SDS MAINFRAME SECURITY

Automatic STIG Compliance Monitoring for z/OS and iSeries with One Tool

SDS MAINFRAME SECURITY

About SDS

- ▶ Celebrating 40 years in the mainframe industry!
- ▶ Expert development & technical support teams based in MN.
- ▶ 25+ products for mainframe and distributed platforms.
- ▶ Hundreds of organizations worldwide rely on SDS solutions.
- ▶ Focus on mainframe security and compliance.
- ▶ Long-standing global partnerships complement SDS software.
- ▶ Recognized for providing highest quality technical support.

Silver Business Partner IBM.

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

database TREND-SETTING PRODUCTS 2021

IRONSPHERE INSPECTOR

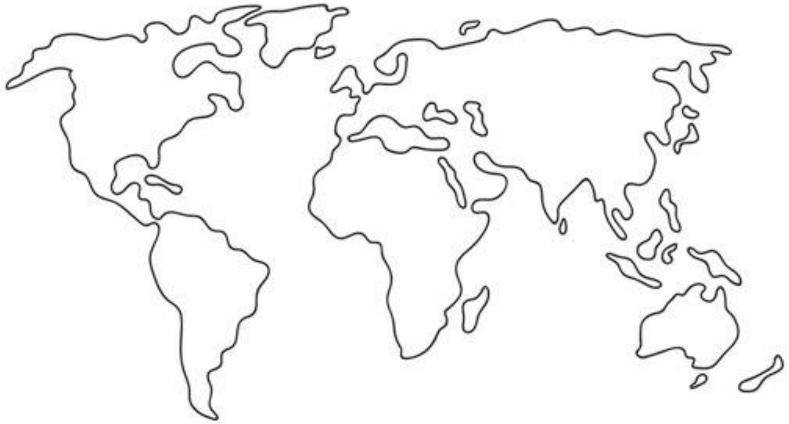
Modern Security monitoring, Review & Document for IBM Legacy Systems

A Product of IronSphere Systems Ltd.

Monitor | Discover | Assess | Report | Investigate | Fix

Who We are

- IronSphere Systems (Subsidiary of SecuriTeam Software)
- Based in Israel (Caesarea Industrial zone)
- Founded in 1999
- Privately Held
- Clients in three continents
  - Major US Banks; US Government



What We do

- Legacy (zSeries & iSeries) Security Automation products
- Standard based (DISA, NIST)
- Automatic Review of Systems, Products, Applications and Users as an extension to DISA STIGs.
- Readiness Review of active system and products.
- Modernizing and Simplifies Legacy security Reviews.

Monitor | Discover | Assess | Report | Investigate | Fix

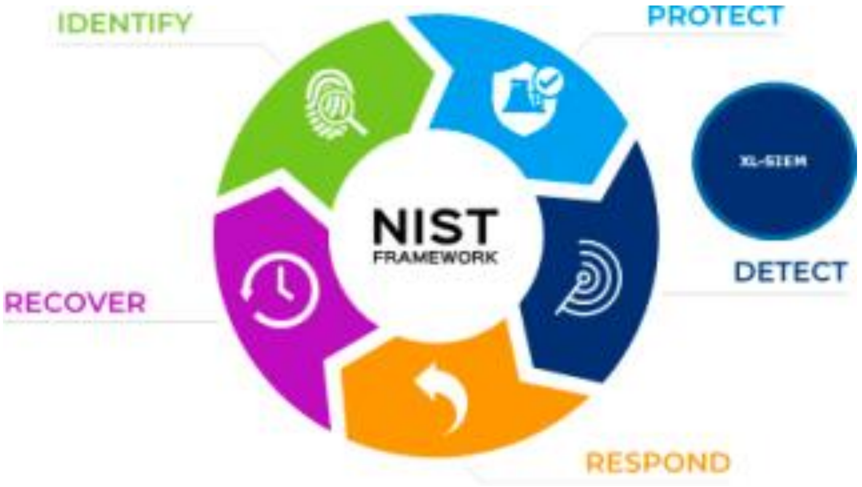
Security STATUS vs EVENT Audit

Event Audit (SIEM)

- Incident reporting based on change or action
- Event source is system logging in various formats.
- Handled by Automation tools and SIEM products
- Has limited information on the event environment
- Has NO information about the effect on security
- Requires technical skills or assistance

Status Audit / Readiness Review (IronSphere)

- Security Control Setting Management (CSM)
- Compares ACTUAL vs RECOMMENDED setting
- Performed periodically based on budget & Skills
- Full information about the risk and potential threat
- Requires technical skills usually consumed as a service



CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE
NIST
RMF
RISK MANAGEMENT FRAMEWORK
nist.gov/rmf

Monitor | Discover | Assess | Report | Investigate | Fix

Threat Landscape is Changing

IBM and Mainframe Changes

- POSIX Unix Since 1994
- Use of Open Source
- Cheaper platforms
- Generation X

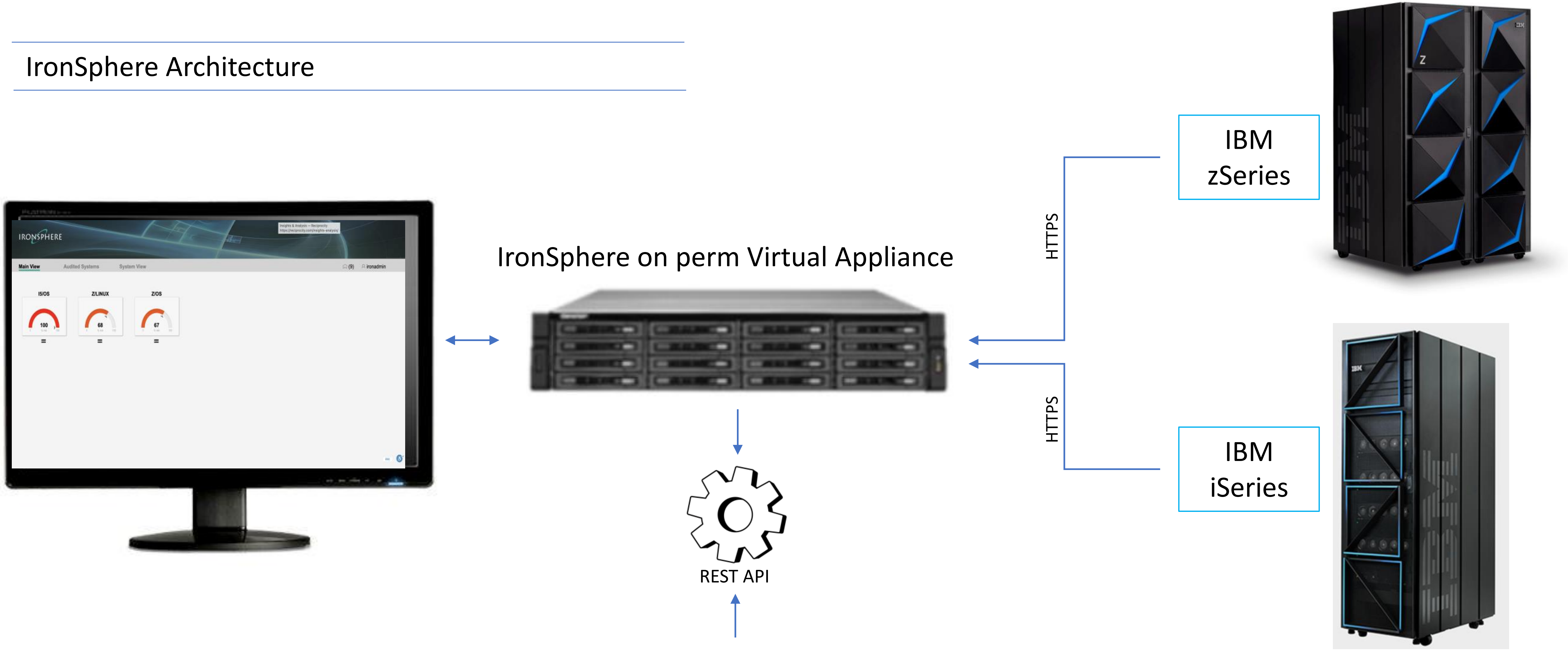
More Malicious Actors

- Foreign Governments
- Terrorist Organizations
- Crime Organizations

Additional Risks

- Client PII
- Organization
- Homeland security

IronSphere Architecture



IronSphere on perm Virtual Appliance

HTTPS

IBM zSeries

HTTPS

IBM iSeries

REST API

Monitor | Discover | Assess | Report | Investigate | Fix

Why IronSphere

Strength

- Does not require legacy system technical skills
- Unattended process based on client’s policy and event triggering
- Standard Based (STIG, ISCM)
- OCO (Object Code Only) – No modification possible
- Active configuration assessment
- Scalable - Single interface - hundreds of LPARs
- Open Architecture (Write your own benchmarks)
- Failure & Success are reported

Tools

- Risk life-cycle management (Exclude / Hide)
- Email notification (policy based)
- Communicate with colleague (Discussion & Document) facility
- Exclude & Hide
- Role-Based access to findings
- Export to XML, CSV, PDF & signed PDF
- Standard extensions to OS components & ISV products

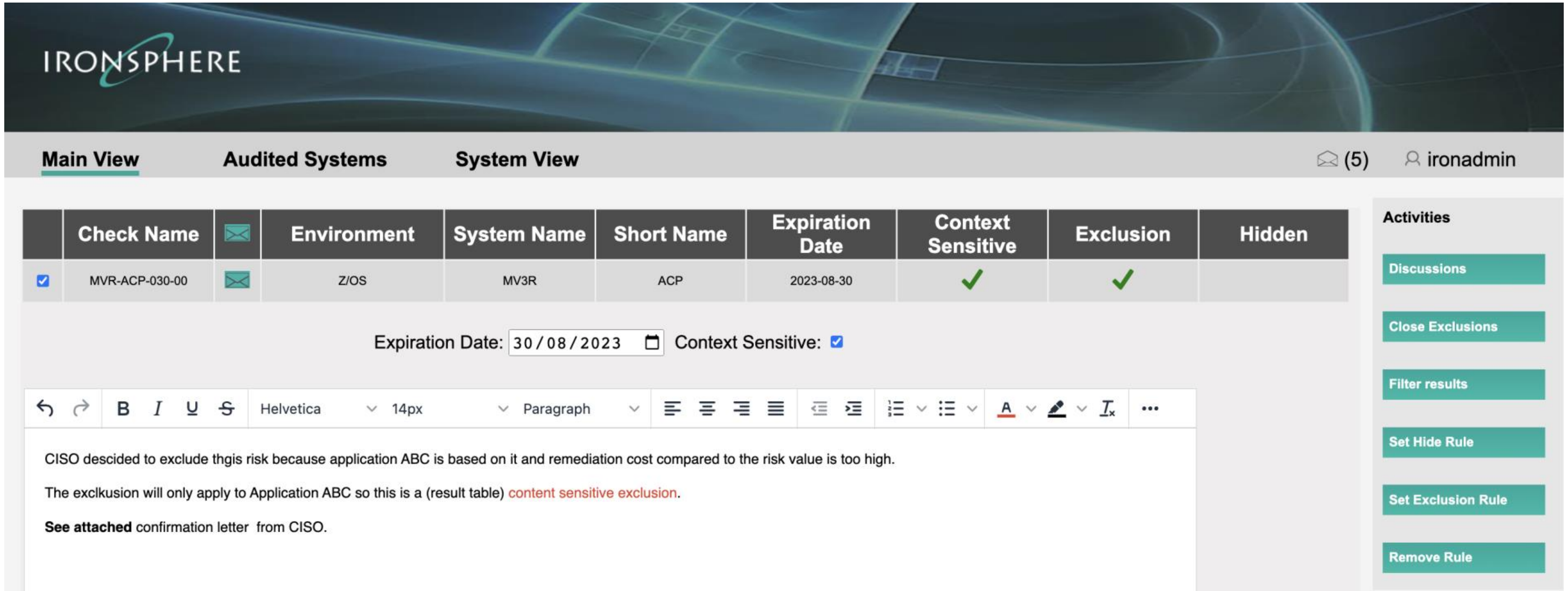
Monitor | Discover | Assess | Report | Investigate | Fix

IronSphere Differentiators

- Starts automatically at IPL as a SUBSYSTEM.
- Scalable. Can assess hundreds of LPARs in minutes!
- Dynamically discover system configuration from working components.
- No GREEN SCREENS, no login to I & Z, Single point of reporting.
- Modernize IBM I & Z assessment.

Exclude & Document finding

- Exclusion means that the risk exists but accepted by client. The calculated risk is reduced by the check severity.
- Every check can be documented in the same way by opening a discussion that allows registered users to respond, open new topics and upload files.
- This way, the long term memory about remediation decision is kept even if people are leaving.



	Check Name	✉	Environment	System Name	Short Name	Expiration Date	Context Sensitive	Exclusion	Hidden
☑	MVR-ACP-030-00	✉	Z/OS	MV3R	ACP	2023-08-30	✓	✓	

Expiration Date: 30/08/2023 Context Sensitive: ☑

CISO descided to exclude thgis risk because application ABC is based on it and remediation cost compared to the risk value is too high.

The exclkusion will only apply to Application ABC so this is a (result table) content sensitive exclusion.

See attached confirmation letter from CISO.

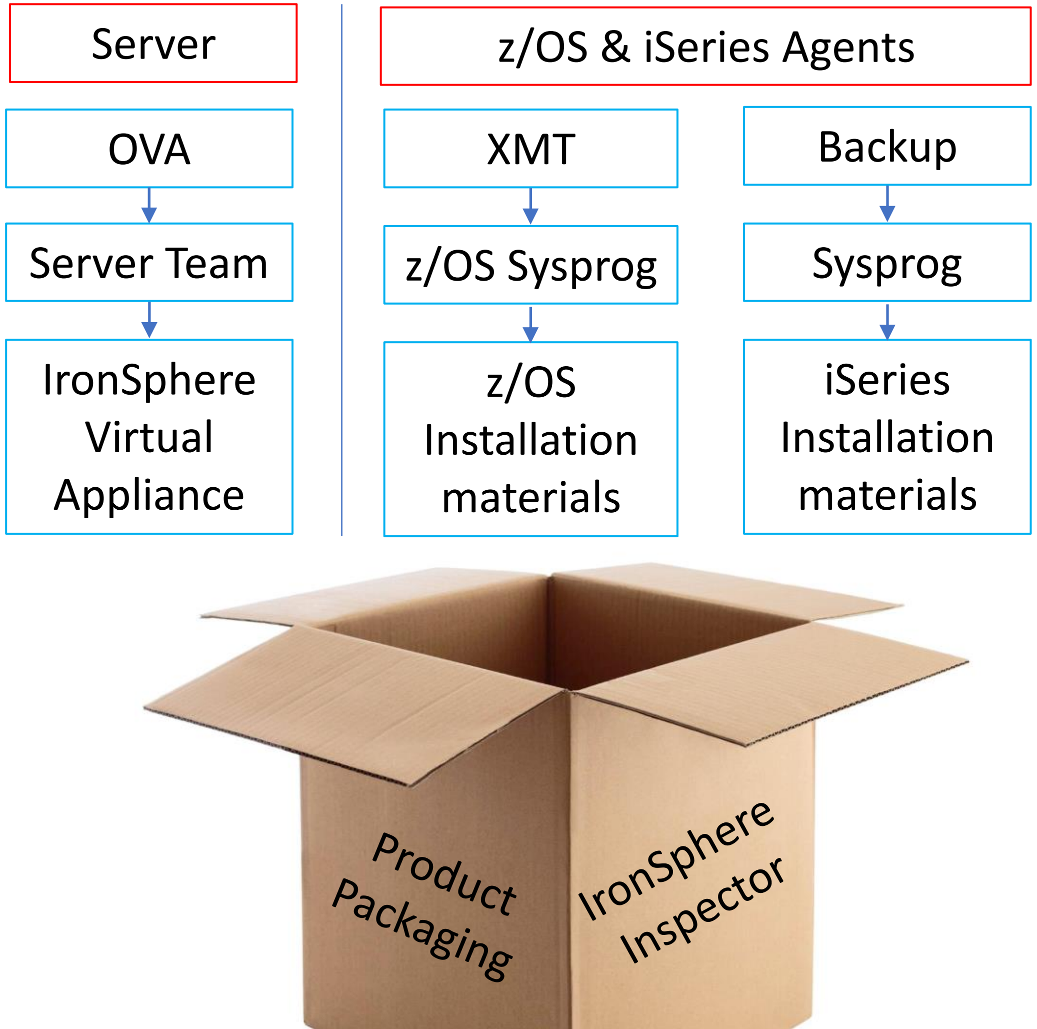
Try it Yourself

Royalty free POC

Benchmarks demonstrate:

- Dynamic Discovery methods
- Interfaces with Systems & Products
- Variety of components
- Web Interface & Tools

24x7 Support during POC



Server

OVA

Server Team

IronSphere Virtual Appliance

z/OS & iSeries Agents

XMT

z/OS Sysprog

z/OS Installation materials

Backup

Sysprog

iSeries Installation materials

Product Packaging

IronSphere Inspector

SDS MAINFRAME SECURITY

Would you like additional information?

info@sdsusa.com

(800) 443-6183
(763) 571-9000

www.sdsusa.com