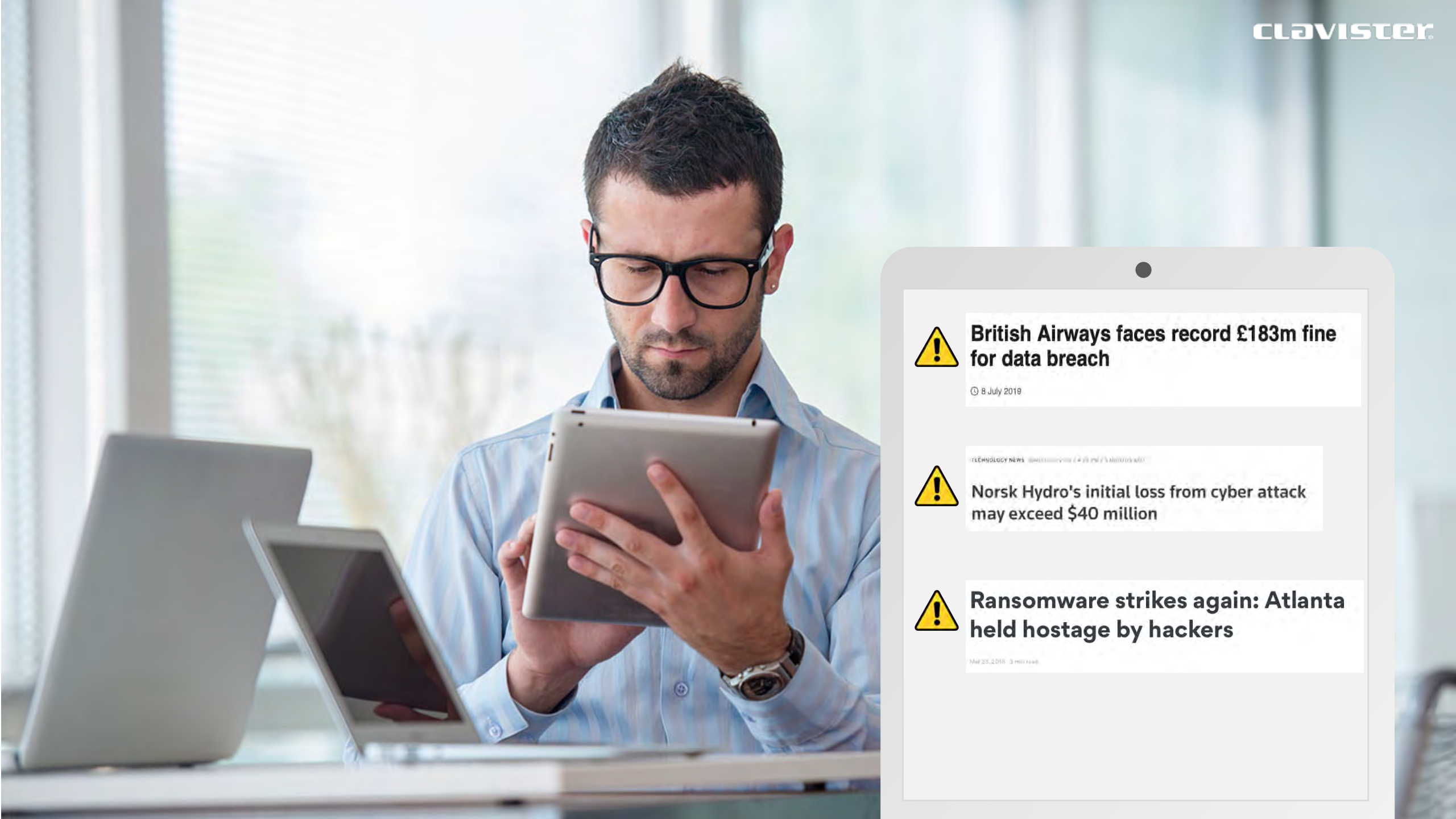
Get scored! Find out if you are as protected as you think.

Clavister Protects Webinar

2020Q1-0306

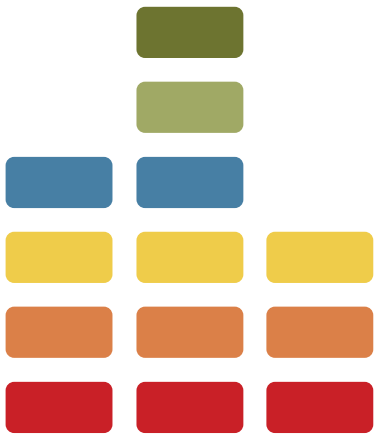

John, CEO


Anna, IT Manager


British Airways faces record £183m fine for data breach
8 July 2019
TECHNOLOGY NEWS
Norsk Hydro's initial loss from cyber attack may exceed $40 million
Ransomware strikes again: Atlanta held hostage by hackers

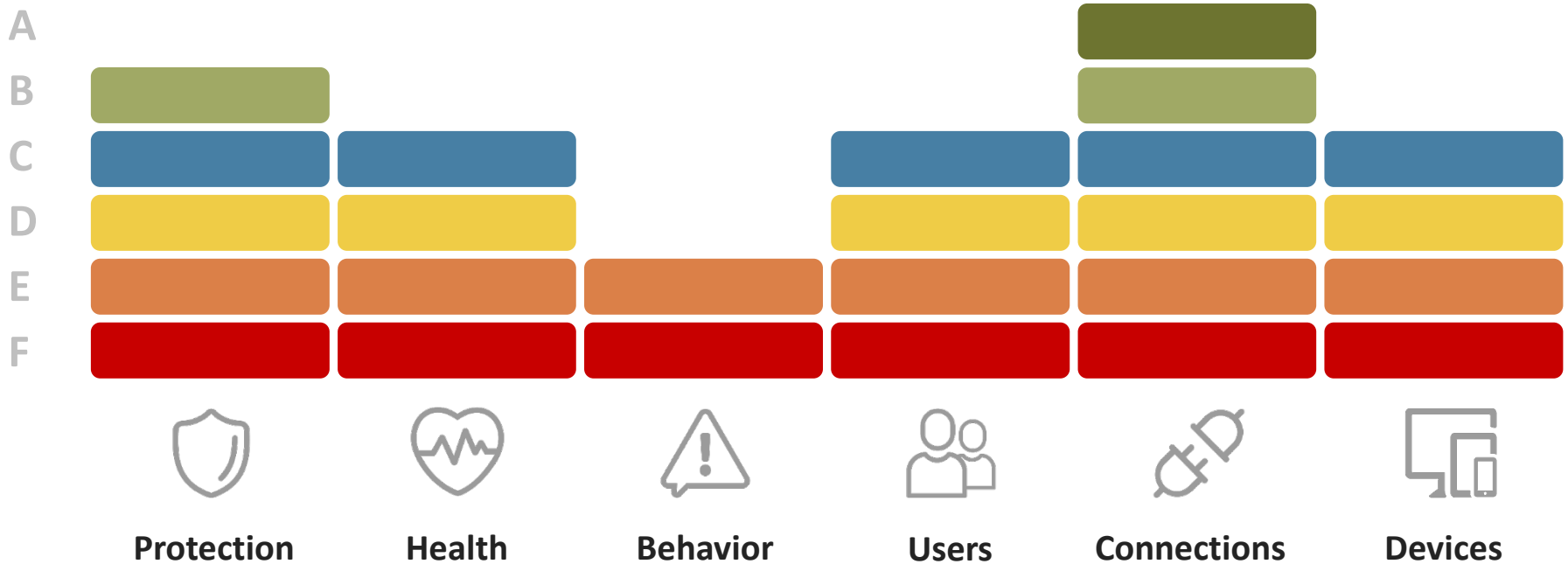

?
!
clavister


ENERG
A+++
A++
A+
A
B
C
D
E
A+++
A+++ !!!



CyberSecurity™ ScoreCard

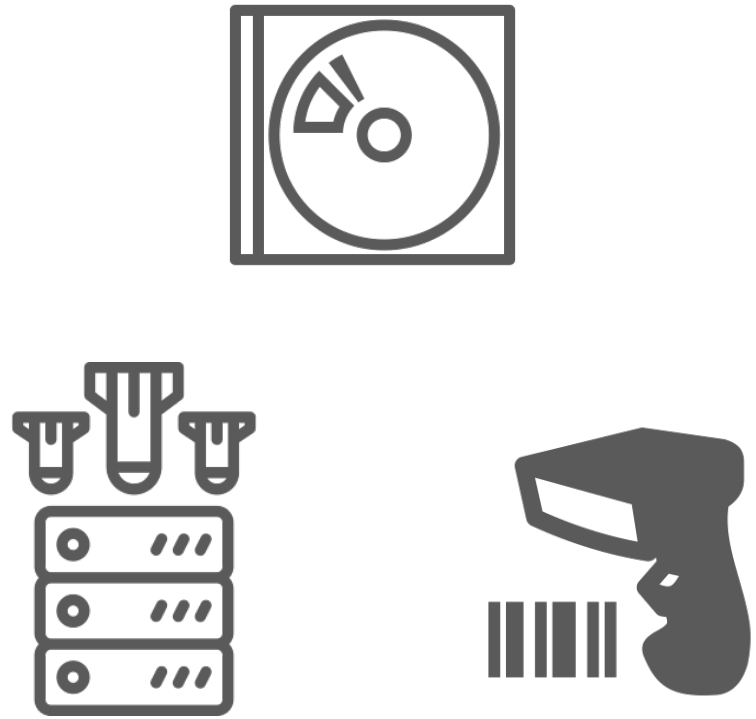
Categories


A
B
C
D
E
F
Protection
Health
Behavior
Users
Connections
Devices

Categories

Protection

Detecting insecure network settings and patching cadence.

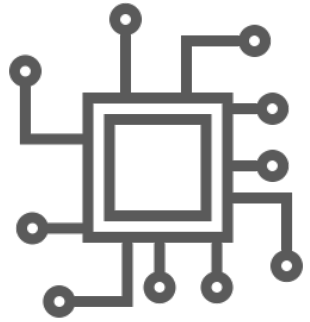


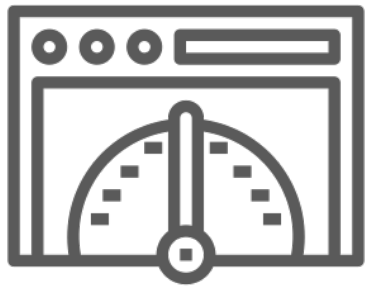
CyberSecurity™ ScoreCard

Categories

Health

Grading the performance level of the security infrastructure.



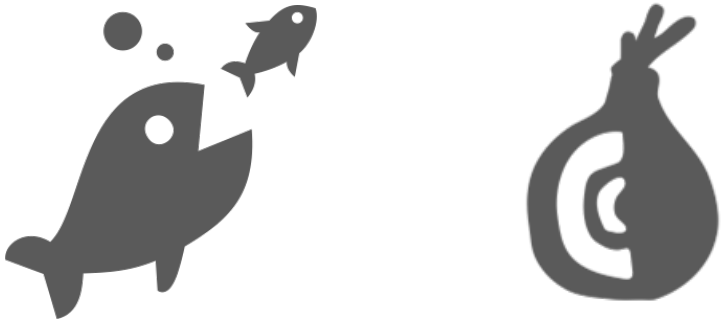


CyberSecurity™ ScoreCard

Categories

Behavior

Detecting internal network threats based on traffic patterns.



CyberSecurity™ ScoreCard

Categories

Users

Expose the traffic and authentication level of your users.

Categories

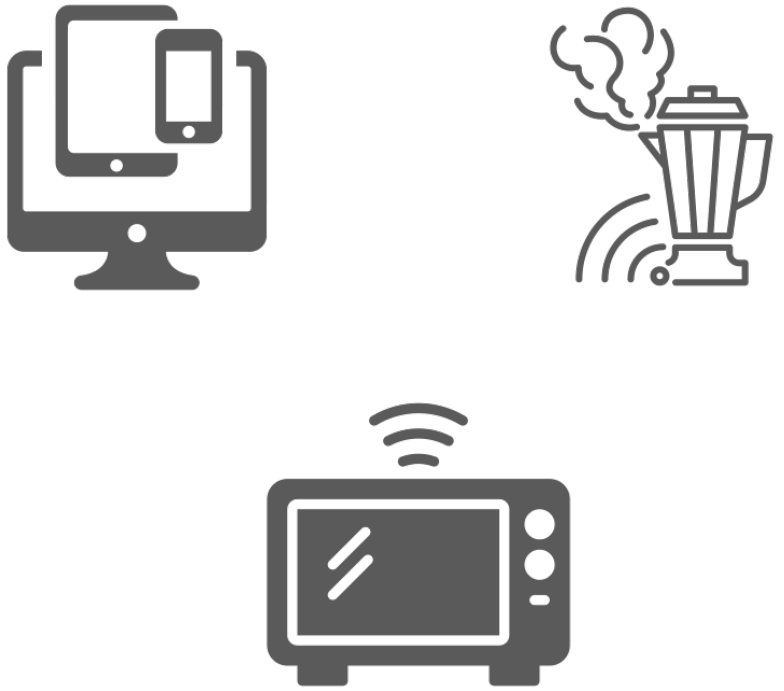
Connections

The status and quality of SD-WAN and VPN links.

Categories

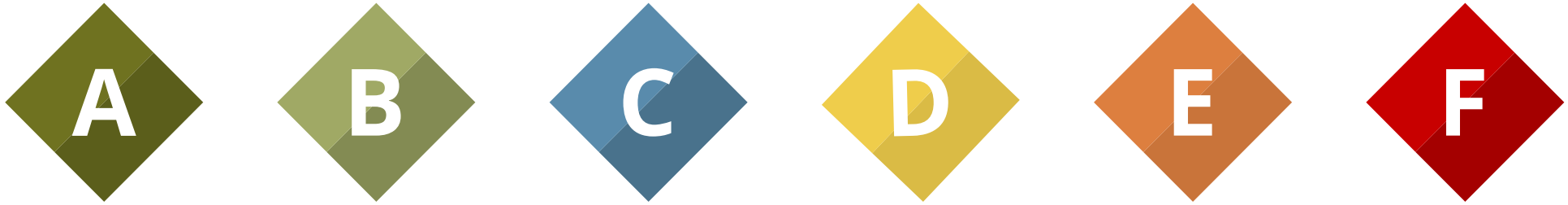
Devices

Understanding the traffic from IoT, mobile and corporate units.



CyberSecurity™ ScoreCard

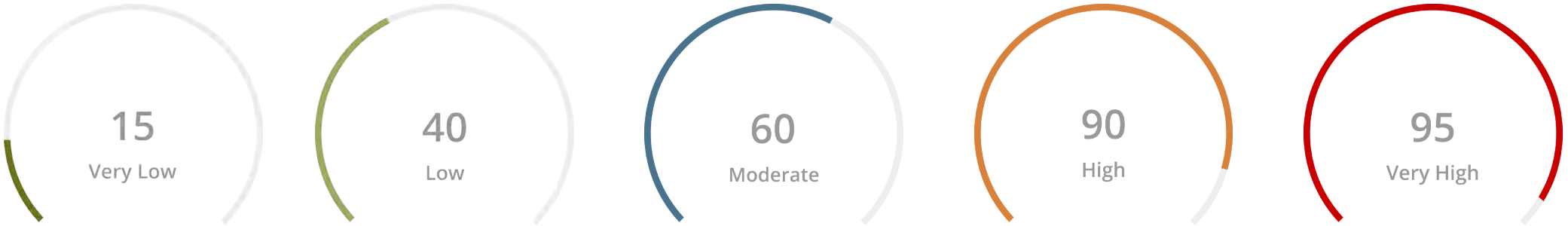
Categories



Overall Score

Ranging from A to F very simply explaining the status of the solution.

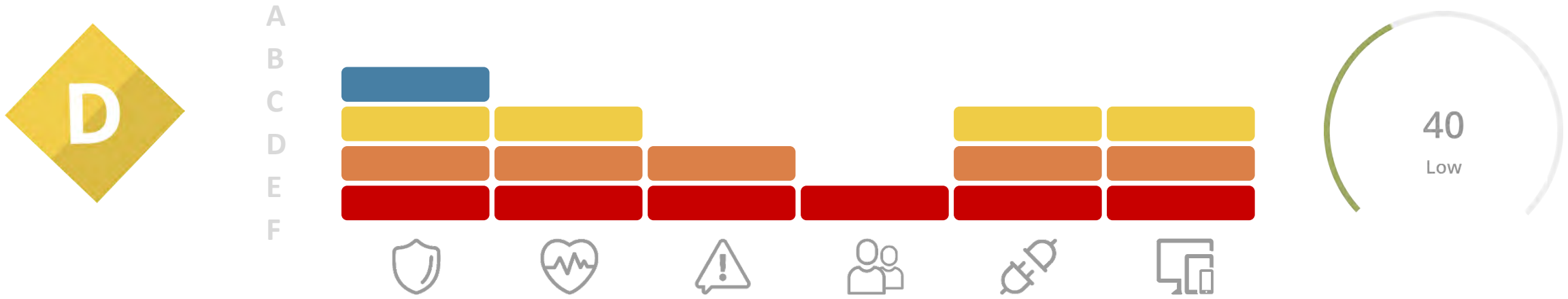
Categories



Threat Level

Together with the Threat Level, summarizing the malicious activity going on towards us.

CyberSecurity ScoreCard



Top 3 Suggested Improvements

Category	Suggested Improvement
Users	Enforce MFA for VPN connections.
Connections	Disable IPsec algorithms with key length < 256.
Behaviour	Users within your network is communicating with know botnets. Perform malware scan.

CyberSecurity™ ScoreCard


clavister
D
40
Low
Protection
Health
Behavior
Users
Devices


CyberSecurity ScoreCard
D
60

Clavister InCenter

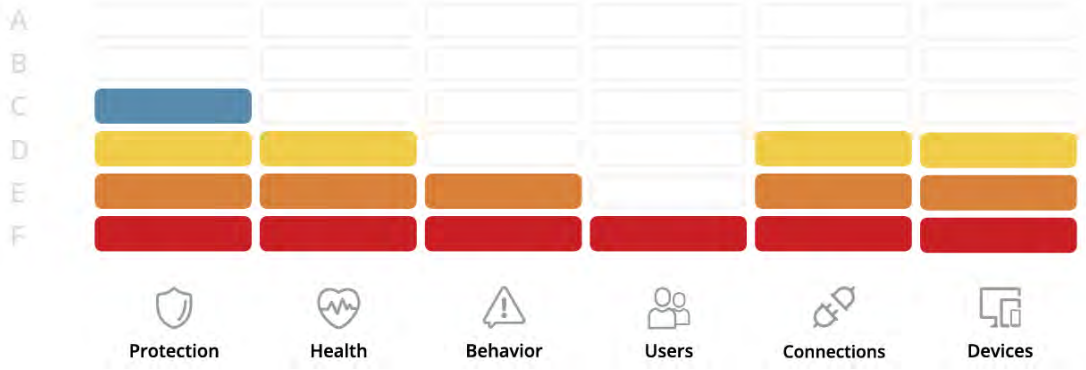
- Overview
- CyberSecurity ScoreCard (BETA)
  - Overview
  - Details
- Analyze
- Manage
- Alerting
- System
- Reporting

CyberSecurity ScoreCard (BETA)

CyberSecurity **Score**Card

Filter: All

Overall Score

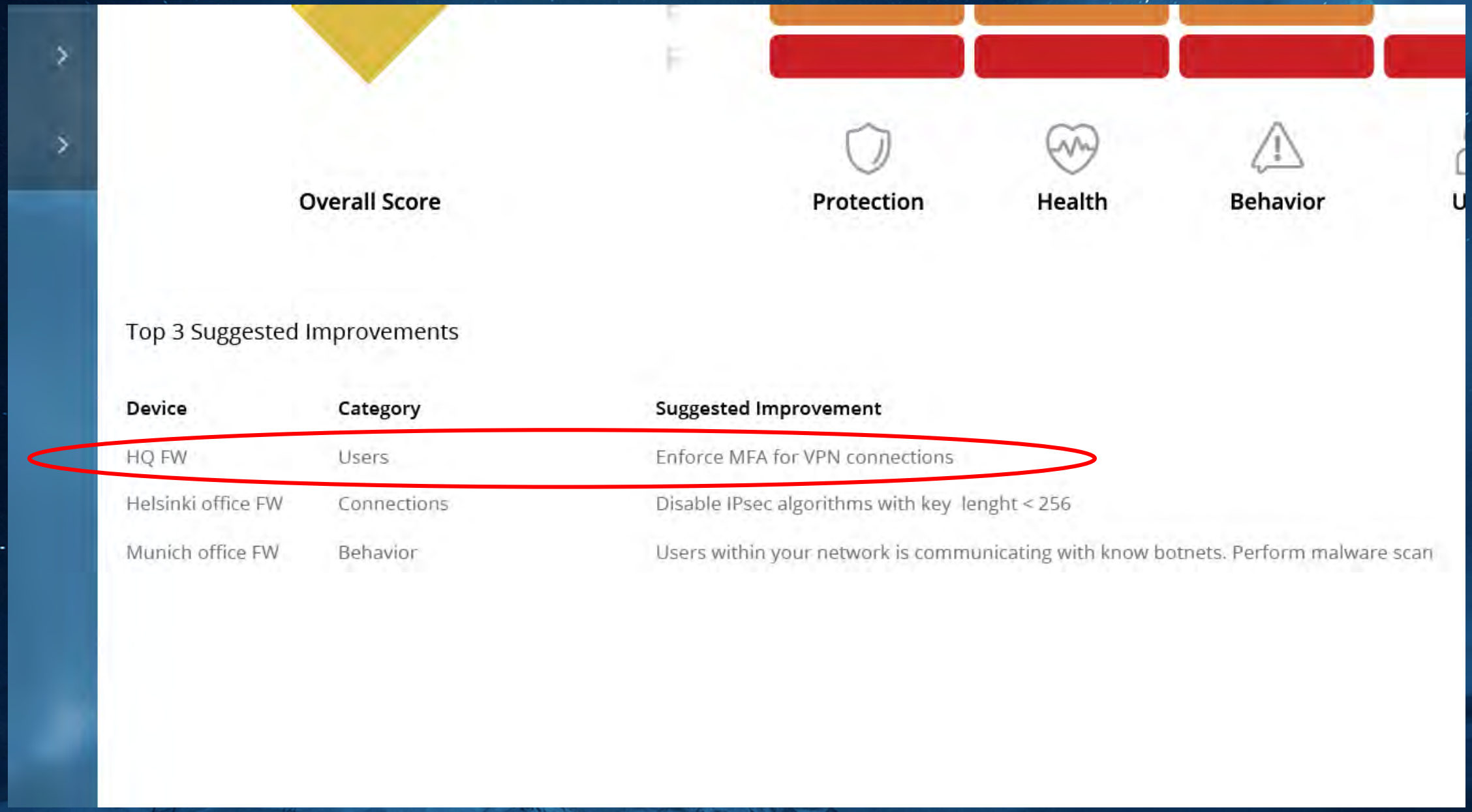


Threat Level

Top 3 Suggested Improvements

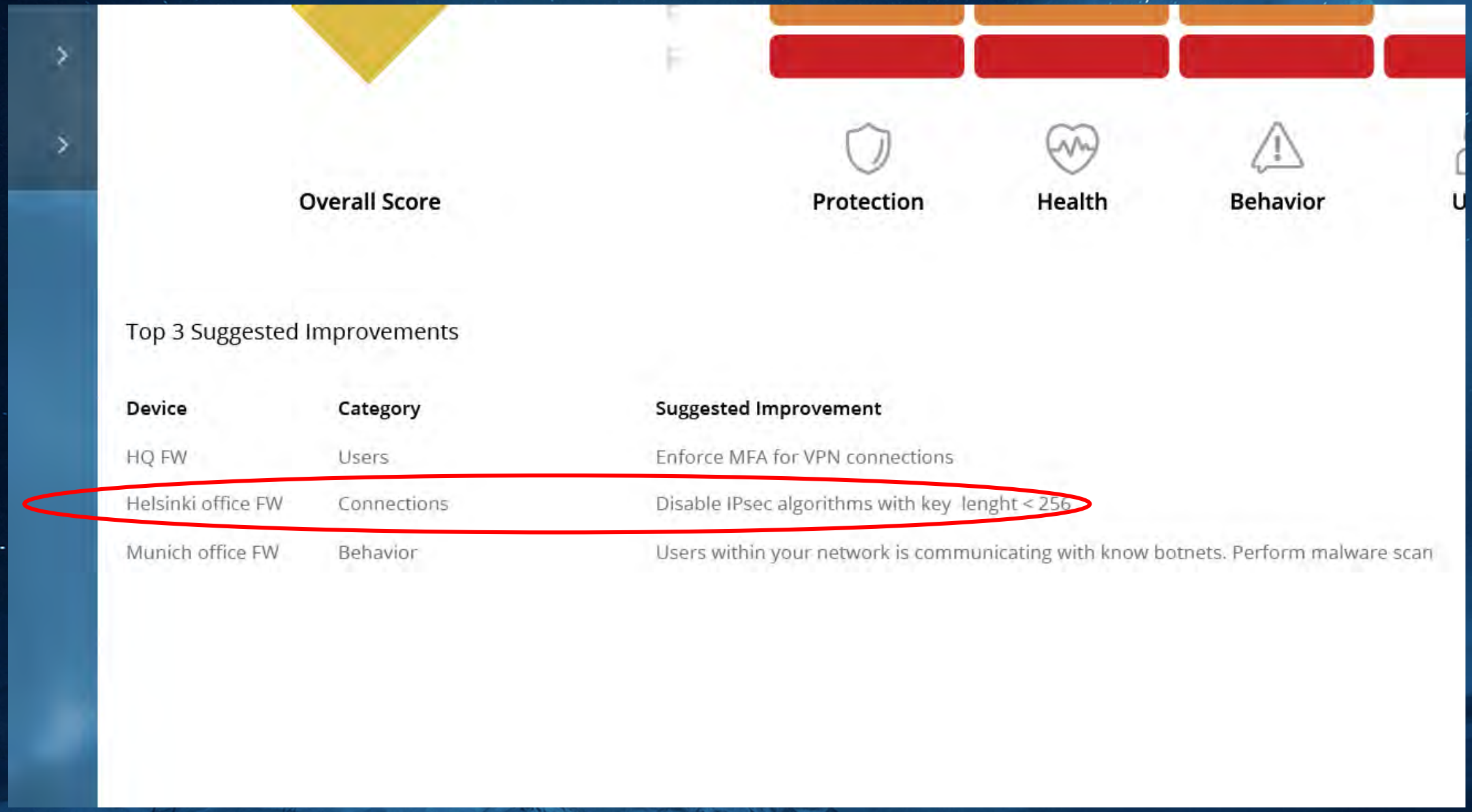
Device	Category	Suggested Improvement
HQ FW	Users	Enforce MFA for VPN connections
Helsinki office FW	Connections	Disable IPsec algorithms with key lenght < 256
Munich office FW	Behavior	Users within your network is communicating with know botnets. Perform malware scan

SECURITY BY SWEDEN



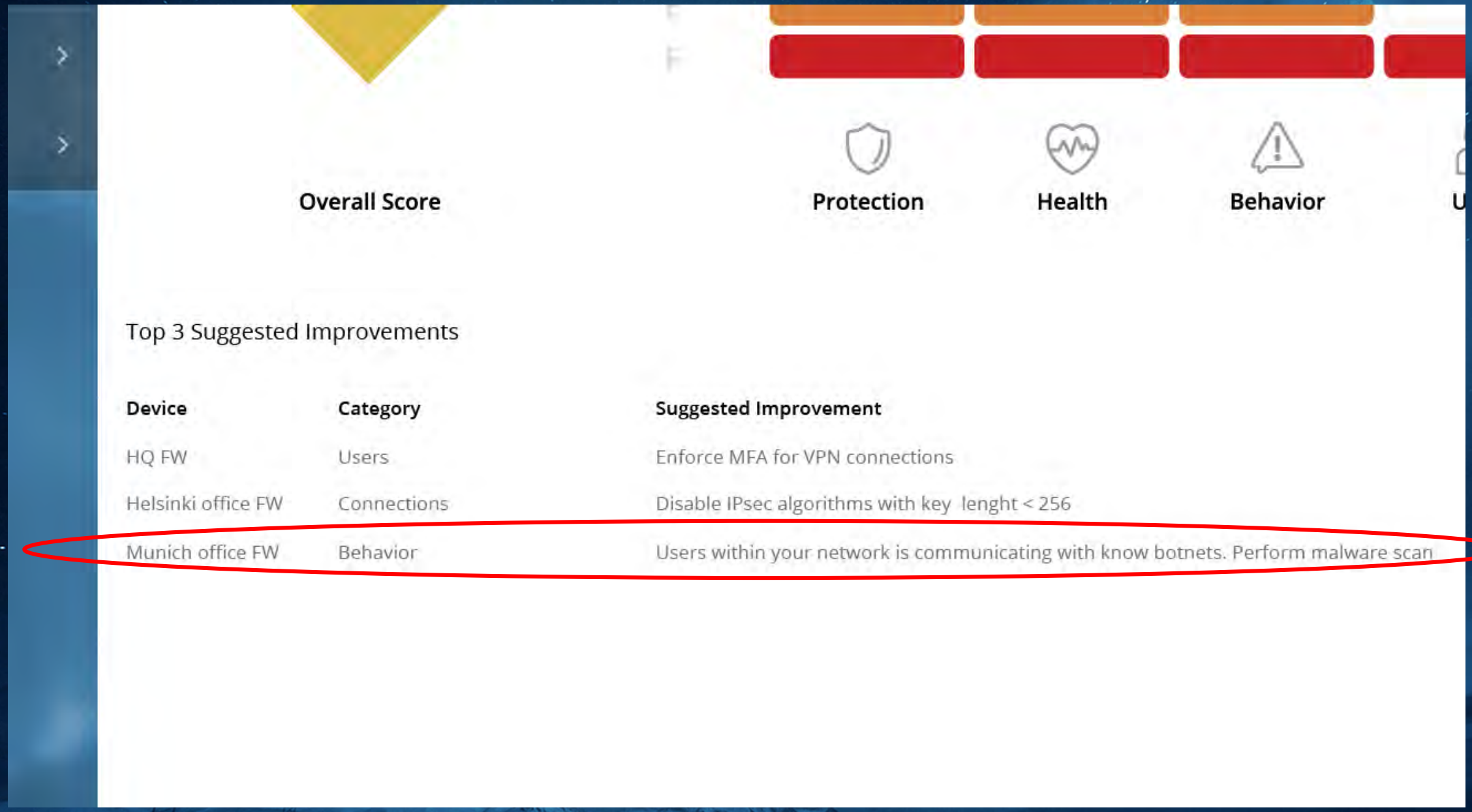
Top 3 Suggested Improvements

Device	Category	Suggested Improvement
HQ FW	Users	Enforce MFA for VPN connections
Helsinki office FW	Connections	Disable IPsec algorithms with key lenght < 256
Munich office FW	Behavior	Users within your network is communicating with know botnets. Perform malware scan



Top 3 Suggested Improvements

Device	Category	Suggested Improvement
HQ FW	Users	Enforce MFA for VPN connections
Helsinki office FW	Connections	Disable IPsec algorithms with key lenght < 256
Munich office FW	Behavior	Users within your network is communicating with know botnets. Perform malware scan



Top 3 Suggested Improvements

Device	Category	Suggested Improvement
HQ FW	Users	Enforce MFA for VPN connections
Helsinki office FW	Connections	Disable IPsec algorithms with key lenght < 256
Munich office FW	Behavior	Users within your network is communicating with know botnets. Perform malware scan

clavister

Clavister InCenter

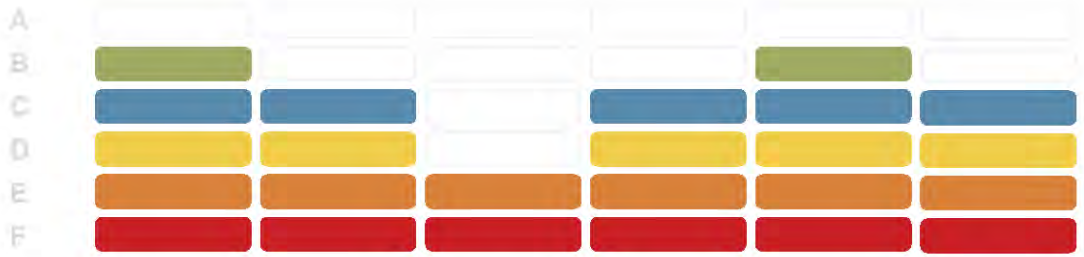
- Overview
- CyberSecurity ScoreCard (BETA)
  - Overview
  - Details
- Analyze
- Manage
- Alerting
- System
- Reporting

CyberSecurity ScoreCard (BETA)

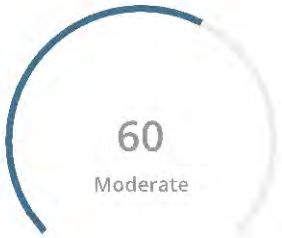
CyberSecurity **Score**Card

Filter: All

Overall Score



Protection | Health | Behavior | Users | Connections | Devices



Threat Level

Top 3 Suggested Improvements

Device	Category	Suggested Improvement
HQ FW	Behavior	Users within your network is communicating with know botnets. Perform malware scan
Helsinki office FW	Devices	Make sure Microsoft Windows Update is enabled on all Windows clients
Munich office FW	Behavior	Applications identified as high risk are used, consider blocking high risk applications

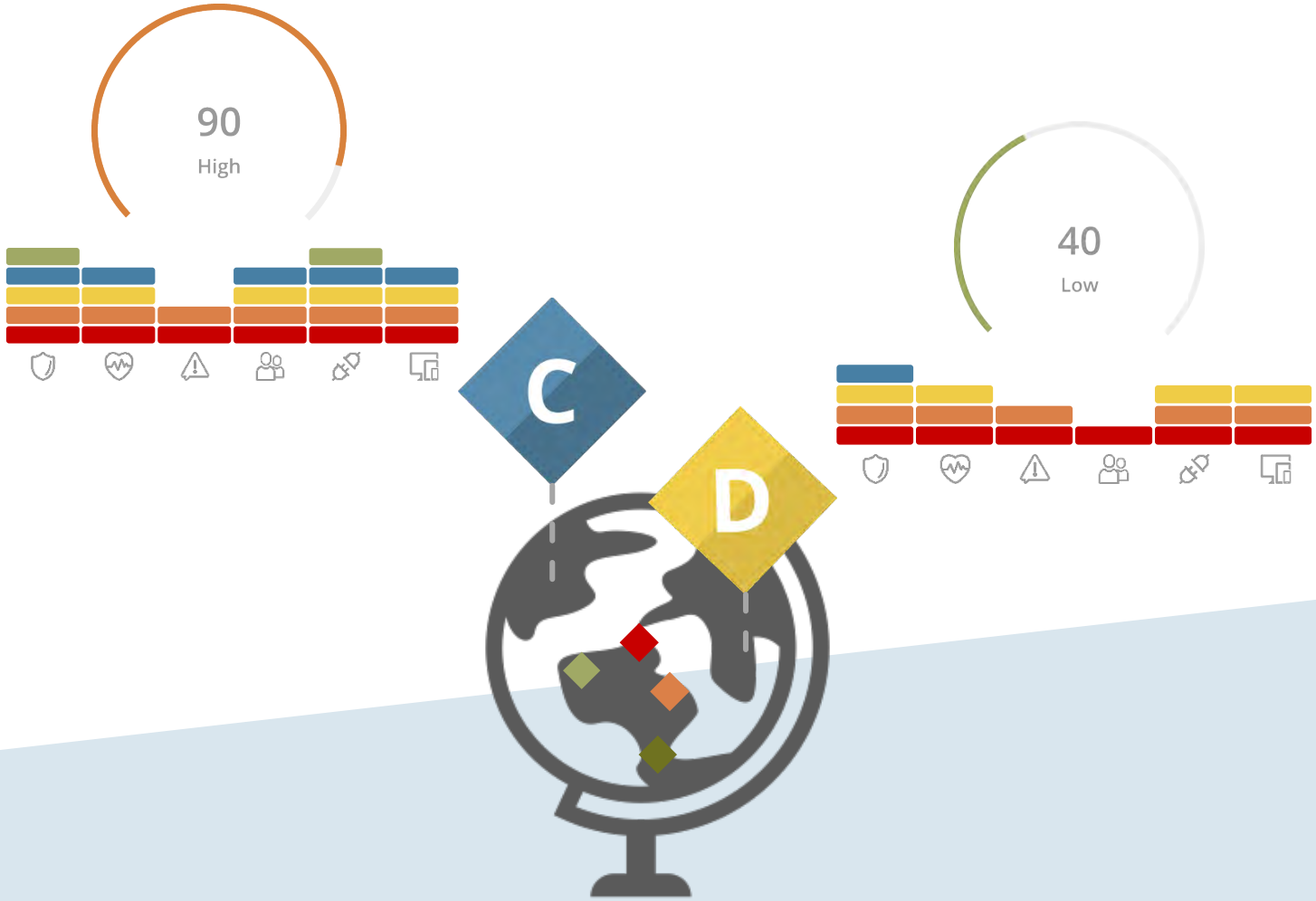
SECURITY BY SWEDEN


Cybersecurity Scorecard

Example actions

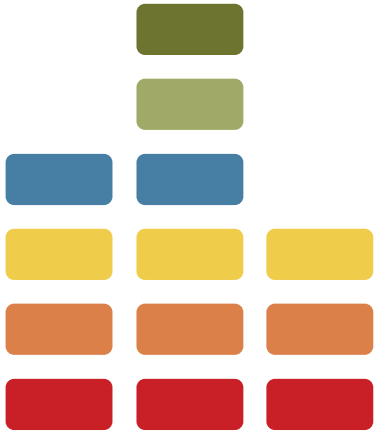
- Activate IP Reputation
- Block applications with high risk
- Uppgrade firmware
- …

Geographically Compare



Compare over time


clavister
A
40
Low
Protection
Health
Behavior
Users
Connections
Devices



CyberSecurity™ ScoreCard

Simplified Actionable Security Analytics


As CyberSecurity is evolving
form a *technical burden* to
a business priority…
Simplicity is **Key**
SECURITY BY
SWEDEN

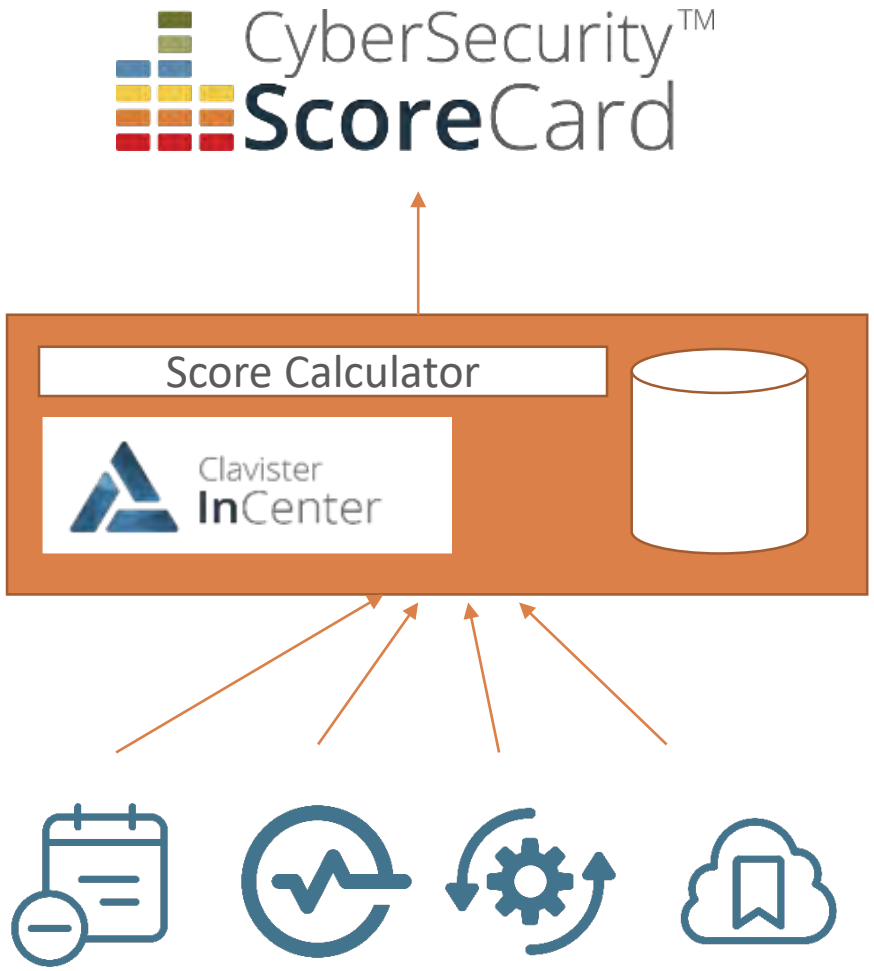

clavister
”By 2020, 100% of large enterprises will be asked to report to their boards of directors on cybersecurity and technology risk at least annually, which is up from 40% in 2016. ”
Gartner®


Clavister
Architecture

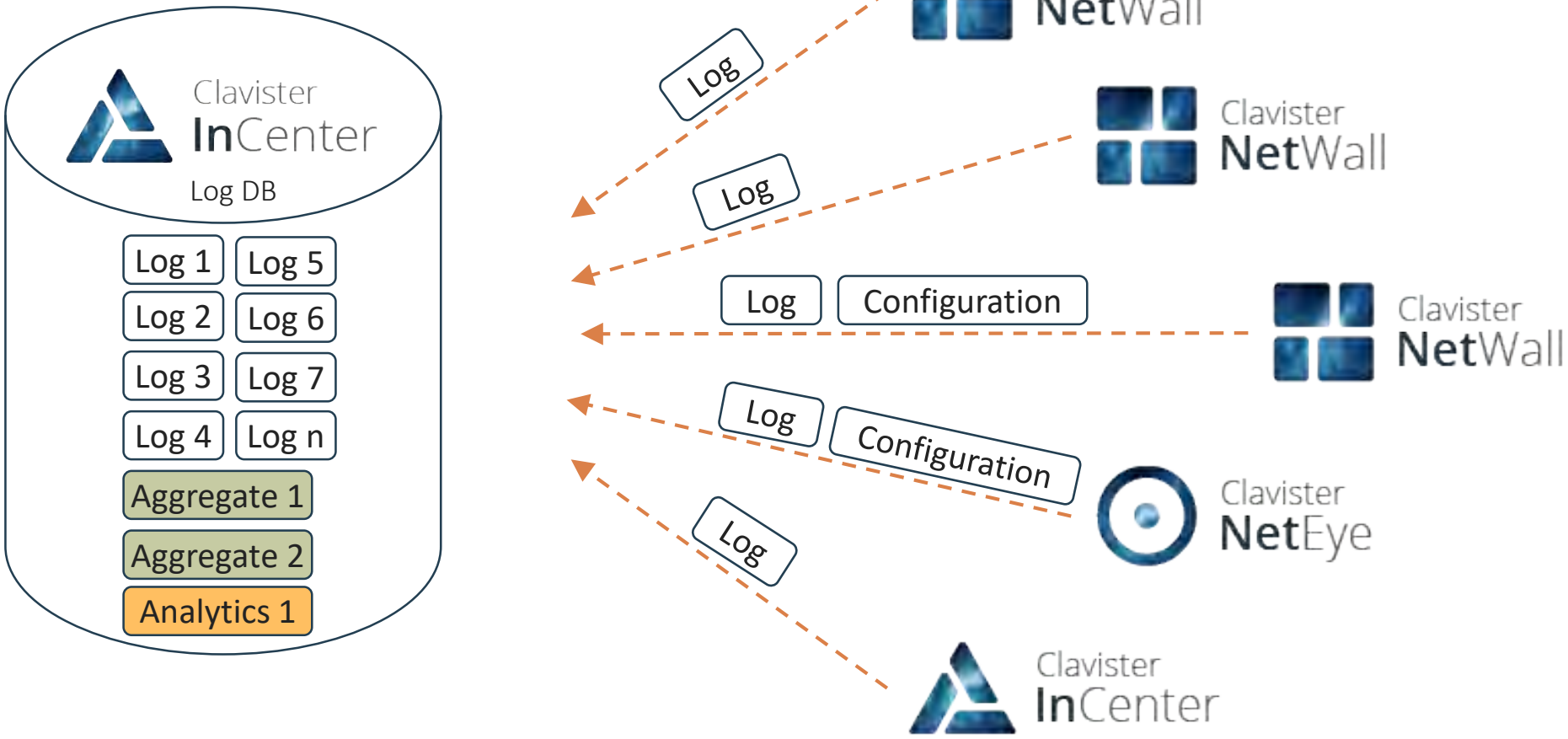
Architecture - Data sources

- **Event logs**
  - From NetWall, EasyAccess, …
- **Status information**
  - Windows API via OneConnect
- **Configuration data**
  - From NetWall, EasyAccess, …
- **Reference data**
  - From myClavister, Clavister Service Provisioning Network

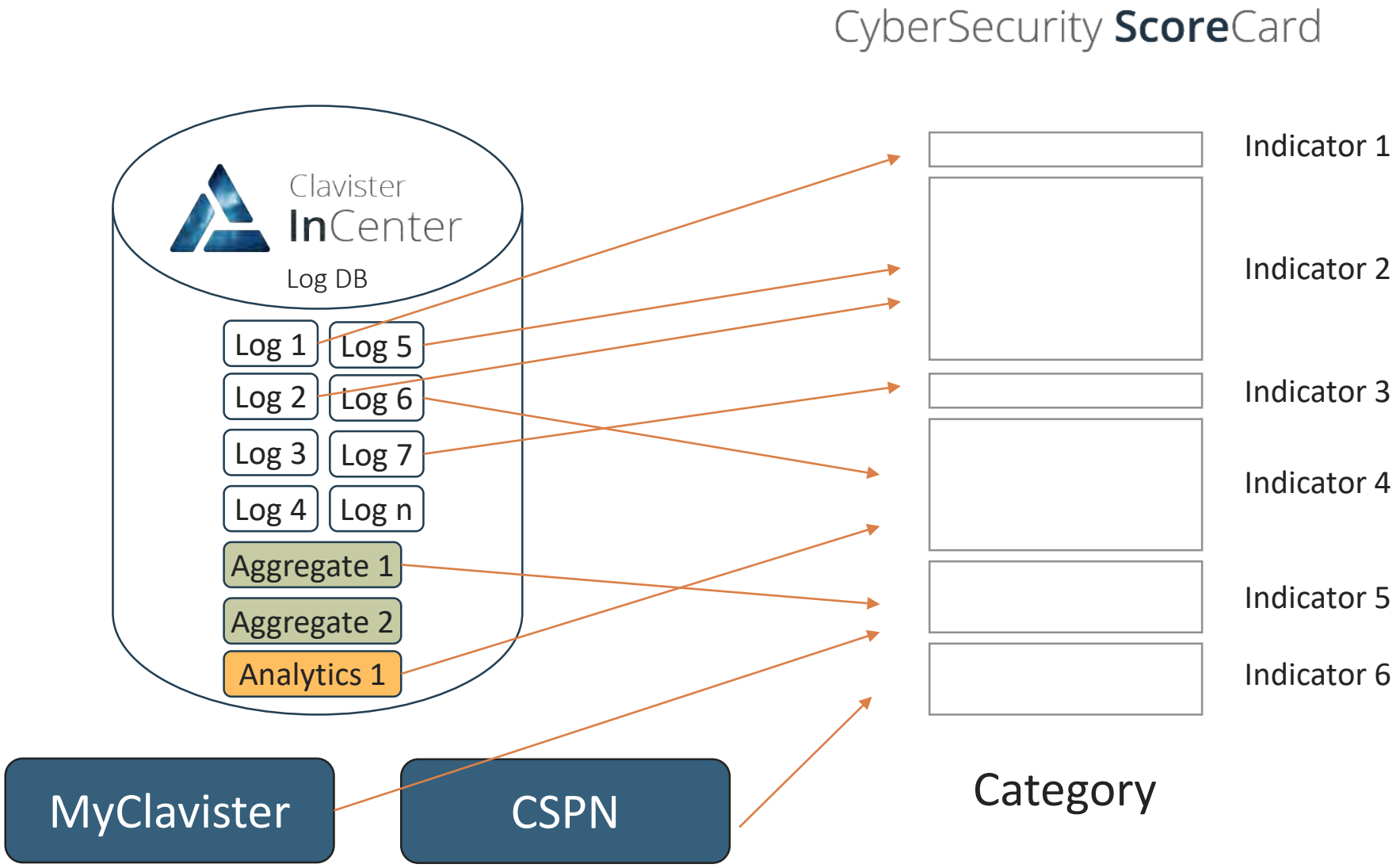
Daily computation updates



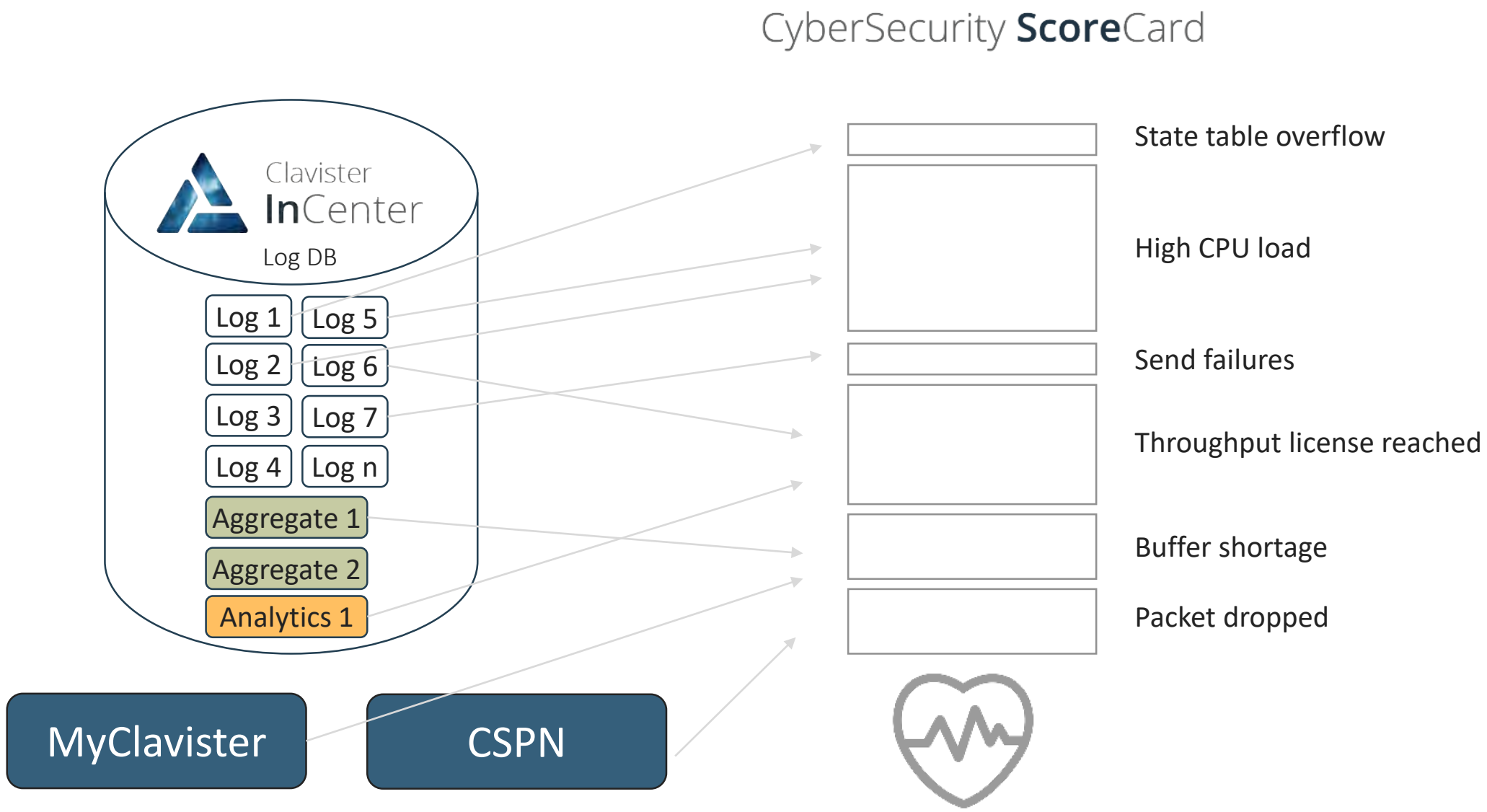
Gathering data



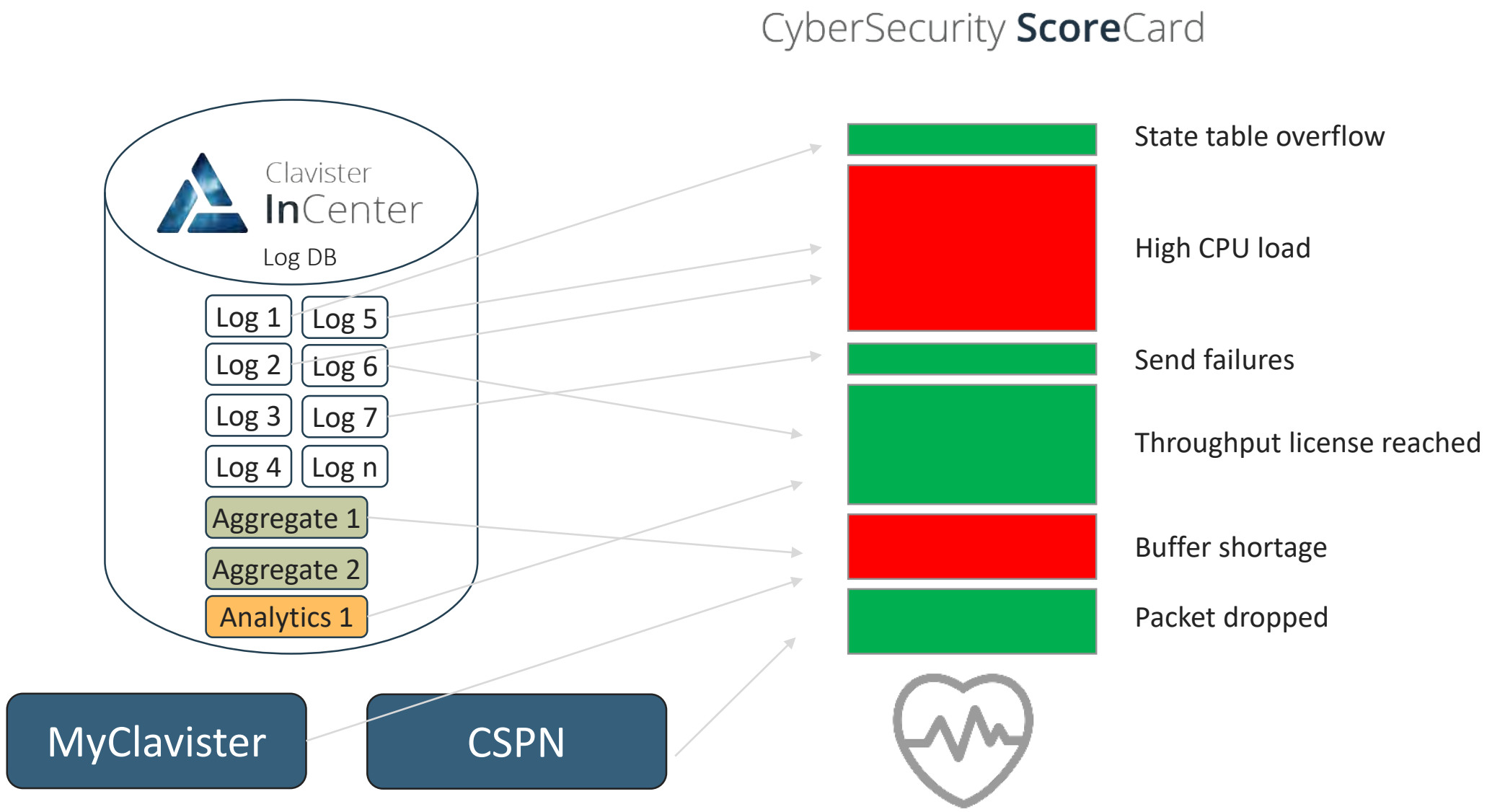
Indicators and Categories



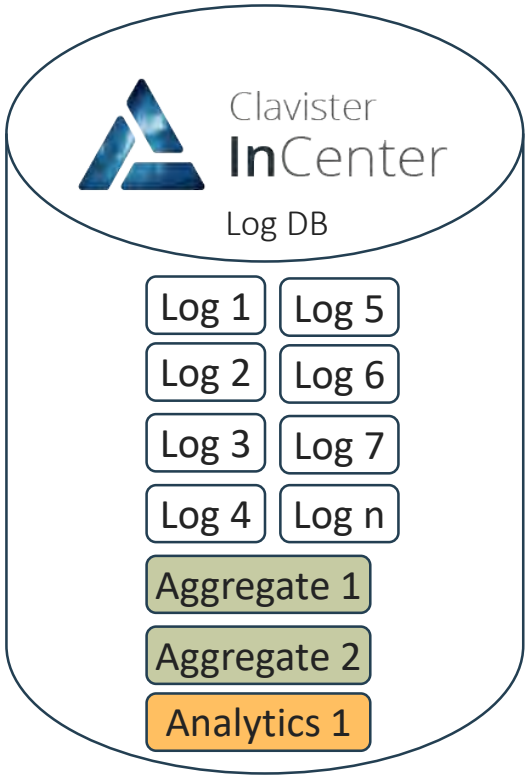
Indicators and Categories



Indicators and Categories



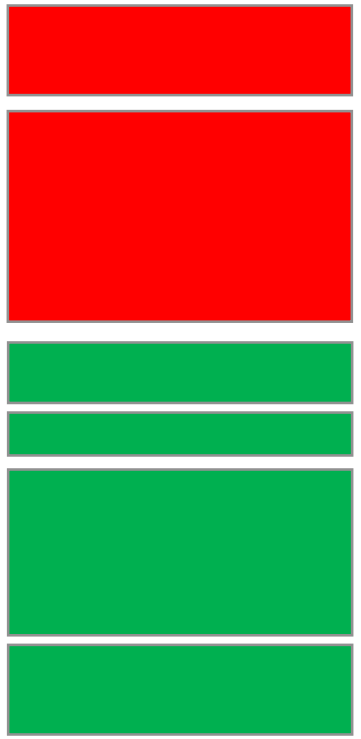
Indicators and Categories



MyClavister

CSPN

CyberSecurity **Score**Card



Buffer shortage

High CPU load

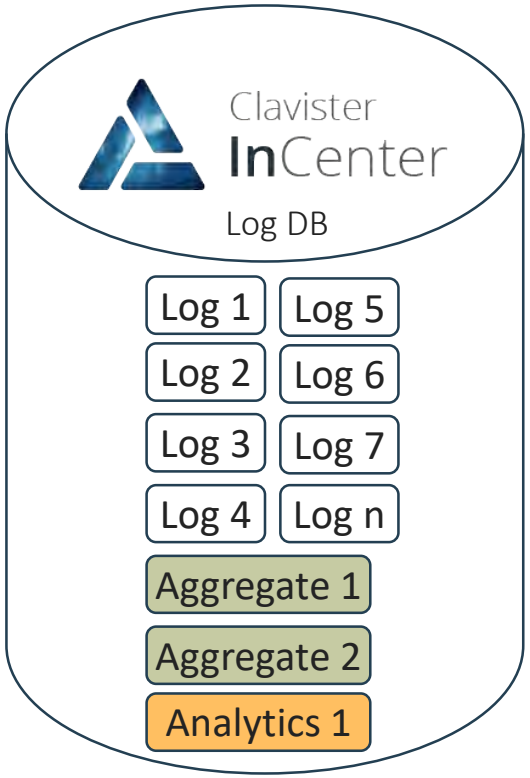
State table overflow

Send failures

Throughput license reached

Packet dropped

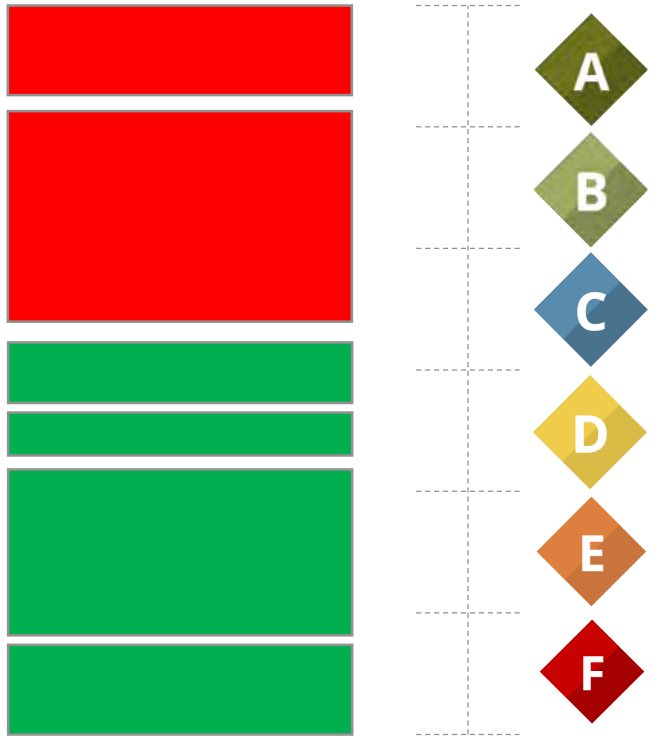
Indicators and Categories



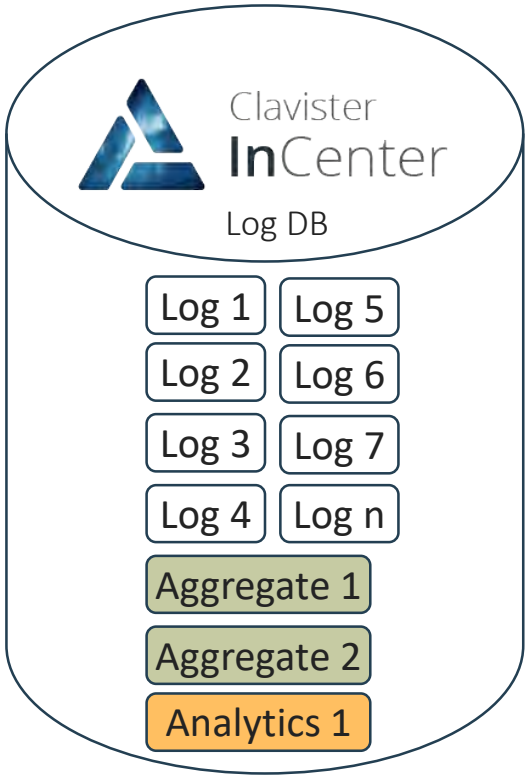
MyClavister

CSPN

CyberSecurity **Score**Card



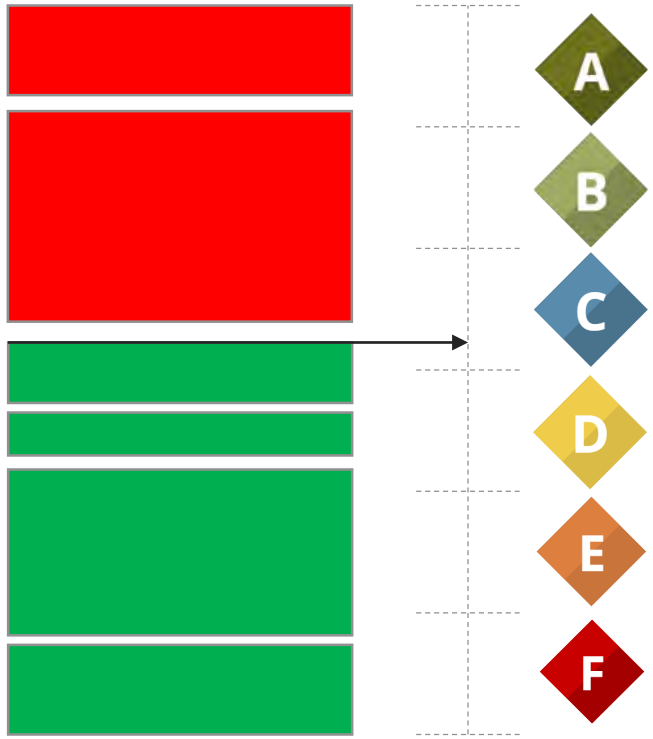
Indicators and Categories



MyClavister

CSPN

CyberSecurity **Score**Card



clavister

Clavister InCenter

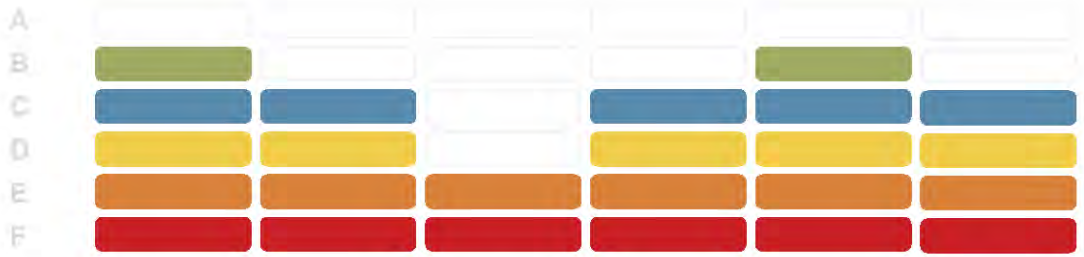
- Overview
- CyberSecurity ScoreCard (BETA)
  - Overview
  - Details
- Analyze
- Manage
- Alerting
- System
- Reporting

CyberSecurity ScoreCard (BETA)

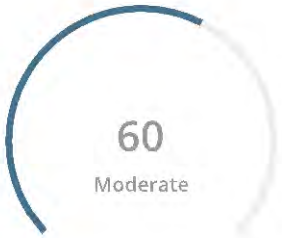
CyberSecurity **Score**Card

Filter: All

Overall Score



Protection | Health | Behavior | Users | Connections | Devices

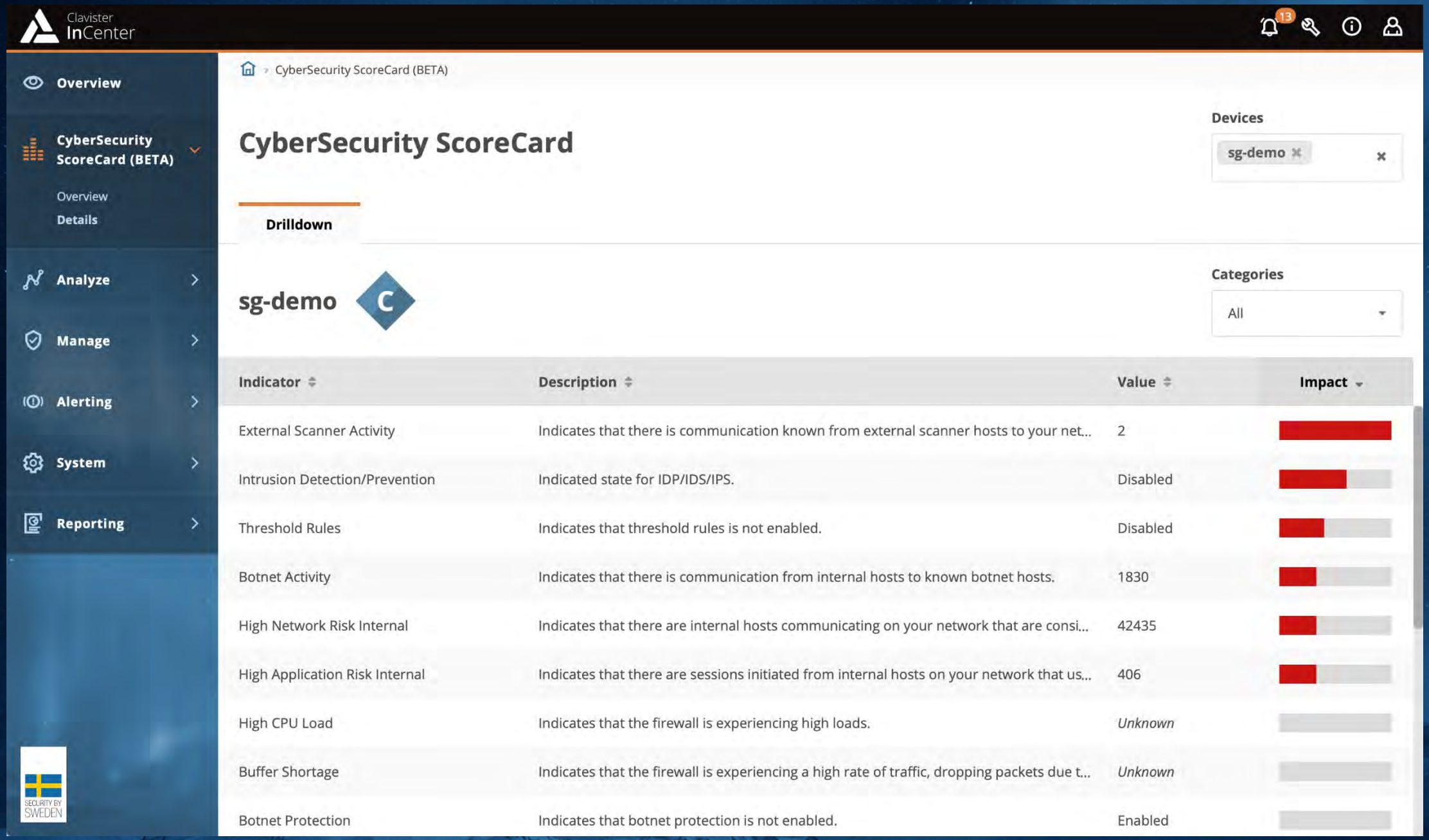


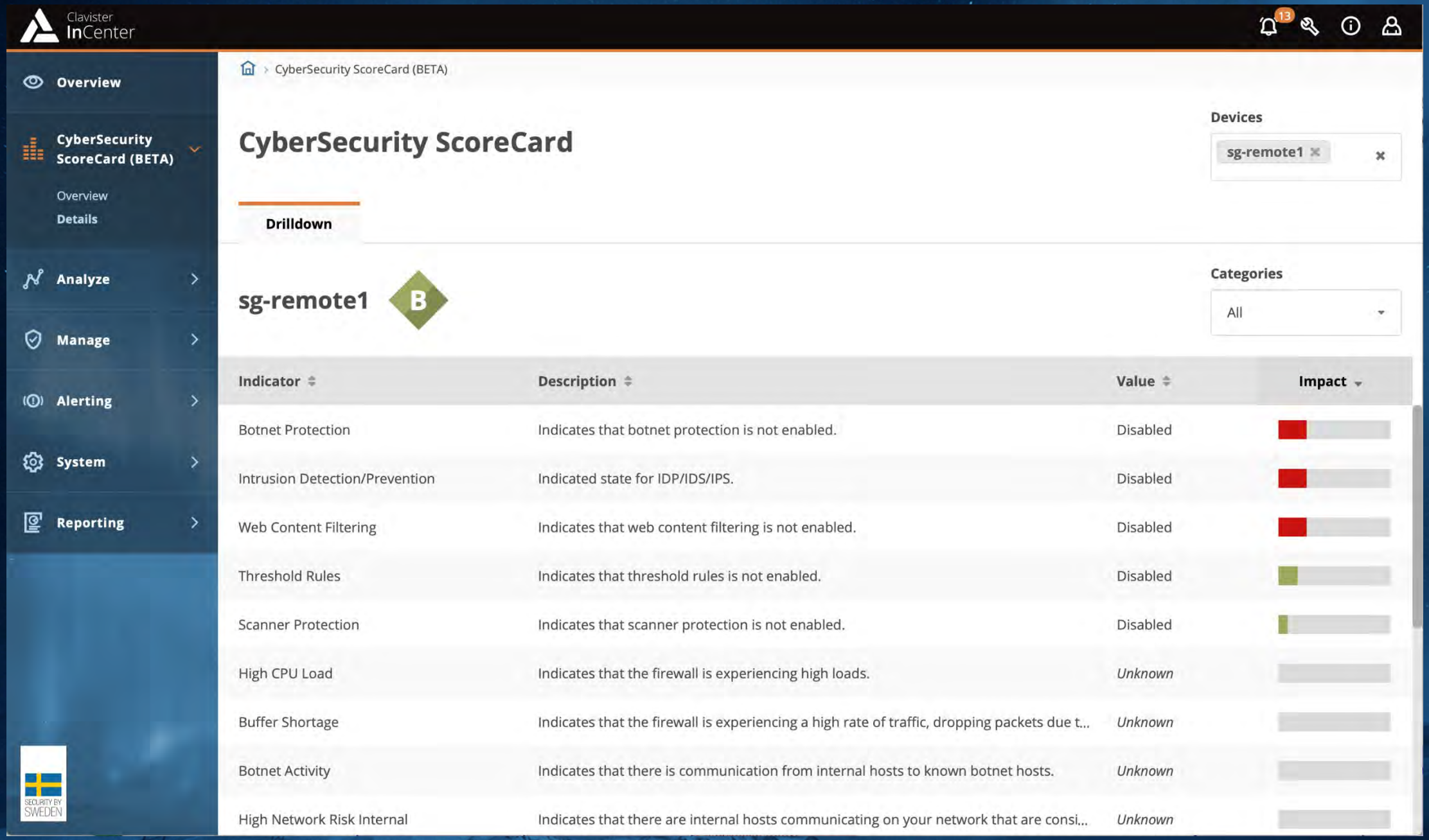
Threat Level

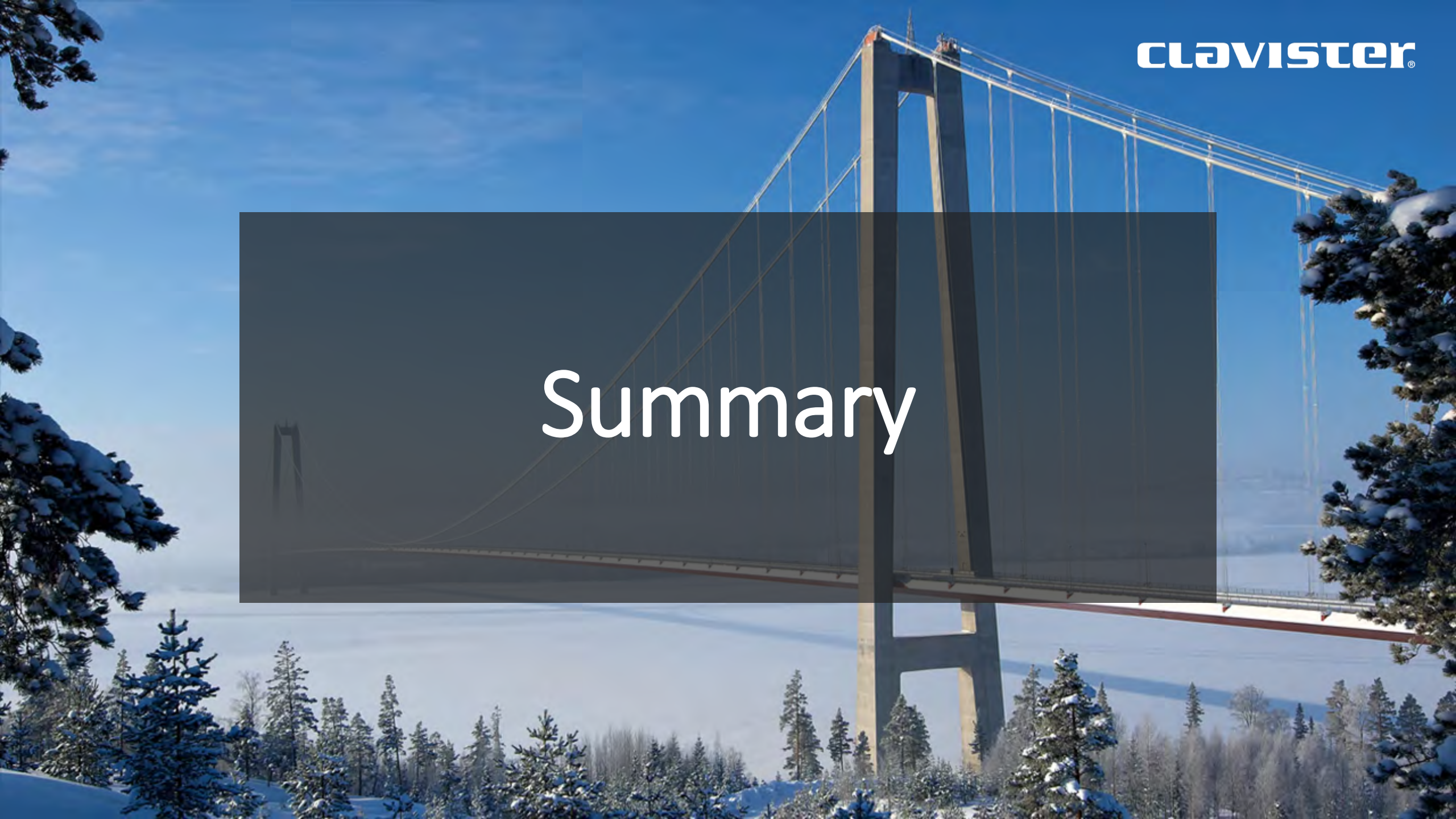
Top 3 Suggested Improvements

Device	Category	Suggested Improvement
HQ FW	Behavior	Users within your network is communicating with know botnets. Perform malware scan
Helsinki office FW	Devices	Make sure Microsoft Windows Update is enabled on all Windows clients
Munich office FW	Behavior	Applications identified as high risk are used, consider blocking high risk applications

SECURITY BY SWEDEN


Clavister InCenter
13
Overview
CyberSecurity ScoreCard (BETA)
Overview
Details
Analyze
Manage
Alerting
System
Reporting
CyberSecurity ScoreCard (BETA)
CyberSecurity ScoreCard
Devices
sg-demo
Drilldown
sg-demo
C
Categories
All
Indicator
Description
Value
Impact
External Scanner Activity
Indicates that there is communication known from external scanner hosts to your net...
2
Intrusion Detection/Prevention
Indicated state for IDP/IDS/IPS.
Disabled
Threshold Rules
Indicates that threshold rules is not enabled.
Disabled
Botnet Activity
Indicates that there is communication from internal hosts to known botnet hosts.
1830
High Network Risk Internal
Indicates that there are internal hosts communicating on your network that are consi...
42435
High Application Risk Internal
Indicates that there are sessions initiated from internal hosts on your network that us...
406
High CPU Load
Indicates that the firewall is experiencing high loads.
Unknown
Buffer Shortage
Indicates that the firewall is experiencing a high rate of traffic, dropping packets due t...
Unknown
Botnet Protection
Indicates that botnet protection is not enabled.
Enabled
SECURITY BY SWEDEN

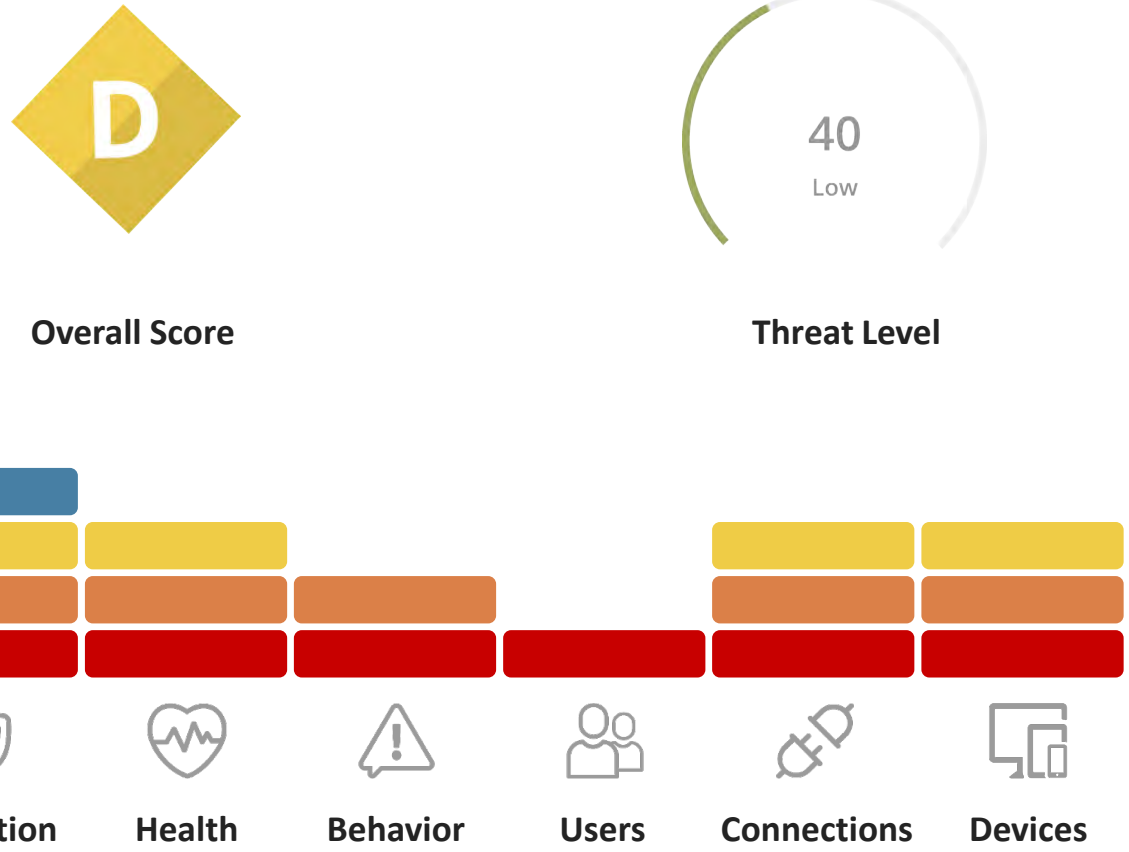

Clavister InCenter
13
Overview
CyberSecurity ScoreCard (BETA)
Overview
Details
Analyze
Manage
Alerting
System
Reporting
CyberSecurity ScoreCard (BETA)
CyberSecurity ScoreCard
Devices
sg-remote1
Drilldown
sg-remote1
B
Categories
All
Indicator
Description
Value
Impact
Botnet Protection
Indicates that botnet protection is not enabled.
Disabled
Intrusion Detection/Prevention
Indicated state for IDP/IDS/IPS.
Disabled
Web Content Filtering
Indicates that web content filtering is not enabled.
Disabled
Threshold Rules
Indicates that threshold rules is not enabled.
Disabled
Scanner Protection
Indicates that scanner protection is not enabled.
Disabled
High CPU Load
Indicates that the firewall is experiencing high loads.
Unknown
Buffer Shortage
Indicates that the firewall is experiencing a high rate of traffic, dropping packets due t...
Unknown
Botnet Activity
Indicates that there is communication from internal hosts to known botnet hosts.
Unknown
High Network Risk Internal
Indicates that there are internal hosts communicating on your network that are consi...
Unknown
SECURITY BY SWEDEN



Summary

CyberSecurity ScoreCard

- **Simplified** Visibility
- **Instant** view → peace of mind
- **Prescriptive** analytics → actionable
- **Comparable** → justifying investments



Top 3 Suggested Improvements

Category	Suggested Improvement
Users	Enforce MFA for VPN connections.
Connections	Disable IPsec algorithms with key length < 256.
Behaviour	Users within your network is communicating with know botnets. Perform malware scan.

Included in:

Clavister
InCenter

Clavister
InCenter Cloud

SECURITY BY SWEDEN


CyberSecurity™
ScoreCard
Simplified Actionable Security Analytics
Helps IT Manager Anna:
Reveal
Prioritize
Communicate
The status of IT Security
clavister

CyberSecurity™
ScoreCard

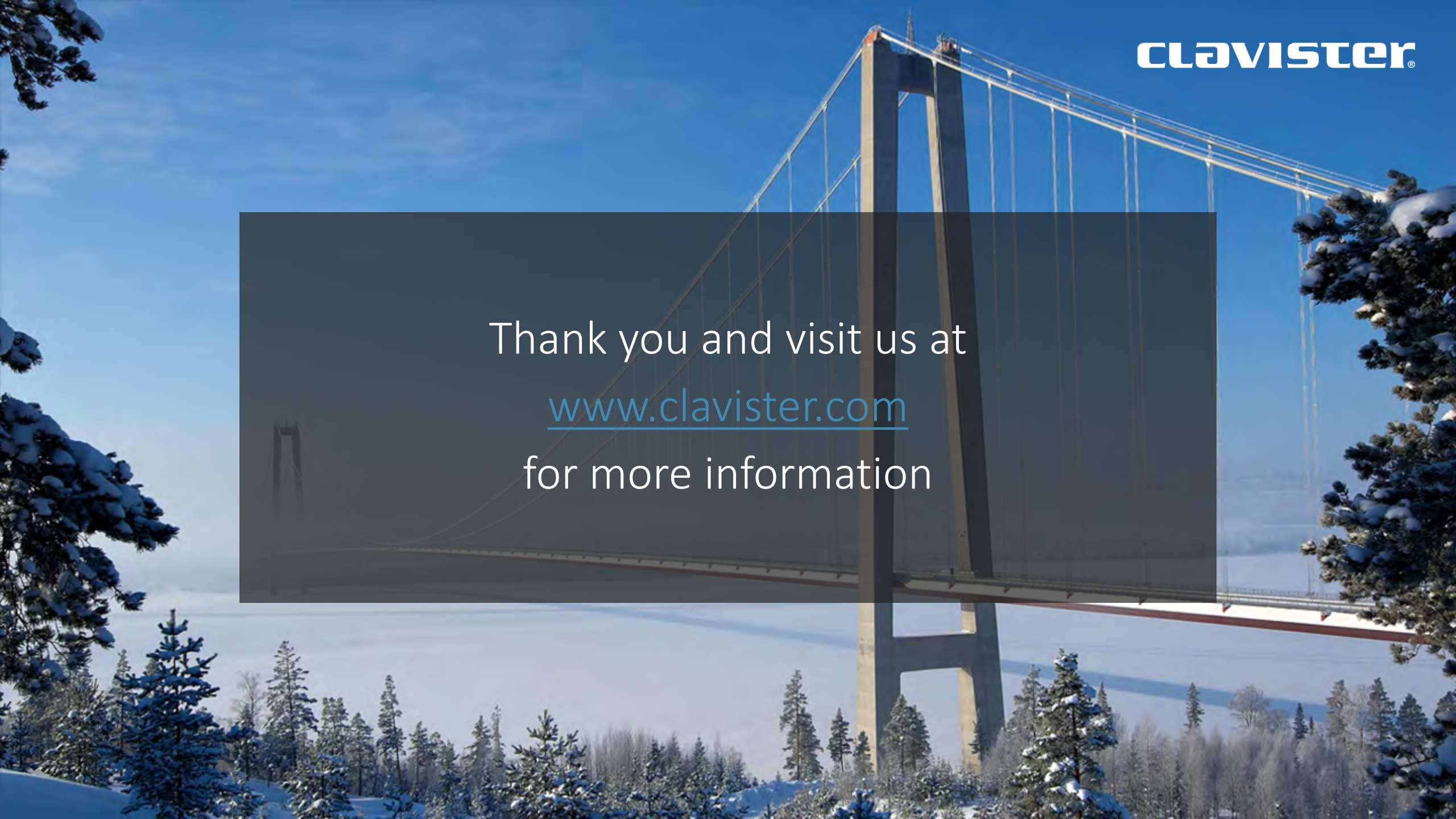
Simplified Actionable Security Analytics

Helps CEO John:

- See status
- Understand need
- See impact

Feel at ease!


clavister®
The Leading European
CyberSecurity Expert
SECURITY BY
SWEDEN


clavister
Thank you and visit us at
www.clavister.com
for more information