CERT-GOV

DRIDI Mohamed

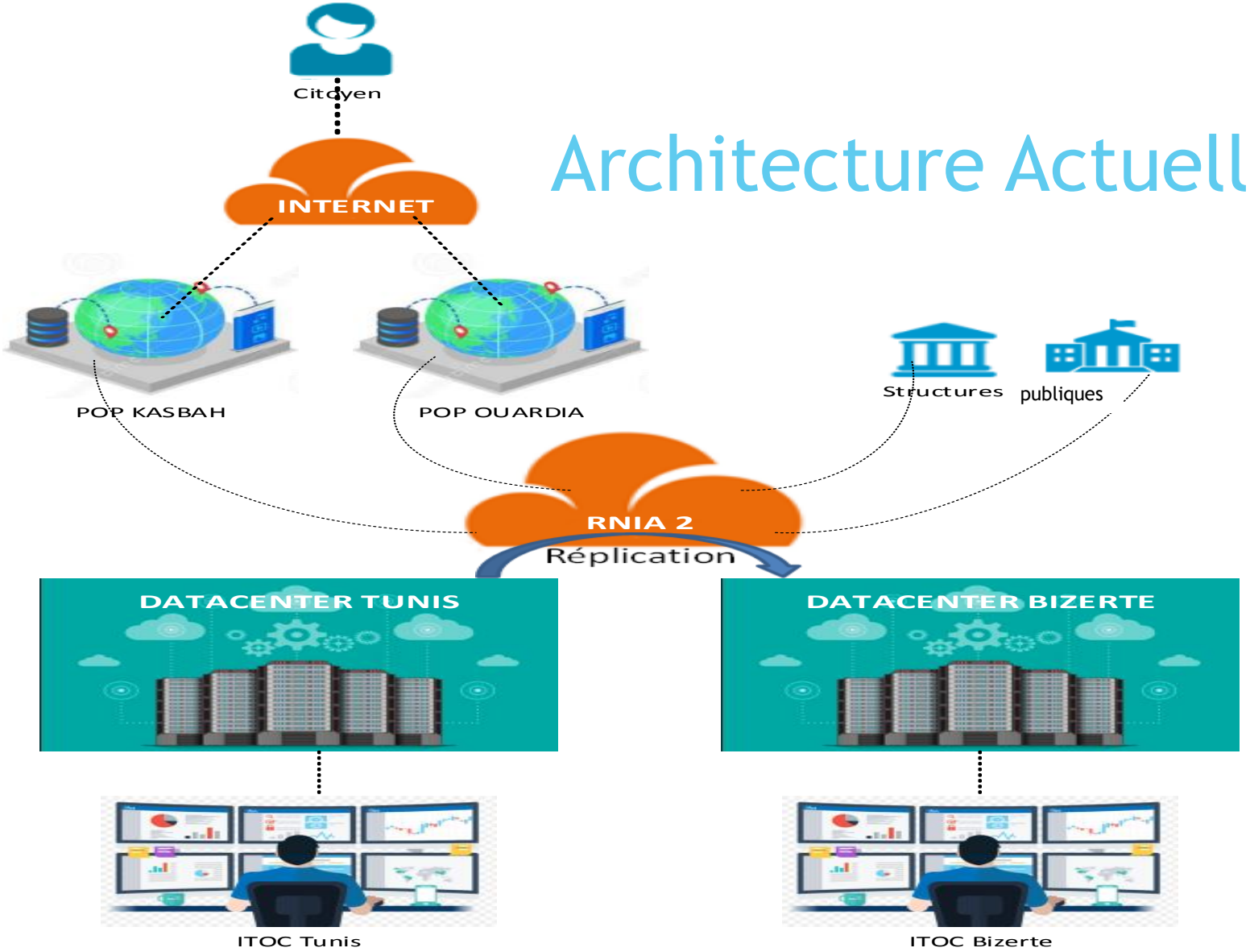
Octobre 2018

Périmètre

Les applications nationales les plus critiques exploitées par les ministères, les municipalités et les établissements publics (tel que INSAF, RACHED, ADEB, GEC, MADANIA, Suivi des grands projets et GRB, …) ainsi que les utilisateurs de ces applications.

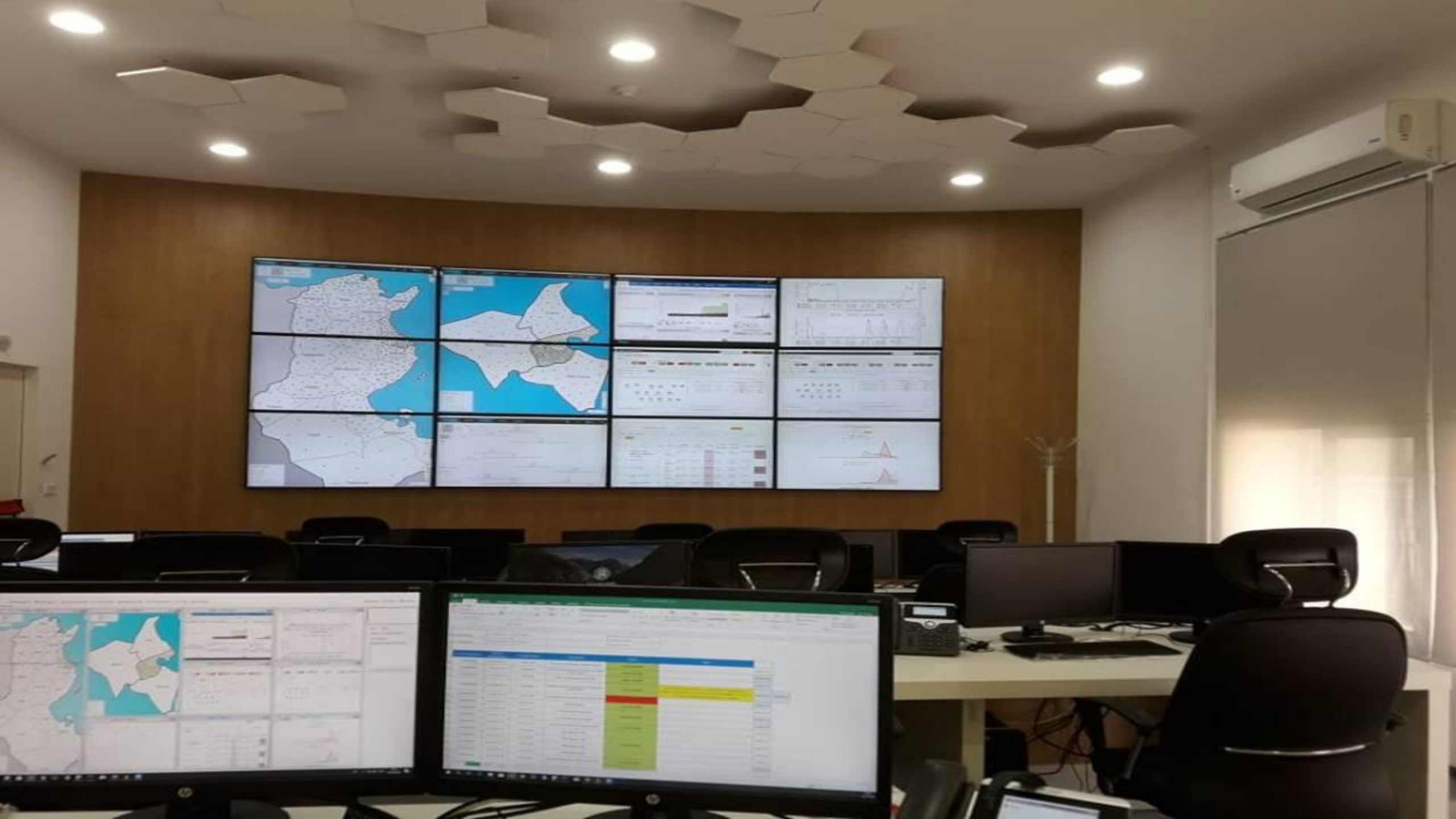
- RNIA
- Les DATACENTERS du CNI

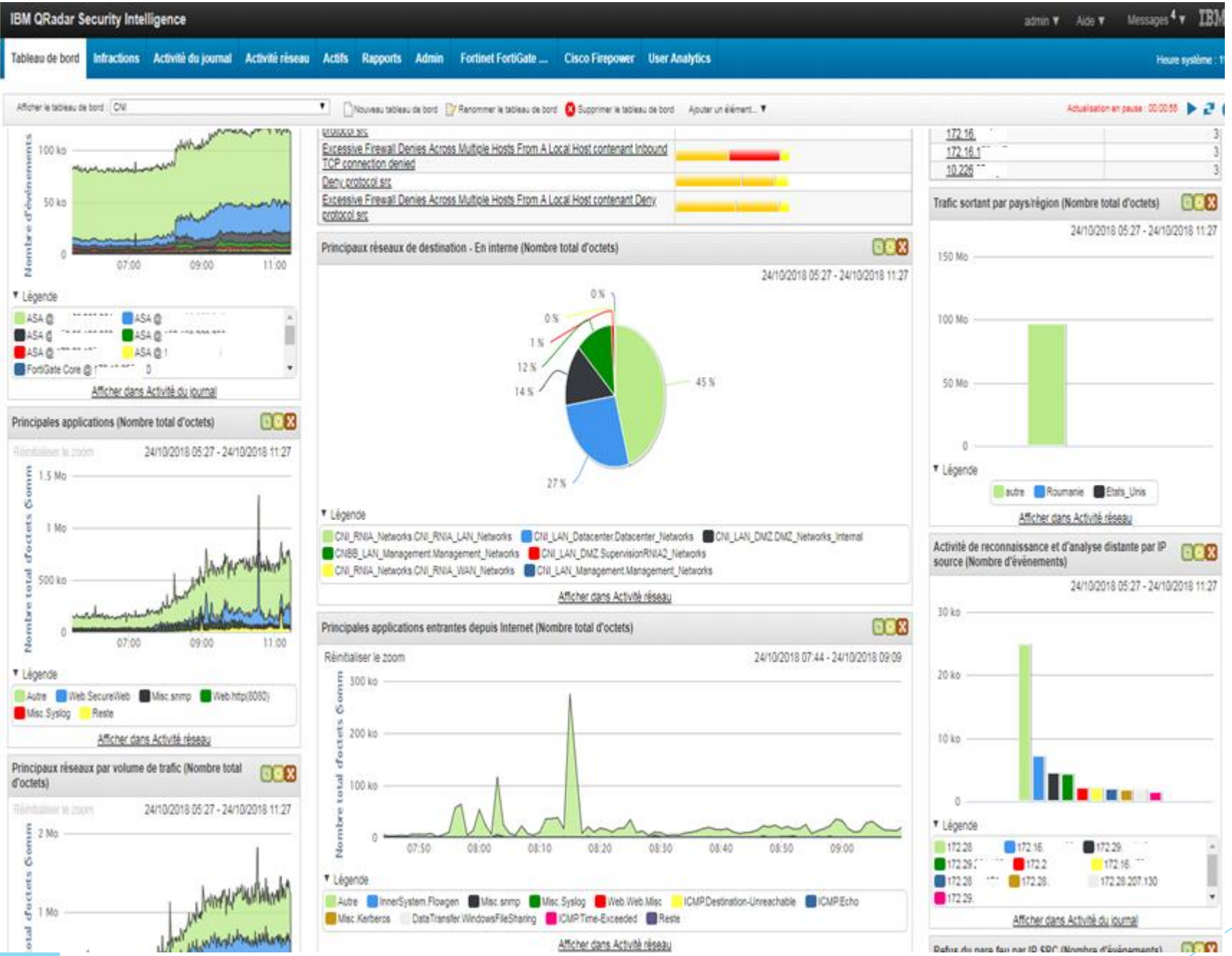
Architecture Actuelle



SOC

- Assurer la supervision du SI, la détection et la résolution des incidents de sécurité
- Rapidité du temps de réponse. (En cas de malware ou d'une attaque par déni de service la vitesse d'intervention de l'équipe est primordiale)
- Capacité à se remettre d'une attaque en un temps raisonnable
- Identification plus rapide d'attaques potentielles et prévention desdites attaques avant qu'elles ne causent des dommages
- Le SIEM est le principal outil du SOC
  - Permet d'agréger les événements de sécurité en un point
  - Avoir une visibilité de l'ensemble du périmètre




IBM QRadar Security Intelligence
admin
Aide
Messages
Tableau de bord
Intractions
Activité du journal
Activité réseau
Actifs
Rapports
Admin
Fortinet FortiGate ...
Cisco Firepower
User Analytics
Heure système
Afficher le tableau de bord : CNI
Nouveau tableau de bord
Renommer le tableau de bord
Supprimer le tableau de bord
Ajouter un élément...
Actualisation en pause : 00:00:55
Nombre d'événements
100 ko
50 ko
0
07:00
09:00
11:00
Légende
ASA @
ASA @
ASA @
ASA @
ASA @
ASA @
ASA @
ASA @
FortiGate Core @
Afficher dans Activité du journal
Excessive Firewall Denies Across Multiple Hosts From A Local Host contenant Inbound TCP connection denied
Deny protocol src
Excessive Firewall Denies Across Multiple Hosts From A Local Host contenant Deny protocol src
172.16.
172.16.1
10.226
Principaux réseaux de destination - En interne (Nombre total d'octets)
24/10/2018 05:27 - 24/10/2018 11:27
0 %
0 %
1 %
12 %
14 %
45 %
27 %
Légende
CNI_RNIA_Networks.CNI_RNIA_LAN_Networks
CNI_LAN_Datacenter.Datacenter_Networks
CNI_LAN_DMZ.DMZ_Networks_Internal
CNIBB_LAN_Management.Management_Networks
CNI_LAN_DMZ.SupervisionRNIA2_Networks
CNI_RNIA_Networks.CNI_RNIA_WAN_Networks
CNI_LAN_Management.Management_Networks
Afficher dans Activité réseau
Trafic sortant par pays/région (Nombre total d'octets)
24/10/2018 05:27 - 24/10/2018 11:27
150 Mo
100 Mo
50 Mo
0
Légende
autre
Roumanie
Etats_Unis
Afficher dans Activité réseau
Principales applications (Nombre total d'octets)
Réinitialiser le zoom
24/10/2018 05:27 - 24/10/2018 11:27
Nombre total d'octets (Somm
1.5 Mo
1 Mo
500 ko
0
07:00
09:00
11:00
Légende
Autre
Web SecureWeb
Misc snmp
Web http(8080)
Misc Syslog
Reste
Afficher dans Activité réseau
Principales applications entrantes depuis Internet (Nombre total d'octets)
Réinitialiser le zoom
24/10/2018 07:44 - 24/10/2018 09:09
Nombre total d'octets (Somm
300 ko
200 ko
100 ko
0
07:50
08:00
08:10
08:20
08:30
08:40
08:50
09:00
Légende
Autre
InnerSystem Flowgen
Misc snmp
Misc Syslog
Web Web Misc
ICMP Destination-Unreachable
ICMP Echo
Misc Kerberos
DataTransfer WindowsFileSharing
ICMP Time-Exceeded
Reste
Afficher dans Activité réseau
Activité de reconnaissance et d'analyse distante par IP source (Nombre d'événements)
24/10/2018 05:27 - 24/10/2018 11:27
30 ko
20 ko
10 ko
0
Légende
172.28
172.16.
172.29.
172.29.
172.2
172.16.
172.28
172.28.
172.28.207.130
172.29.
Afficher dans Activité du journal
Refus du pare-feu par IP SRC (Nombre d'événements)
Overview
Analysis
Policies
Devices
Objects
AMP
Context Explorer
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom
Lookup
Search
Intrusion Events by Priority
Top Targets
Top Ingress Security Zones
No Data
Intrusion Event Details
Event
Classification
Priority
Events
BLACKLIST DNS request for known malware domain proxim.ircgalaxy.pl -
A Network Trojan was Detected
high
115
Overview
Analysis
Policies
Devices
Objects
AMP
Dashboards
Reporting
Summary
Detailed Dashboard
Provides a detailed view of activity on the appliance
Intrusion Events
Context
Correlation
Status
Intrusion Events
Last 1 hour
EPS
All Intrusion Events (Not Dropped)
Classification
Count
A Network Trojan was Detected
109
Last updated 2 minutes ago
All Intrusion Events
Dropped Intrusion Events
Classification
Count
A Network Trojan was Detected
843

Projet Cert-Gov

Il s'agit de mettre en place une structure de réponse aux incidents informatique et de veille technologique, qui permettra de :

- **Identifier** et **analyser** les menaces potentielles qui peuvent toucher les applications nationales .
- **Fournir** de l'assistance en matière de sécurité informatique, pour le **recueil** des déclarations d'incidents de sécurité et d'**intervenir** à distance ou sur place avec les parties prenantes pour réduire ses impacts ;
- **Alerter** les utilisateurs des applications nationales sur les menaces de sécurité et les **assister** à prendre les mesures de prévention nécessaires ;
- **Sensibiliser** les utilisateurs des applications nationales sur les problèmes de sécurité informatique et les **informer** sur les risques encourus et sur les solutions recommandées.
- **Coordination** avec les autres entités (hors du domaine d'action) : opérateurs et fournisseurs d'accès à Internet, CERT nationaux et internationaux.

MERCI DE VOTRE ATTENTION