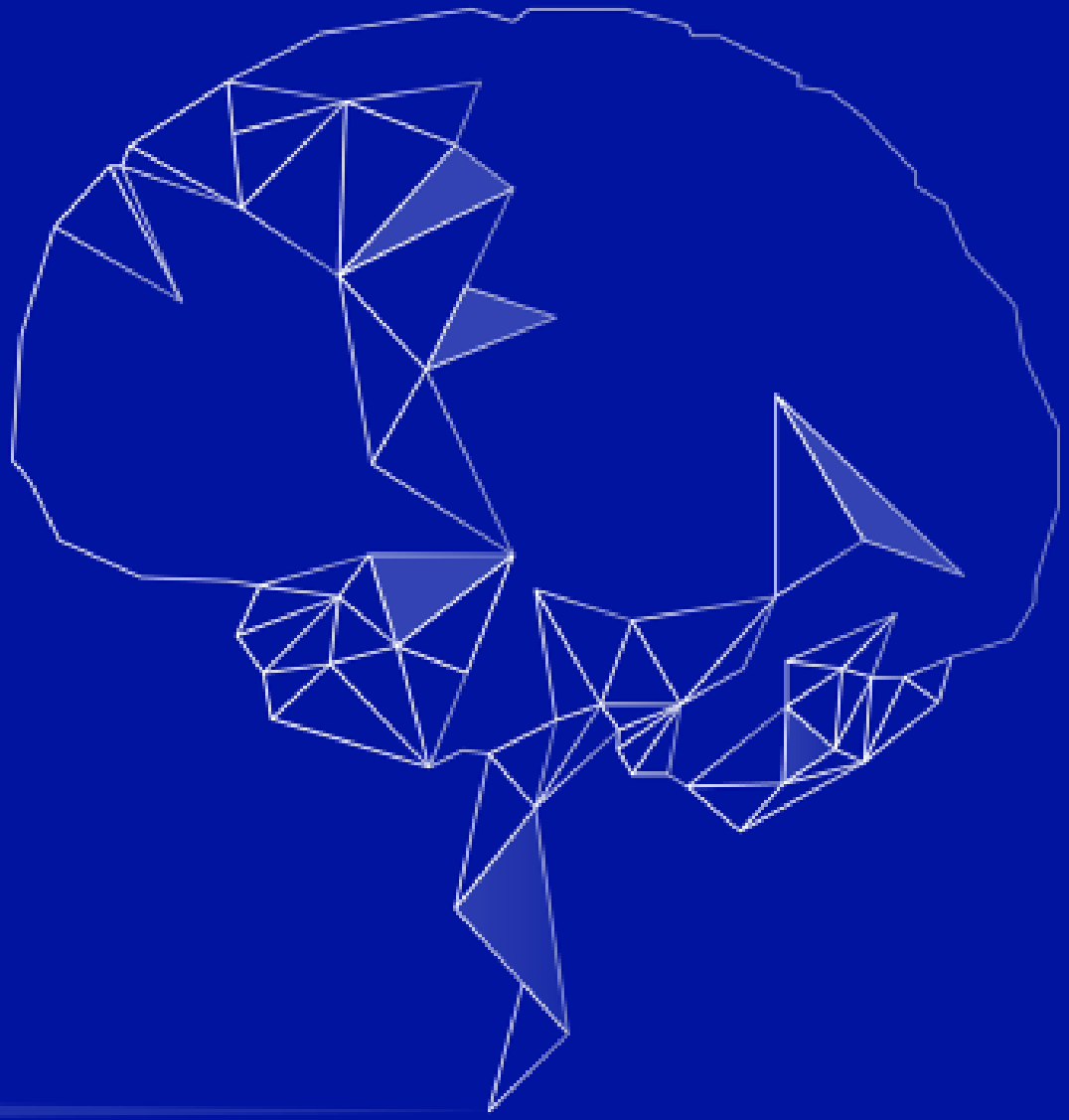
MAN & MACHINE IN DETECTION & RESPONSE

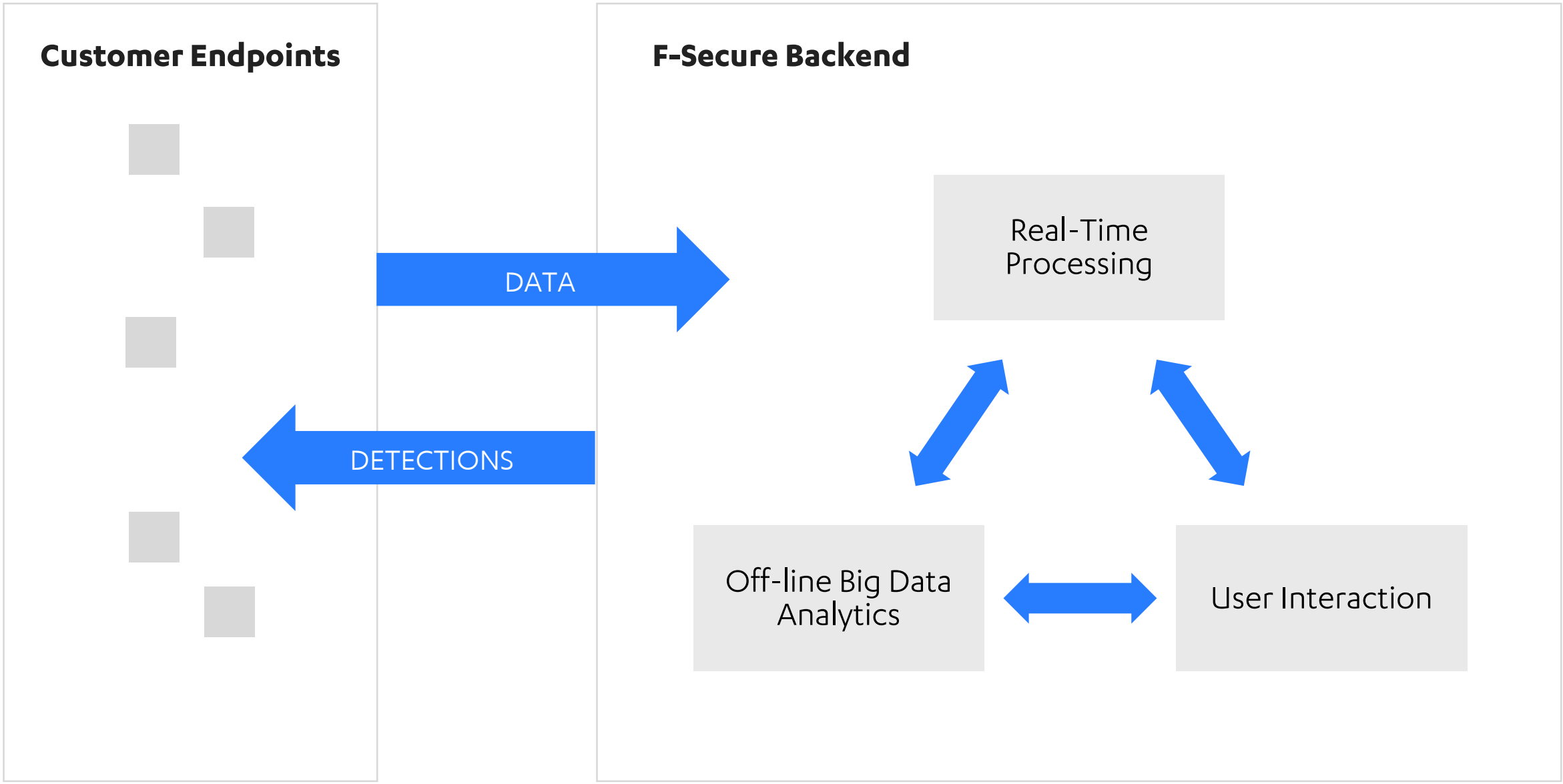
Sami Ruohonen | Tactical Defense Unit | F-Secure

F-Secure

ARTIFICIAL INTELLIGENCE



F-Secure.


Customer Endpoints
F-Secure Backend
DATA
DETECTIONS
Real-Time Processing
Off-line Big Data Analytics
User Interaction

DATA COLLECTION SENSORS

HUMAN IN DETECTION AND RESPONSE

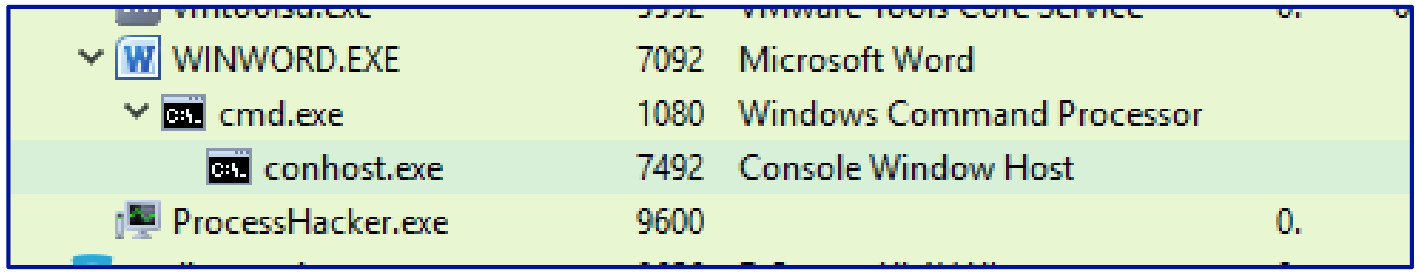
Practical example

F-Secure

HUMAN IN DR #1: DETECTING ANOMALOUS PROCESSES

Is the new process which is starting suspicious?

1. New process is launched
2. Is this combination very rare (i.e. anomalous)?
3. Can any of these processes used maliciously?



F-Secure

HUMAN IN DR #2: DETECTING DEFENSE EVASION

Assumption: most people who are not up to something odd don't try to hide their actions

1. Analyze the script
2. Is the script obfuscated?

```
<html><body><textarea id="KSHD29FC" style="display:none;">115,52,81,71,66,64,50,
42,114,83,93,102,43,40,51,119,76,34,111,123,74,75,97,96,90,32,44,45,37,104,57,58,94,116,
82,108,87,112,85,110,117,86,121,103,124,63,79,84,62,38,89,88,105,91,35,126,68,65,69,55,
118,100,125,53,107,92,113,47,54,106,122,99,95,39,72,77,120,61,78,70,73,98,36,46,59,67,
80,49,41,56,48,109,60,101,33</textarea>
<div style="display:none;" id="KSHD29FCa">+
%5D%60H%20sG8Jg%3AWALPT1X210G@Q9%3CkExH%5DP%3D+%3Dn%26%2CM-HIxd%
3A3_W/eCGZM%5D%7D%209*jm6%7C9*G/%2CjT*hGZ%7E%5DLw2%20/+Gt%3CK9O%3B
/H%3C%3Do%21TQ%3DC%3Dy%7D._9i%3E-lc/%7E%23G%24F%5DkSsu%60EP%216

        . . .

%5EdG219R6zwIted%5EPXEga%5DIV+%23%22-c%29xo%5Bt</div>
<script>function skfjAd08djs(Cd9fs){return String["fromCharCode"](Cd9fs);}</script>
<script>function xh7z8ckkMGe(FFzD54hch5){var Cc9yP8XdVx8M=0,rcA29Zt,
TbxK0cw=FFzD54hch5.length, MMsk77R3=0,EkI59FcVW="";
Ceup1xb=document.getElementById('KSHD29FC').value.split(',');
for(;Cc9yP8XdVx8M<TbxK0cw;Cc9yP8XdVx8M++){if(!MMsk77R3)
{eval("rcA29Z"+"t=125^FFzD54hch5.cha"+"rCo"+"deAt(Cc9yP8XdVx"+"8M)&2"+"55");
eval("EkI59FcVW+"+"=skfjAd08djs(Ceup1xb[(125"+"^rcA29Zt)-"+"32])");
MMsk77R3=2;}else{MMsk77R3--;}}return (EkI59FcVW);}var
Ii2nzK=window["unesc"+"ape"](document.getElementById('KSHD29FCa').innerHTML);
eval(xh7z8ckkMGe(Ii2nzK));</script></body></html>
```


F-Secure

HUMAN IN DR #2: PROBLEMS

AI IN DETECTION AND RESPONSE

Practical example

F-Secure

AI IN DR #1: ANOMALOUS PROCESS CREATION DETECTION

Is the new process which is starting suspicious?

1. New process is launched
2. We know the parent and the child processes
3. Is this combination very rare (i.e. anomalous)?

Parent process	Child process	Score
Explorer.exe	Chrome.exe	0.05
Explorer.exe	Winword.exe	0.008
Chrome.exe	Acroread32.exe	0.001
Mail.exe	Winword.exe	0.03
Winword.exe	Powershell.exe	0.000001
Chrome.exe	Chr-tmp-dfadfs-installer.exe	0.0002
Chr-tmp-dfadfs-installer.exe	Chrome.exe	0.0004
Winword.exe	Excel.exe	0.07
Explorer.exe	Wow.exe	0.002

F-Secure

AI IN DR #2: OBFUSCATION DETECTION

Assumption: most people who are not up to something odd don't try to hide their actions

1. Analyze command line parameters of a Powershell command
2. Is the command line obfuscated?

```
SQBGACgAJABQAFMAVgBFAFIAcwBJAE8ATgBUAEEAQgBsAEUALgBQAFMAVgBFAFIAcwBpA
AC0AZwBFACAAMwApAHsAJABHAFAARgA9AFsAUgBlAEYAXQAuAEEAUwBTAGUATQBiAEwAe
KAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhA
AHMAJwApAC4AIgBHAGUAdABGAEkARQBgAEwARAAiACgAJwBjAGEAYwBoAGUAZABHAHIAb
UwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0A
ACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYALgBHAEUAdABWAGEATABVAGUAK
RgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnA
AFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJ
ZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwA
AHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AY
dABCAGwAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9A
AG8ATABMAEUA
```

F-Secure

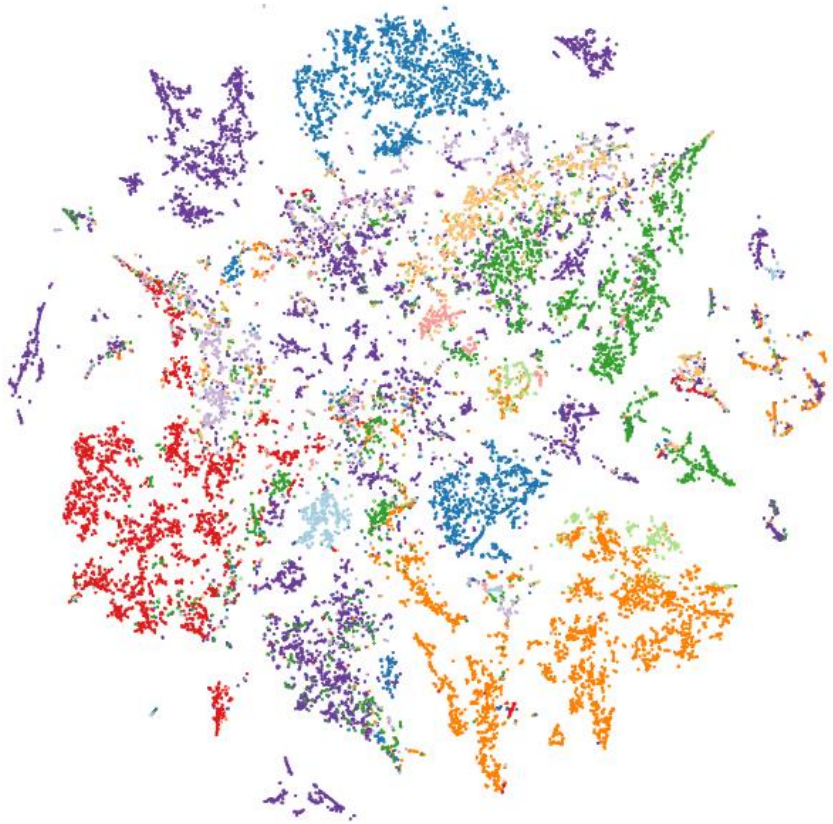
MACHINE LEARNING IMPROVED ACCURACY FROM 62% TO 99,995%

F-Secure

AI IN DR #3: HOST PROFILING

We automatically profile types of hosts, and the profiles can then be used to:

1. Categorize new hosts
2. Prioritize or refine detections
3. Identify contextually anomalous behavior



F-Secure

AI IN DR #4: DETECTION FALSE POSITIVE PREVENTION

Is this detection a false positive?

1. Our threat hunters (or partners) analyze and label some detections as false positives
2. We build and automatically retrain classifiers using these labels and the context of the detection
3. Each incoming detection is ranked in real time by the classifier

F-Secure

AI IN DR #2: PROBLEMS

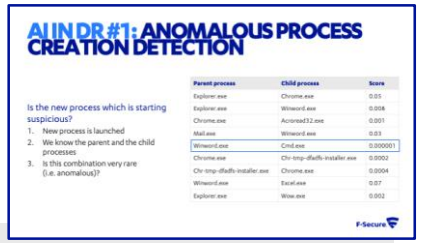
F-Secure

Customer Endpoints

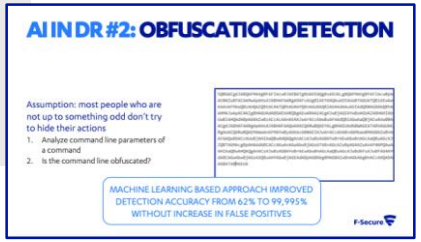
DATA

DETECTIONS

F-Secure Backend

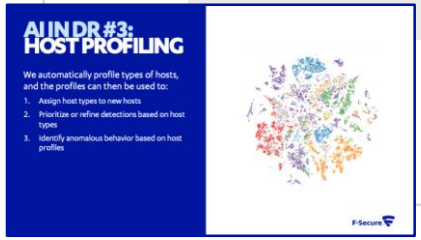


Real-Time Processing



Off-line Big Data Analytics

User Interaction



F-Secure

SUMMARY

- Process flow
- Overcoming problems


F-Secure®