IBM SECURITY DAYS EVENT

NDB

DIGITALL8 | IBM Platinum Partner | telelink BUSINESS SERVICES | IBM Platinum Partner | CNSYS | IBM Gold Partner



CNSYS
COMPUTERS & NETWORKING

www.cybersecurity.cnsys.bg

SOC Platforms Data Enrichment with IBM Threat Intelligence (X-Force)

Vladislav Saykov
Senior IT Solutions Architect
CNSYS



CNSYS
COMPUTERS & NETWORKING

www.cybersecurity.cnsys.bg

- 25 years
- Top 5 SI in Bulgaria
- 200+ employees, 160+ tech staff
- 8 offices around the country
- 70M+ BGN revenue annually
- 50+ IT projects annually



About CNSys

CNSYS
COMPUTERS & NETWORKING

Business Problem

- One security breach can be fatal for the business
- Many security vulnerabilities exist and many threat actors try to exploit them
- No single way to prevent the attacks
- Data and information storm
- Most of the security solutions are noisy



www.cybersecurity.cnsys.bg

CNSYS
COMPUTERS & NETWORKING

Extend your Cyber security xxx with Threat Intelligence

www.cybersecurity.cnsys.bg

CNSYS
COMPUTERS & NETWORKING

What is Threat intelligence

IBM definition - “Threat Intelligence is data containing detailed knowledge about the cybersecurity threats targeting an organization.”

NIST definition - “Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.”



www.cybersecurity.cnsys.bg

CNSYS
COMPUTERS & NETWORKING

Threat Intelligence is more than Data or Information

- **Data** - raw facts and statistics
- **Information** - answers specific question
- **Intelligence** - helps making informed decisions and take effective actions



www.cybersecurity.cnsys.bg

CNSYS
COMPUTERS & NETWORKING

Threat Intelligence Lifecycle

- Planning
- Threat Data Collection
- Processing
- Analysis
- Dissemination
- Feedback



www.cybersecurity.cnsys.bg

Threat Intelligence Types

- **Tactical** - used by SOC to detect and respond to cyberattacks in progress
- **Operational/Technical** - helps to anticipate and prevent future attacks
- **Strategic** - global threat landscape and an organization's place within it



www.cybersecurity.cnsys.bg

STIX/TAXII Feeds

- STIX (Structured Threat Information eXpression) - standardized format
- TAXII (Trusted Automated Exchange of Intelligence Information) - transport protocol



www.cybersecurity.cnsys.bg

- Threat Intelligence - X-Force

  - QRadar SIEM Integration
  - QRadar SOAR Integration
  - QRadar XDR Connect Integration

www.cybersecurity.cnsys.bg



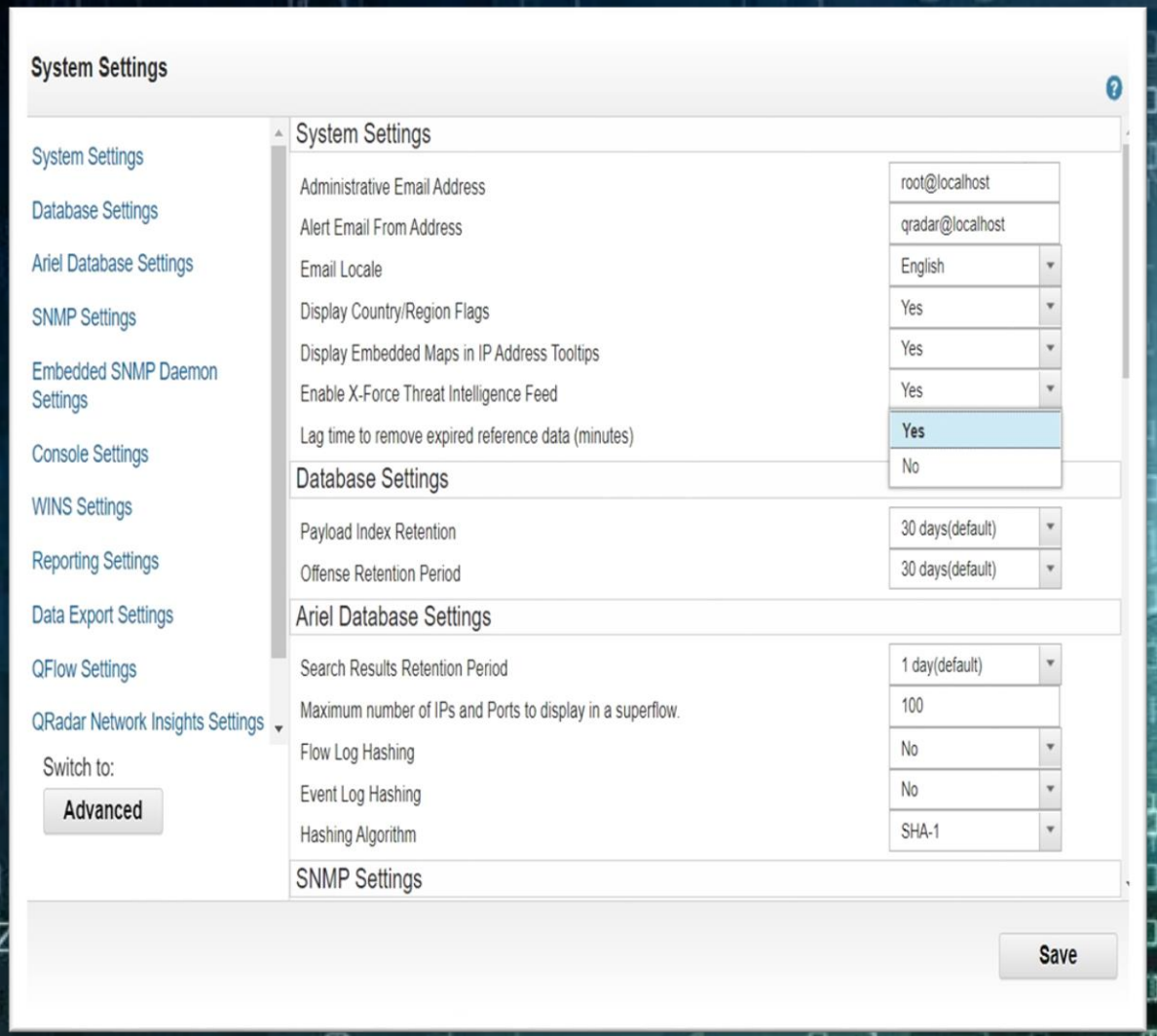
IBM's Threat Intelligence options

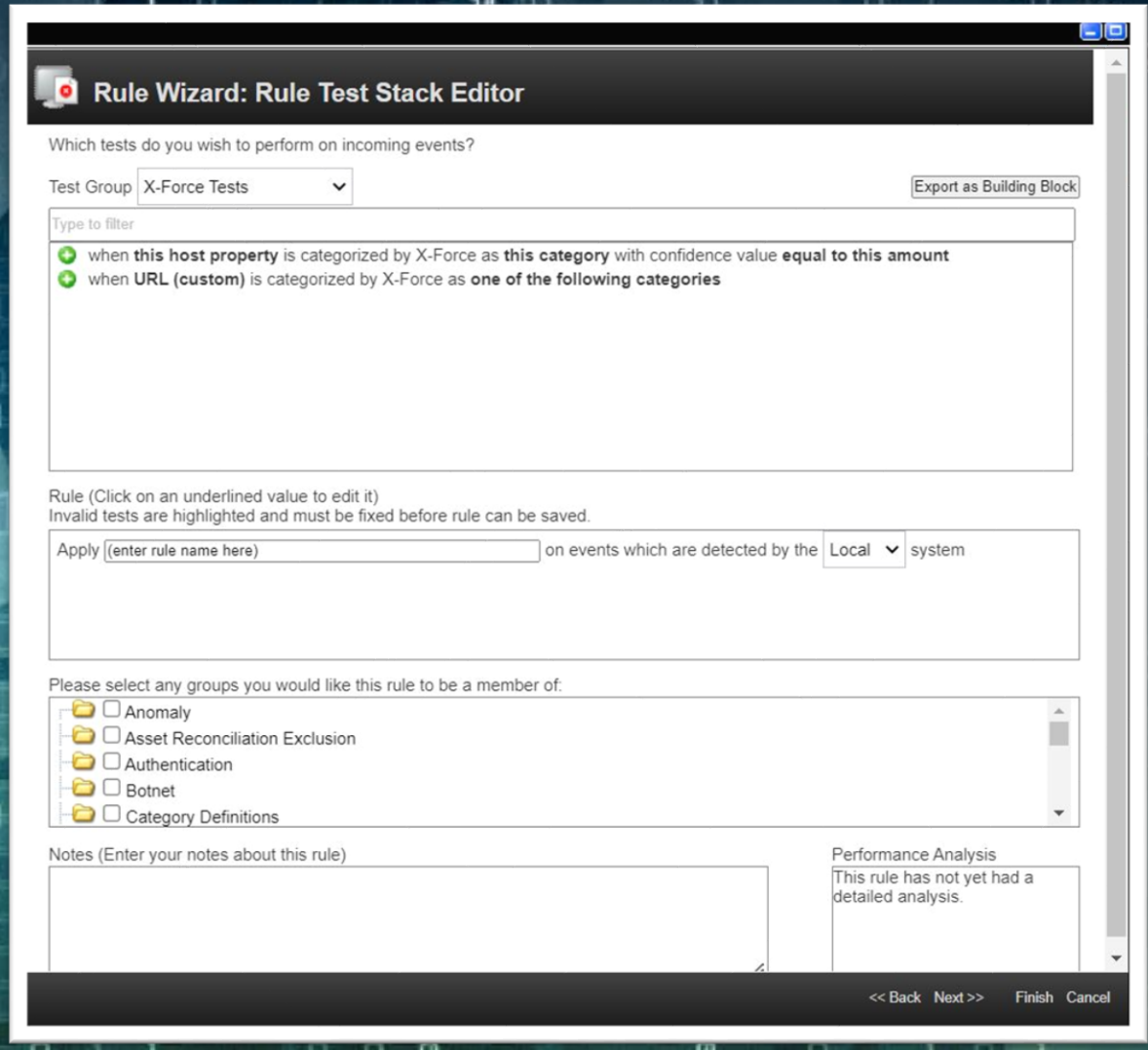
- X-Force Exchange
- X-Force Exchange API Commercial/Enterprise
- Advanced Threat Protection Feed
- Threat Intelligence Insights (XDR Connect)



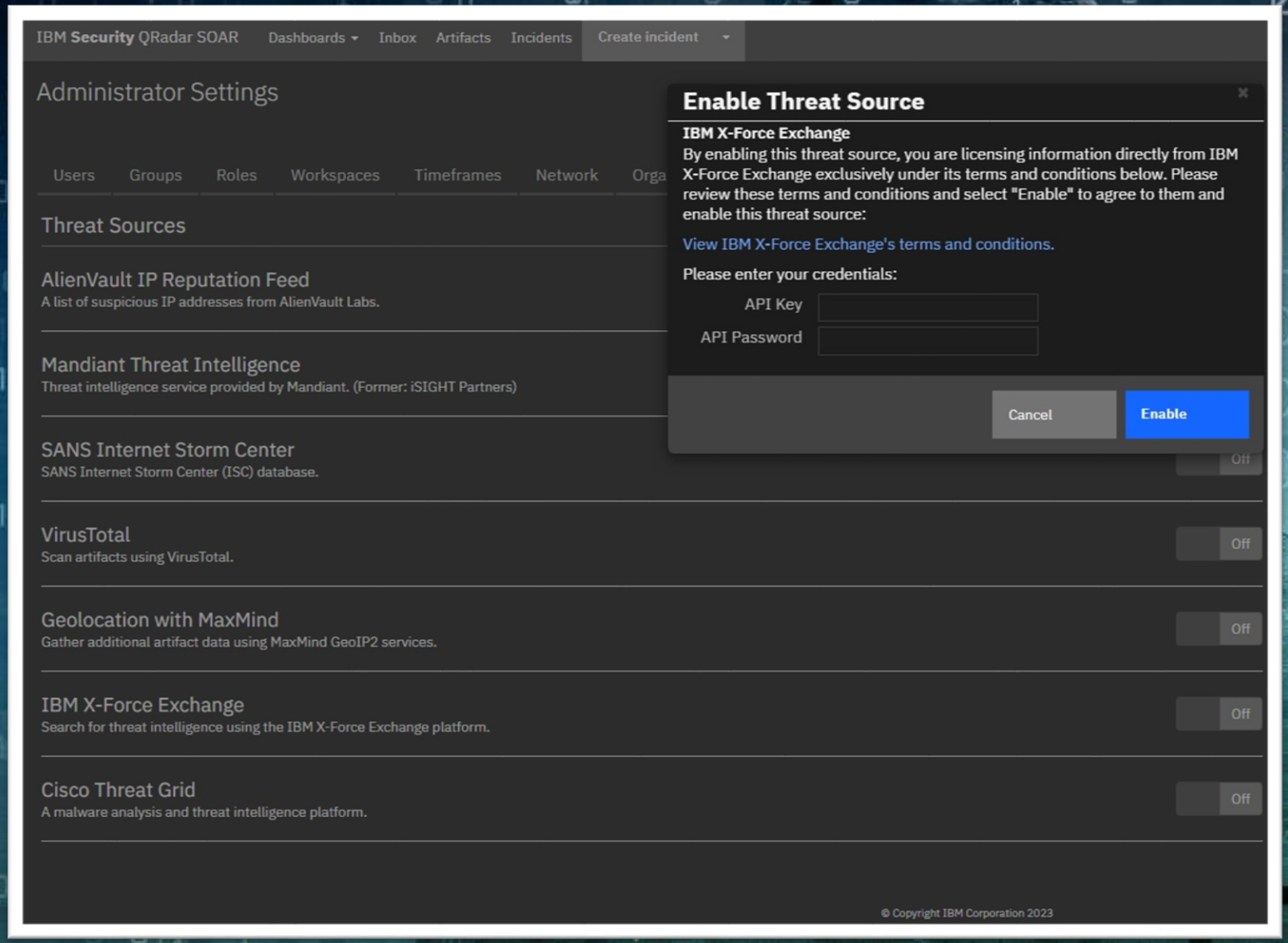
www.cybersecurity.cnsys.bg

X-Force and QRadar SIEM Native Integration





X-Force and QRadar SOAR Integration




HUMAN RESOURCES
OH, NO NEED FOR THAT... WE'VE ALREADY GOT ALL YOUR PERSONAL INFO FROM THE DARK WEB.
Personal
CYBERSECURITY VENTURES
Rothstein /MORGAN 2022

CNSYS
COMPUTERS & NETWORKING

THANK YOU



Vladislav Saykov | CNSys

v.saykov@cnsys.bg

cnsys.bg | +359 2 958 36 00

www.cybersecurity.cnsys.bg