RAZ-LEE

EDR on IBM i:

Detect, Protect and Respond with iSecurity

How to achieve Endpoint Detection & Response with Antivirus, Anti-Ransomware, Firewall, Audit and Action.



The problem: Are we Under Attack?

"What happens after a Threat reaches your IBM i environment?"

Traditional security often focuses on prevention.

EDR adds another question:

"What is happening Right Now, and what can we do about it?"

What Is EDR?

1. Continuous Monitoring

Observe relevant activity across:

- Files
- Processes/jobs
- Network connections
- User activity
- Security events

2. Threat Detection

Identify:

- Malware
- Ransomware
- Suspicious activity
- Unauthorized access
- Network attacks
- Potentially compromised accounts

3. Automated Response

Respond to detected events

:

- Blocking
- Isolation
- Alerts
- Termination
- Security actions

4. Investigation & Forensics

Understand:

- What happened?
- When?
- Which user?
- Which resource?
- Which network connection?
- What changed?
- What action was taken?

RAZ-LEE iSecurity

Why EDR on IBM i?

IBM i is not simply another endpoint. It may be hosting:

- ERP
- Banking applications
- Manufacturing applications
- Databases
- Customer information
- Financial transactions
- APIs
- IFS files
- Business-critical applications

Let´s be clear:

"A security incident on IBM i can therefore have a direct operational impact. “

The objective is not only

"Prevent the Attack. It is:

…”

EDR Objetives



Why Antivirus Alone Is Not EDR

Antivirus is essential, but it addresses only part of the security problem.

For example::



Antivirus

Detects Malware.

But what about?

- **Suspicious network activity?**
- **Ransomware behavior?**
- **Unauthorized user activity?**
- **What should happen when something suspicious is detected?**

EDR is not simply Antivirus with a different name. It is an integrated detection and response strategy.

RAZ-LEE iSecurity

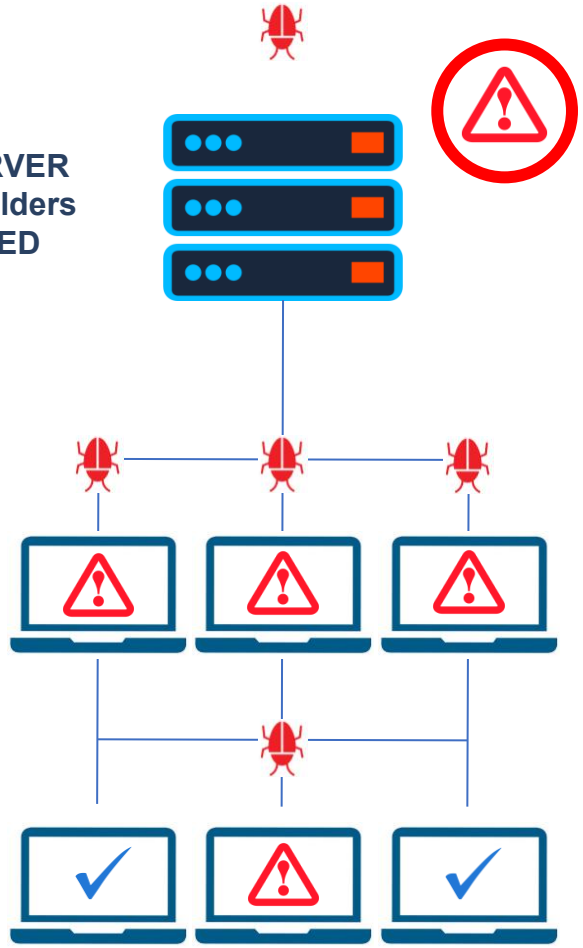
RAZ-LEE

iSecurity Antivirus



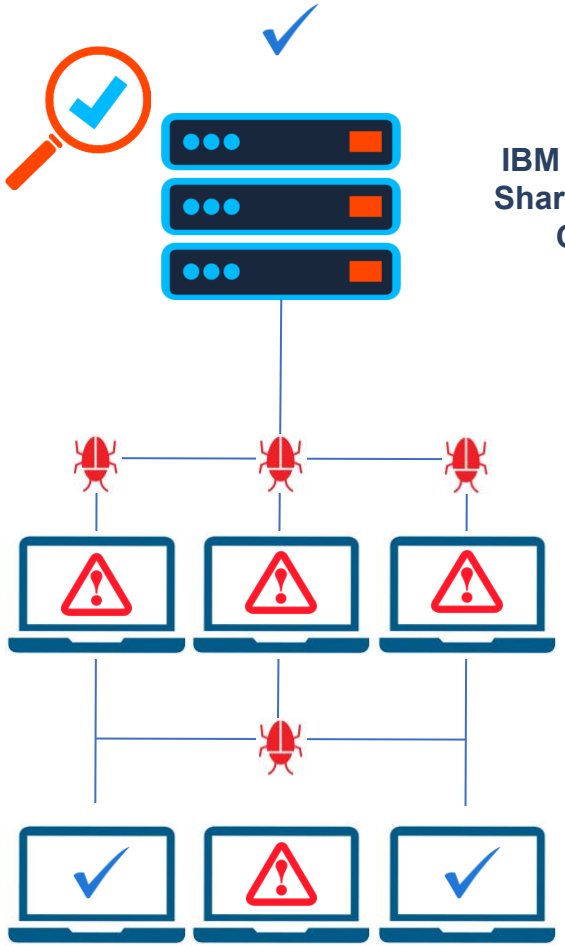
iSecurity Antivirus

IBM i SERVER
Shared Folders
INFECTED





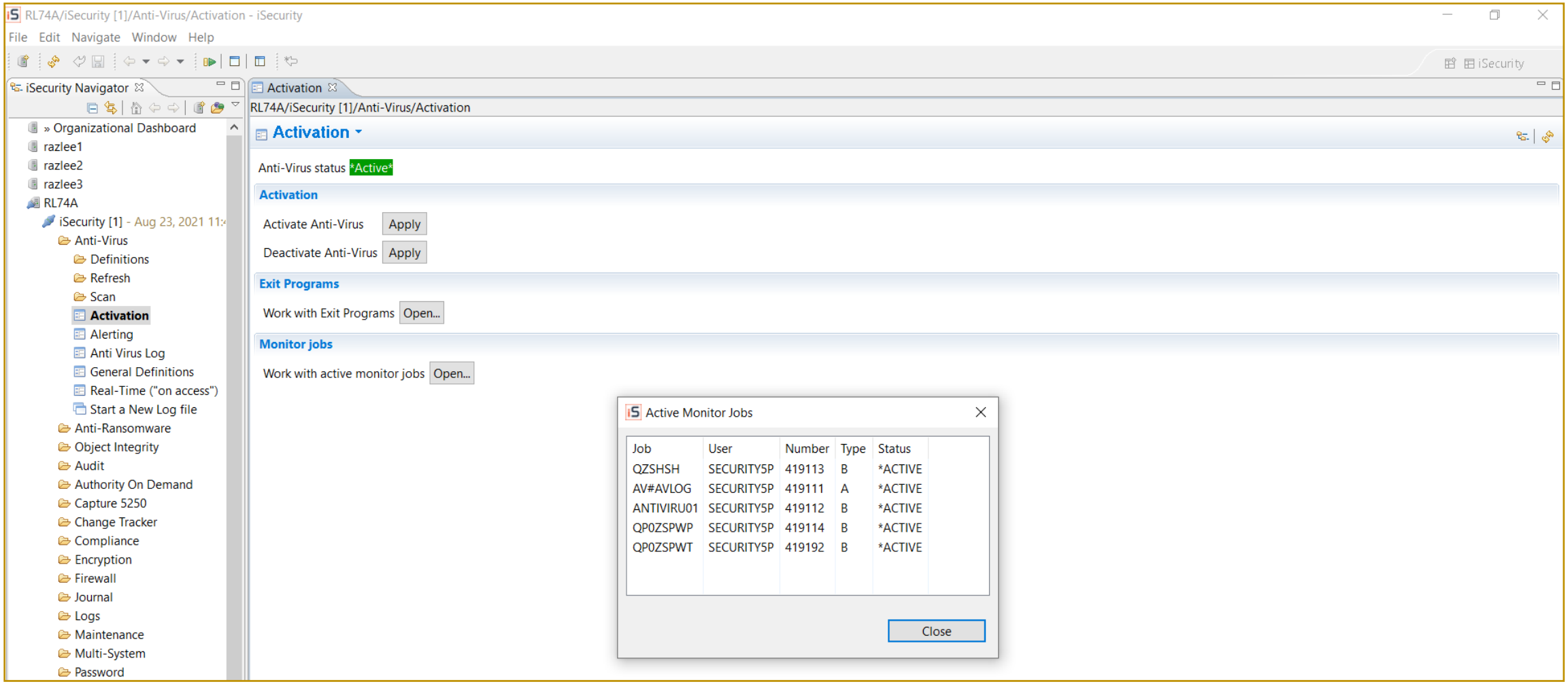
Any PC on the Network
can Execute the Virus



IBM i SERVER
Shared Folders
CLEAN

RAZ-LEE
iSecurity

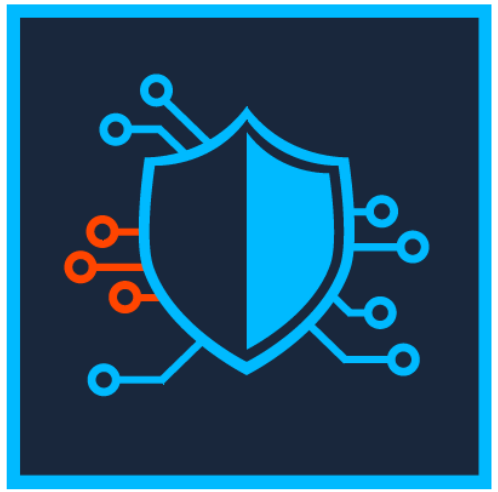
Activation Screen (GUI)



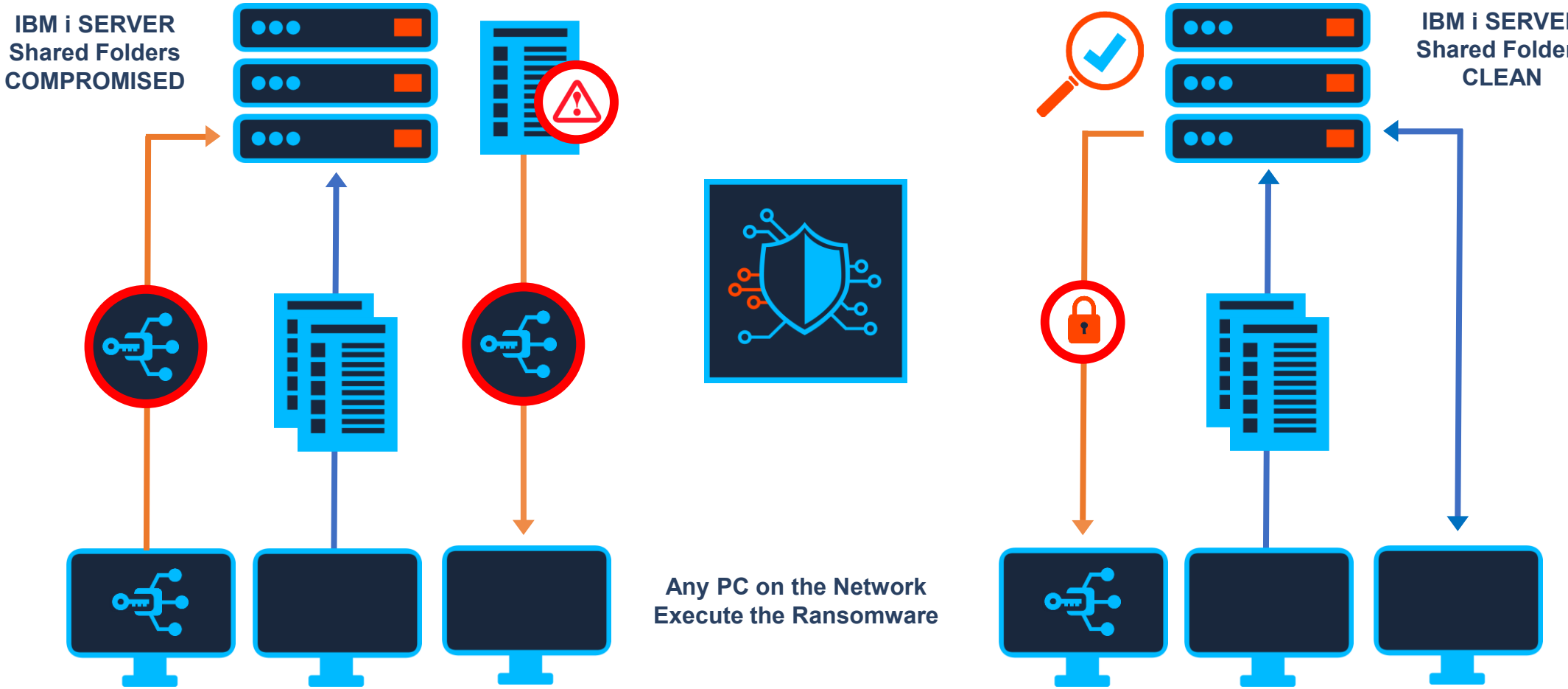
RAZ-LEE

iSecurity

Anti-Ransomware

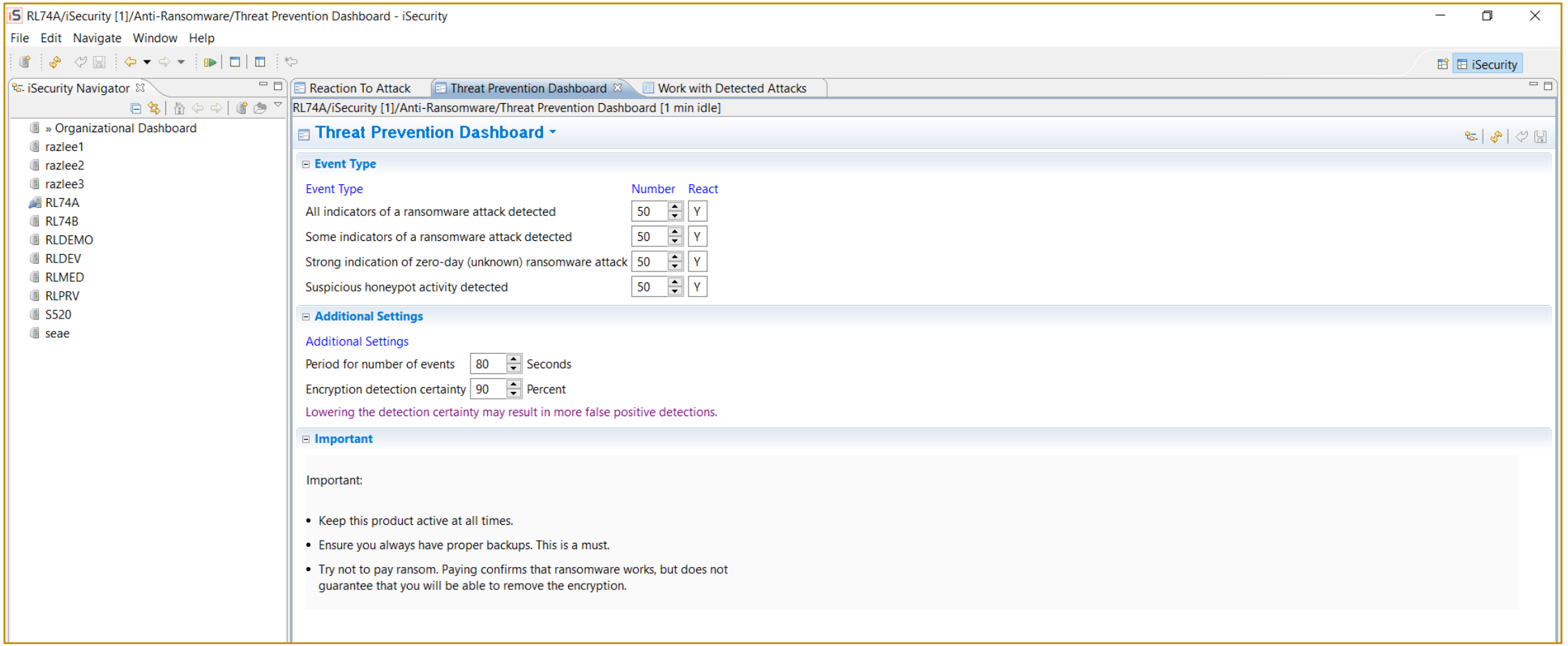


iSecurity Anti-Ransomware



RAZ-LEE iSecurity

Activation Screen (GUI)



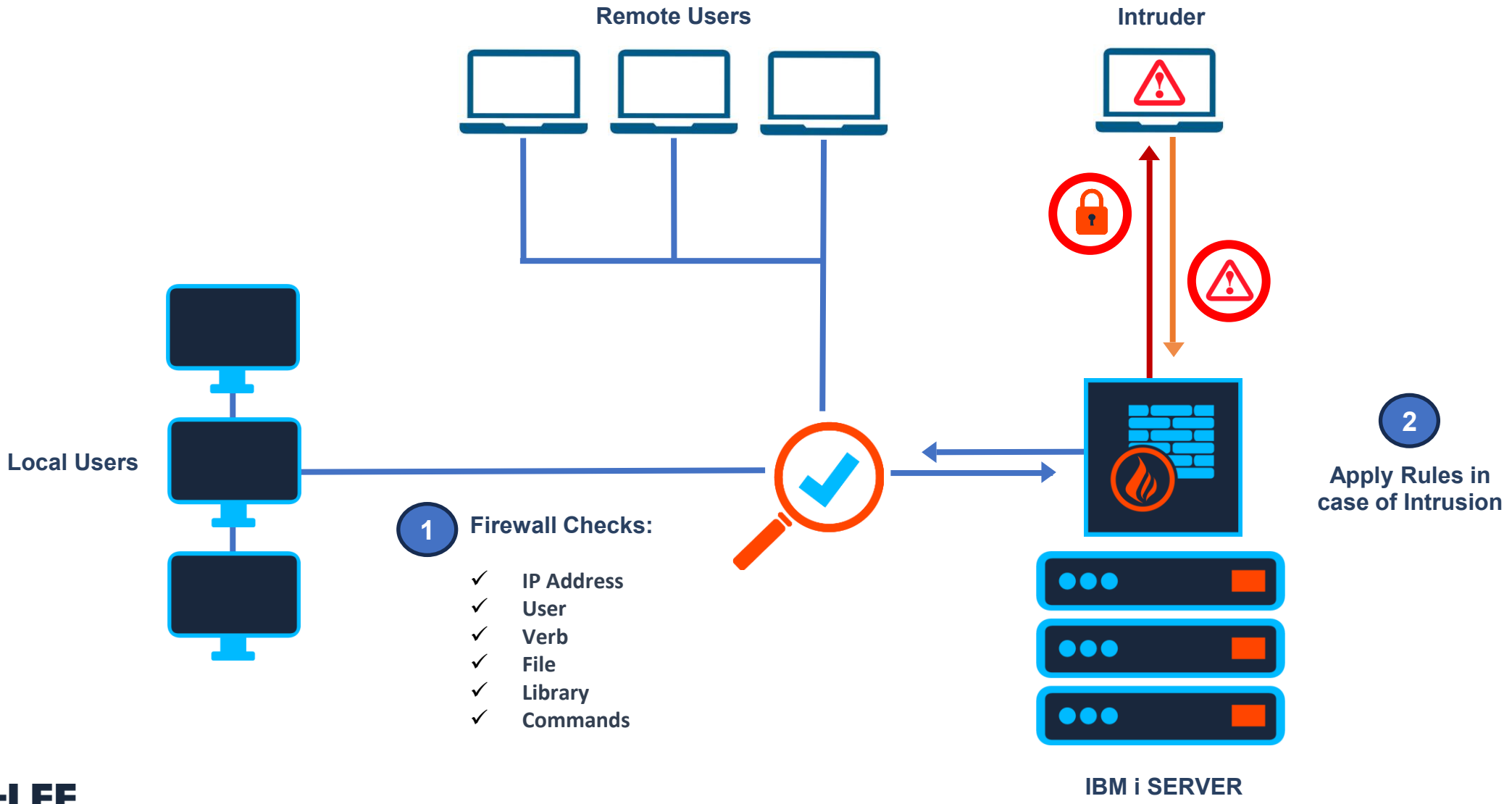
RAZ-LEE iSecurity

RAZ-LEE

iSecurity Firewall

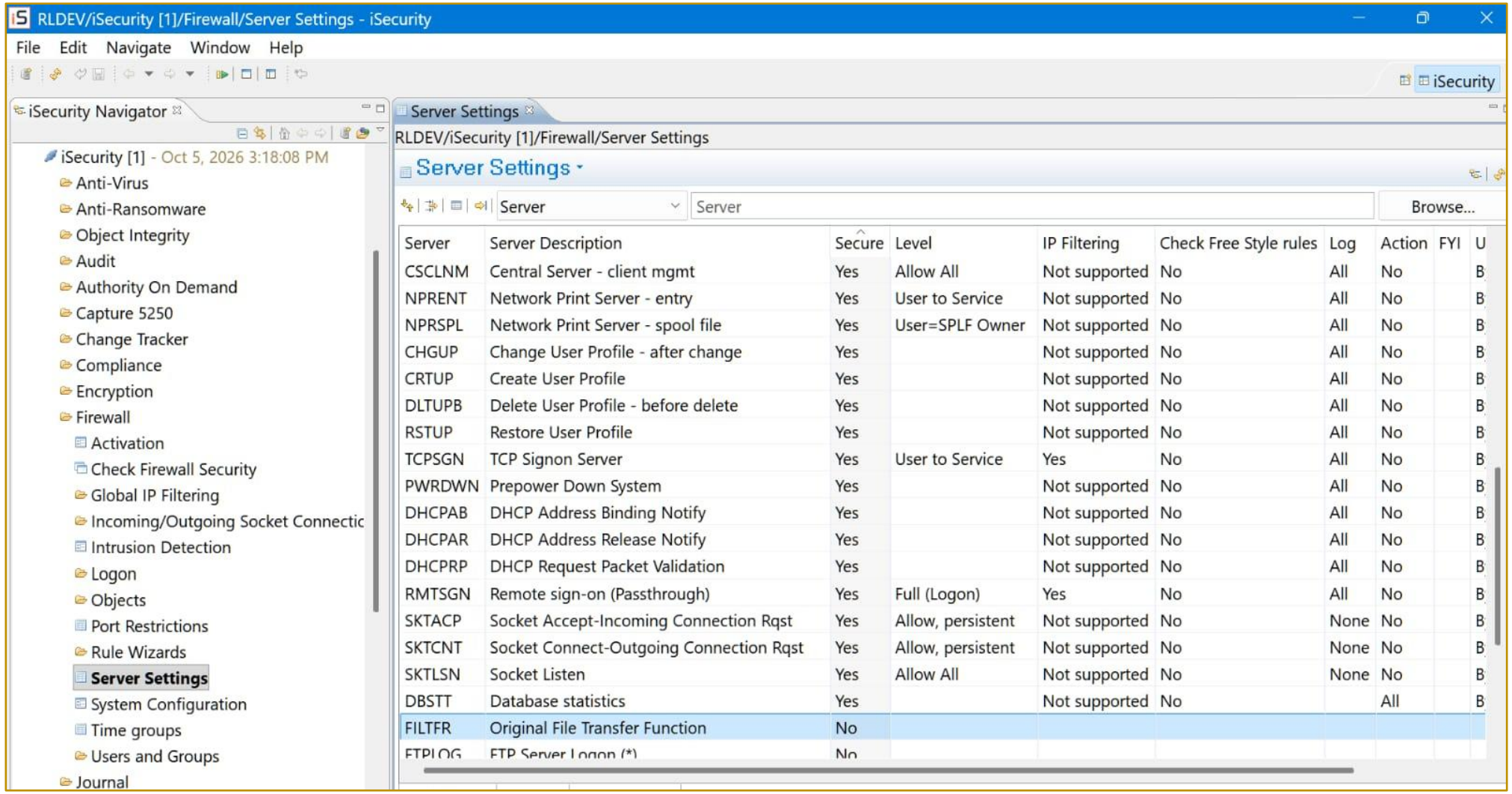


iSecurity Firewall



RAZ-LEE iSecurity

Server Settings Screen (GUI)



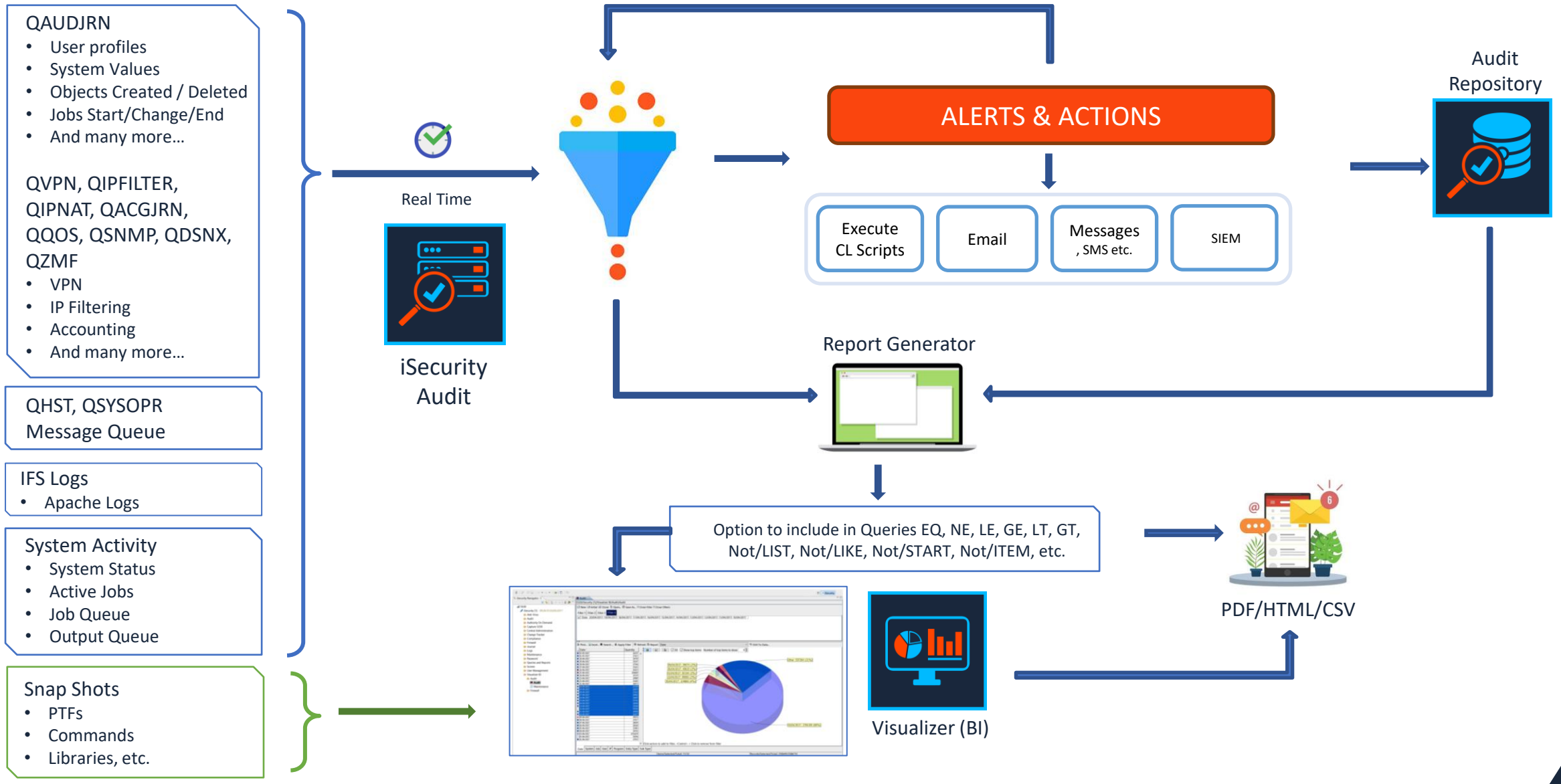
RAZ-LEE iSecurity

RAZ-LEE

iSecurity Audit



iSecurity Audit

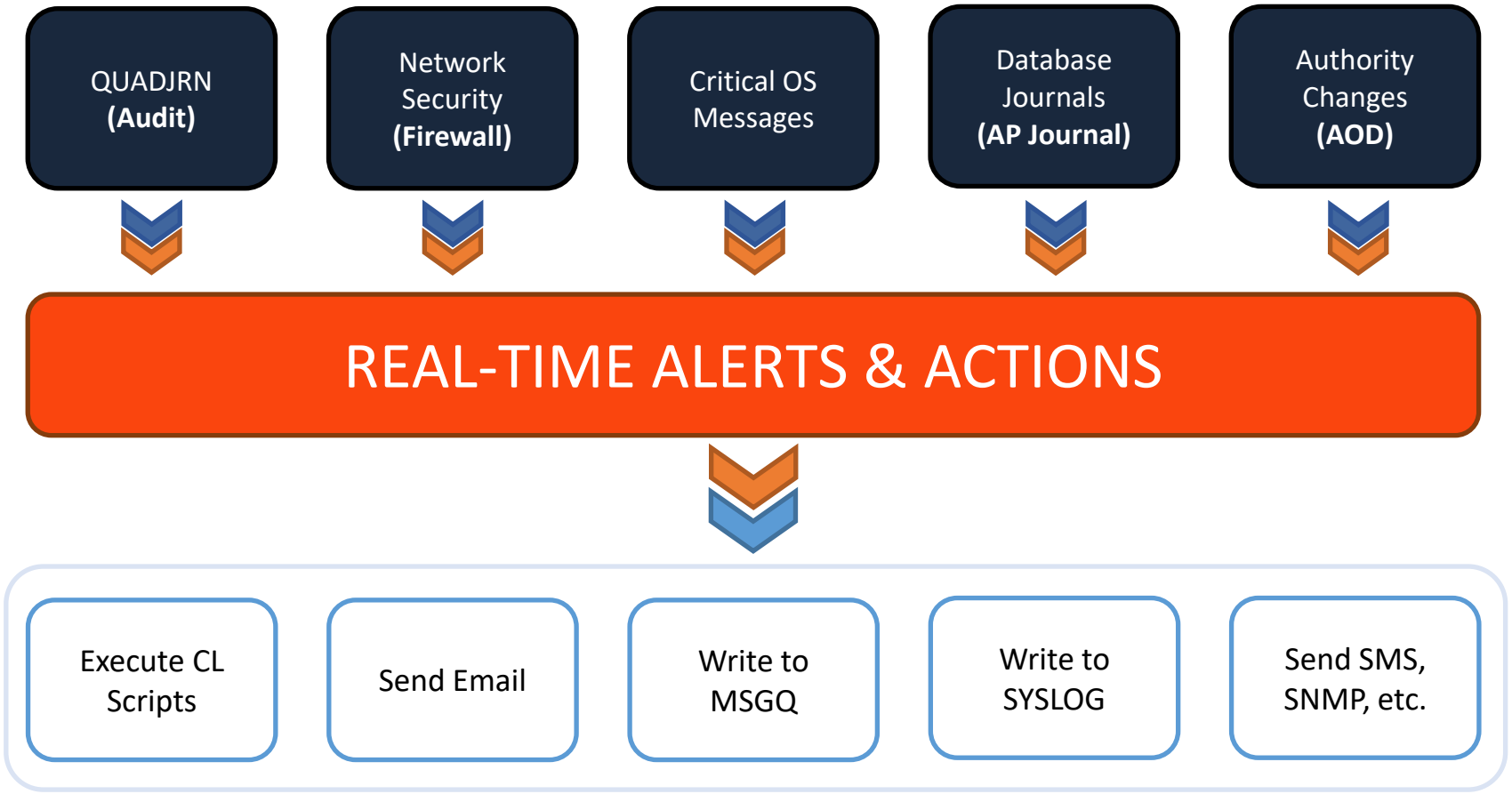


RAZ-LEE

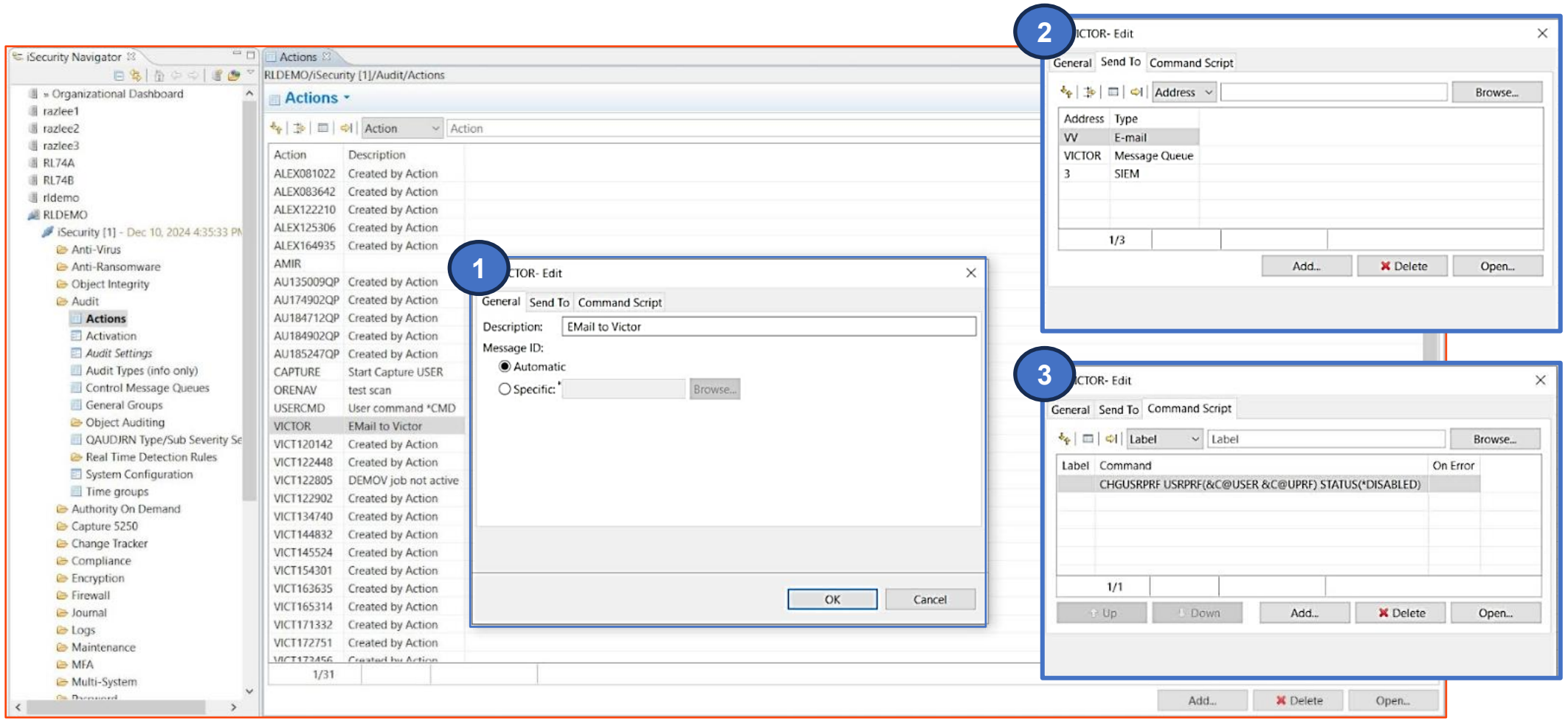
iSecurity Action



iSecurity Action

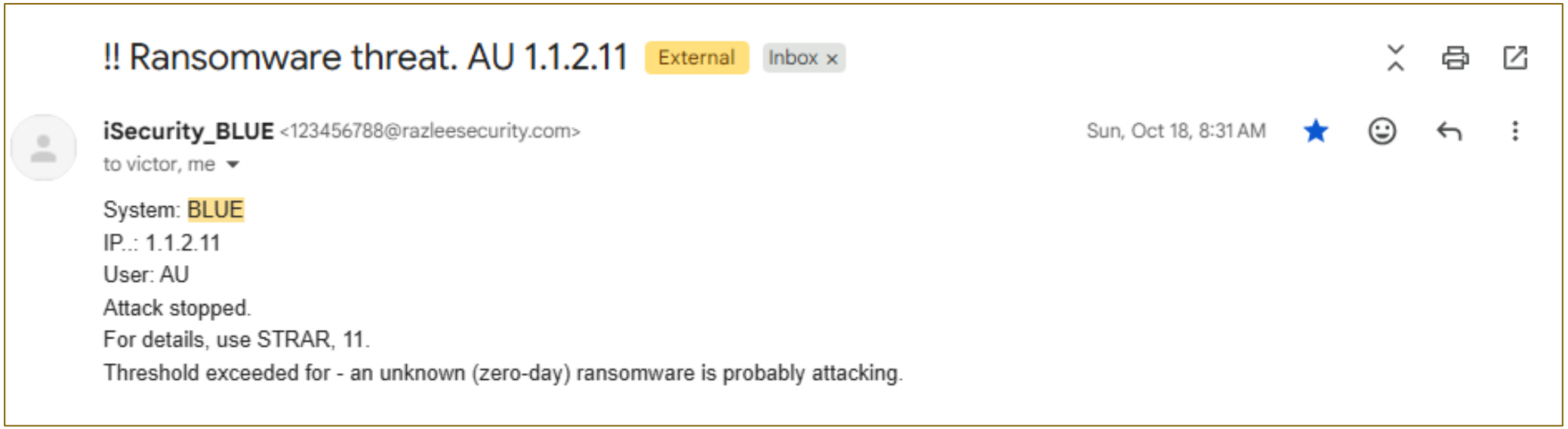


Defining Action that Sends Email and Blocks a User (GUI)



RAZ-LEE iSecurity

e-mail Alert



!! Ransomware threat. AU 1.1.2.11 External Inbox ×

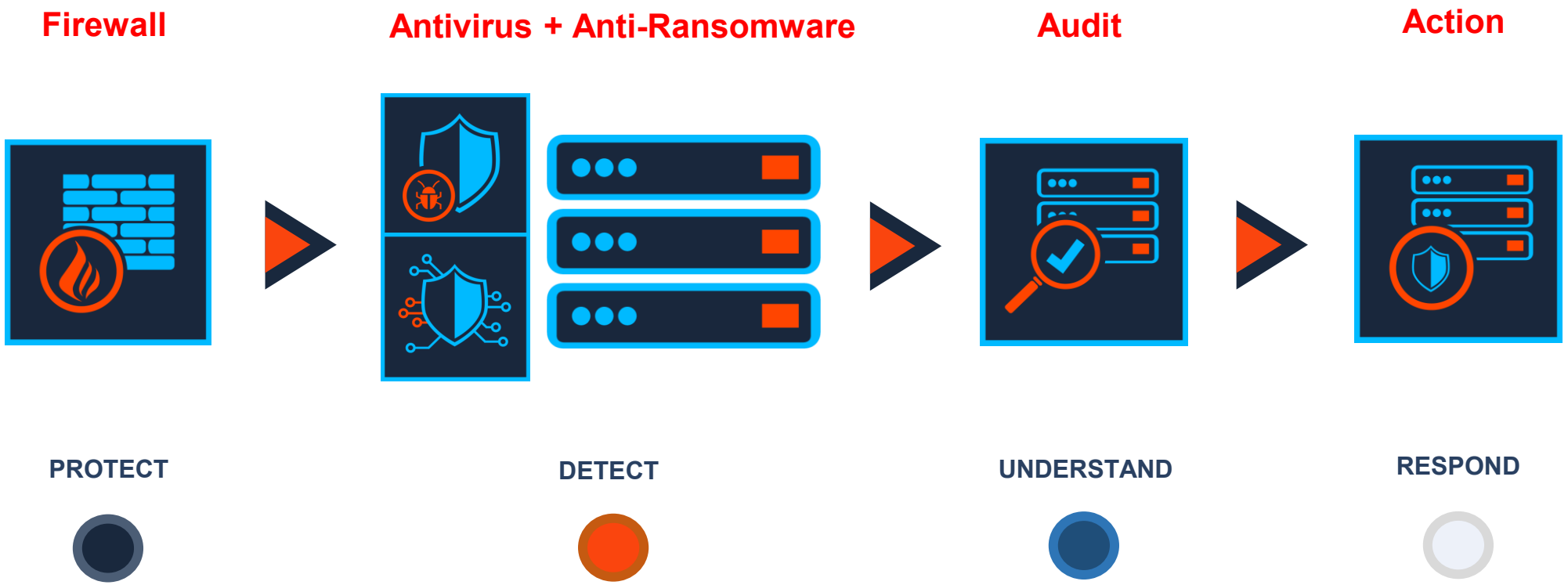
iSecurity_BLUE <123456788@razleesecurity.com> Sun, Oct 18, 8:31 AM

to victor, me

System: BLUE
IP..: 1.1.2.11
User: AU
Attack stopped.
For details, use STRAR, 11.
Threshold exceeded for - an unknown (zero-day) ransomware is probably attacking.

RAZ-LEE iSecurity

Achieving EDR with iSecurity



RAZ-LEE iSecurity

iSecurity Action Advantages

- ✓ Responds to events detected by **Audit**, **Firewall**, **AP-Journal**, etc.
- ✓ Alert messages sent via **Syslog, SNMP, e-mail, SMS, MSGQ or Twitter**.
- ✓ Automatically **takes corrective actions** by running command scripts or programs.
- ✓ **Rule Wizard** makes definition process simple for non-technical users.
- ✓ Rules can use **many different selection criteria**.
- ✓ **Built-in command script interpreter** with replacement variable support.
- ✓ Responds to current **system status parameters and active jobs**.
- ✓ **Restrict user access** during vacations, holidays and other planned absences.
- ✓ Automatically **Disables Inactive User Profiles**.
- ✓ Tight **Control over Authority Adoption**.



RAZ-LEE iSecurity

RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com



RAZ-LEE

See you Soon!

Thanks for your Attention

Marketing Manager

Moshe Sofer

Visit our Website for more Information

www.razlee.com