



foreseeti

**ForeFuture
Risk Analysis in Real Time for Cyber Attacks**

Anders Malmström – Foreseeti CEO



Information about the Project

- **Project Vision**
“Projektets mål är att utveckla en förstärkt förmåga att i realtid genomföra analys verklig risk för cyberattacker mot ett företag eller en organization.”
- Expected outcome is to enable Swedish and international organizations to strengthen and more effectively combat the growing cyber threat
- Start Date: Jun 2021
- Planned Completion: May 2023



**Swedavia
Airports**



**Recorded
Future**



VINNOVA
Sweden's Innovation Agency

Overview



Provides the external Threat Intel perspective

Recorded Future gathers and structures multidimensional information & intelligence from an external perspective in real time in the following areas:

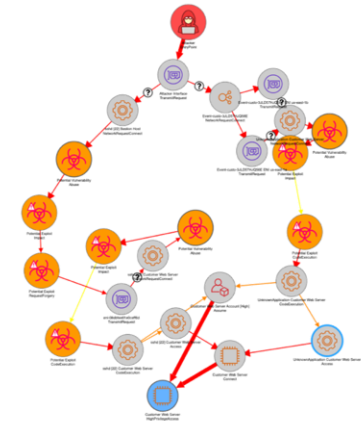
- Threat Intelligence
- Third-Party Intelligence
- SecOps Intelligence
- Vulnerability Intelligence
- Geopolitical Intelligence
- Identity Intelligence
- Fraud Intelligence
- Brand Intelligence



Provides the internal risk assessment perspective

Foreseeti provides capabilities for:

- Contextualizes multidimensional aspects of the environment: Infrastructure, Vulnerabilities, SAST/DAST, Identity and Access Mgmt, etc
- Attack Simulation and Risk assessment engine for risk quantification
- Structured fault injection
- Mitigations based on maximized risk lowering impact




Example Scenario 1 – Recorded Future finds a Cloud Key in the wild and Foreseeti simulates impact and risk

IP ADDRESS

161.129.64.124

ASN: AS8100
 ORG: ASN-QUADRANT-GLOBAL
 GEO: Amsterdam, Netherlands
 First Reference: Mar 10, 2021
 Latest Reference: Mar 18, 2021
 References: 13



71
MALICIOUS RISK SCORE
8 of 54 Risk Rules Triggered

TWO REFERENCES INVOLVING CVE-2021-26857 AND 161.129.64.124

MAR 10 2021
 Multiple APT groups Mass Scanning and Targeting RCE Vulnerability Chain in Microsoft Exchange Servers
 "Multiple APT groups in addition to Hafnium have been observed mass scanning and targeting a pre-authentication RCE vulnerability chain in Microsoft servers. Microsoft initially released out-of-band patches for..." Full note
 Source: Inskit Group on Mar 10, 2021, 00:00 • Reference Actions • 1+ reference

MAR 2 2021
 Security Researchers Publish PoC for "ProxyLogon" Vulnerabilities in Microsoft Exchange Servers
 "As reported on March 2, 2021, Microsoft disclosed that 4 vulnerabilities in the Exchange Mail Server product were being actively exploited, with servers from 2013 onwards (2016, 2019) vulnerable; Microsoft released patches for the vulnerabilities the same day. The exploits were tied to..." Full note
 Source: Inskit Group on Mar 2, 2021, 00:00 • Reference Actions • 1+ reference



Total Risk Exposure

99%

Total risk exposure of all high value assets

High Value Assets At Risk

7/7

Reached by the attacker

High Value Assets

The high value assets of the simulation and the target of the attacker. Expand items in the list to get more details.

NAME	ATTACK STEP	PROBABILITY	TTC	CRITICAL PATH
BI Server	HighPrivilegeAccess	Very Likely	<div style="width: 100%;"></div>	Critical path
Bastion Host	HighPrivilegeAccess	Very Likely	<div style="width: 100%;"></div>	Critical path
Customer App Server	HighPrivilegeAccess	Very Likely	<div style="width: 100%;"></div>	Critical path
Customer Web Server	HighPrivilegeAccess	Very Likely	<div style="width: 100%;"></div>	Critical path
backoffice-bi-db	ReadDatabase	Very Likely	<div style="width: 100%;"></div>	Critical path
customer-db	ReadDatabase	Very Likely	<div style="width: 100%;"></div>	Critical path
customer-records-demo	ReadObject	Very Likely	<div style="width: 100%;"></div>	Critical path

Chokepoints

Key points in your architecture that the attacker exploited or traversed most frequently in the simulation to reach your high value assets.

Click here to show/hide filters

Filter high value assets: customer-records-demo Customer App Server Customer Web Server Bastion Host BI Server backoffice-bi-db customer-db

Show asset IDs: Select all assets:

Attacker: Click on nodes or links to highlight



High value assets: BI Server, Customer Web Server, Bastion Host, customer-db, customer-records-demo, backoffice-bi-db, Customer App Server

Example Scenario 2 – Recorded Future gathers intel about specific attackers for Foreseeti to assess shifting risk

