IT Hygiene Assessment

Cockpit 360°

10-12-2019

Trusted partner for your **Digital Journey**

IT Hygiene Assessment

WITH OUR TECH.PARTNER TANIUM

IS Hygiene Assessment

What is at stake ?

IT organizations operate in a world of growing complexity

Distribution, Scale, & Variety

Threats & Disruptions

Compliance Regulations

Challenge #1

To be able to quickly & effortlessly produce, at a given time, an IS security statement regardless of the type of asset considered : workplace, server, cloud,…

What Atos delivers

A fast and equipped technical assessment on 16 operational indicators

(of 5 different IT domains)

+

3 months of use of the deployed tool (with no limitation in terms of # of covered assets)

IT Hygiene Assessment

Service objectives

- **Service objectives**
  - Quick Assessment focused on IT hygiene
  - Technical solution (tool) is included during the service (around 3 months)
  - <u>Data remains on premises / No data outsourcing</u>
- **Expected outcomes :**
  - **« Security health check » report : 16 KPI (+custom KPIs if needed)**
  - **Global overview of the IT system (workplace, servers, IaaS)**
    - Give you an idea of what could be a Security/Ops *tower control*
    - Reinforced visibility (especially regarding the shadow IT)
  - **The best way to challenge existing reports/dashboards** (CMDB/supervision/audits/vuln.checks…)

3 months

16+

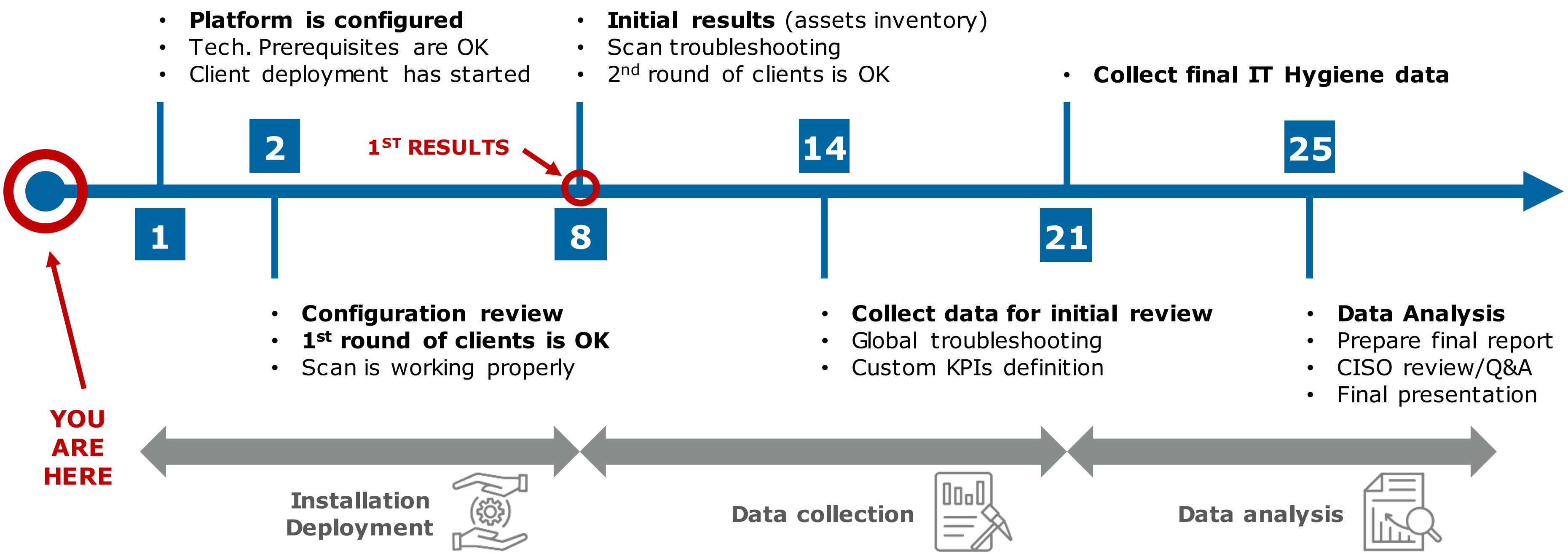
KPIs

1 report

Full Scope	Representative scope (~30%)
1 month of installation/deployment	1 week of installation/deployment
2 weeks of data collection	2 weeks of data collection
1 week of data analysis	1 week of data analysis

Assessment timeline

Main project milestones



- **Platform is configured**
- Tech. Prerequisites are OK
- Client deployment has started

- **Configuration review**
- **1st round of clients is OK**
- Scan is working properly

- **Initial results** (assets inventory)
- Scan troubleshooting
- 2nd round of clients is OK

- **Collect data for initial review**
- Global troubleshooting
- Custom KPIs definition

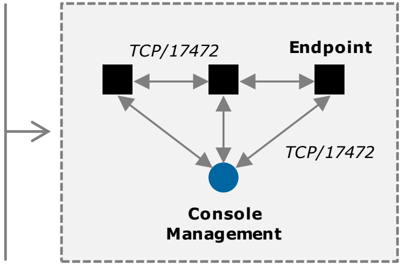
- **Collect final IT Hygiene data**

- **Data Analysis**
- Prepare final report
- CISO review/Q&A
- Final presentation

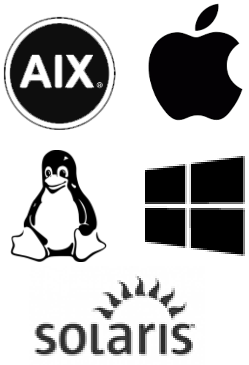
IT Hygiene Assessment

Technical & organizational prerequisites

- **Technical requirements :**
  - The deployment of a **virtual appliance** for the management (aaS is also possible AWS/Azure)
  - The deployment of a **software agent** on endpoints (workplace/server)
    - By existing software management system (SCCM, Puppet, Satellite,…), GPO or Tanium solution (CDT)
    - Configuration of HIPS, AV exclusions
    - **No reboot is required**
  - Flows opening :
    - *Clients to Management server: TCP/17472*
    - *Clients to Clients: TCP/17472*
    - *Admin/CISO/Ops to Console : TCP/443*



- **Organizational requirements**
  - To identify a customer sponsor
  - To identify a customer technical lead



Supported systems

IT Hygiene Assessment

Metrics collection / 1st analysis

- **Objectives:**
  - Leverage the platform's capabilities to produce KPIs
  - 1st "hot" analysis to identify additional KPIs

Tailor-made

Specific/Custom KPIs

- Identified during design workshops
- Needed to get more details on Core KPIs

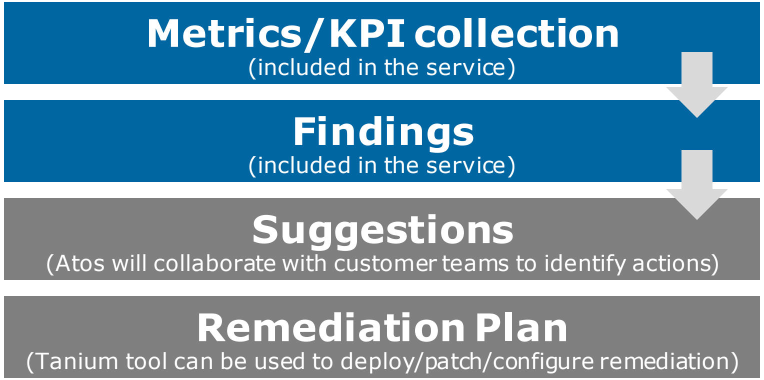
Core KPIs

Asset Discovery - Historic	Missing Critical/Important Patches per Year
Physical / Virtual Infrastructure breakdown	Workstations Missing Critical / Important Patches
Operating System breakdown	Workstations Missing Critical / Important Patches – Historic
Vulnerability Age by Year	Servers Missing Critical/ Important Patches
Vulnerability Count by Severity	Servers Missing Critical / Important Patches - Historic
Vulnerability Breakdown by Operating System	Software Update Eligible by OS
Workstations with Outdated High Severity Vulnerabilities	Workstation Software Update Eligible – Historic
Servers with Outdated High Severity Vulnerabilities	Server Software Update Eligible – Historic

IT Hygiene Assessment

Metrics collection / 1st analysis

- **KPI production & Analysis**
  - Findings Ops
  - Findings Security
  - Findings Shadow IT

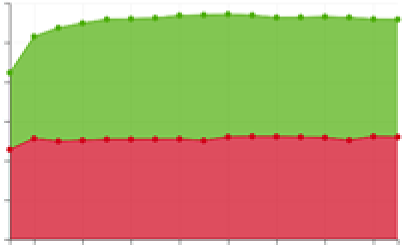


Metrics/KPI collection
(included in the service)

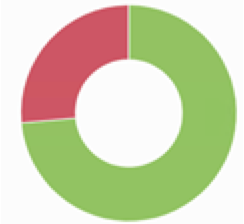
Findings
(included in the service)

Suggestions
(Atos will collaborate with customer teams to identify actions)

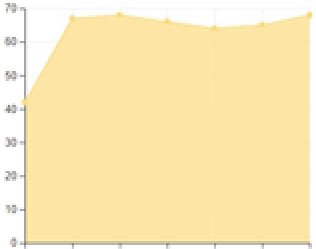
Remediation Plan
(Tanium tool can be used to deploy/patch/configure remediation)



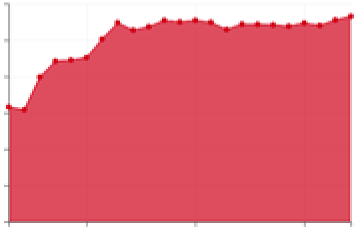
The constant trend of machines that are online and for which Windows is waiting for a reboot to perform an action



How Windows endpoints are currently patched regarding critical security patches released at least 90 days ago



How many users that are primary users of their computers, have been set administrators of it directly



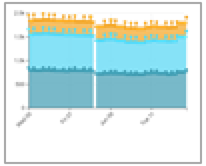
Online computers everyday on corporate network but that do not run any AV software part of our list

Dashboard example 1/2

To be completed with specific/on-demand KPIs

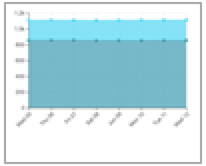
Asset Discovery

Asset Discovery - Historic

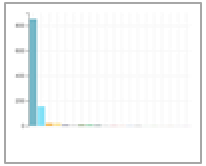


Asset Inventory

Physical/Virtual Infrastructure breakdown

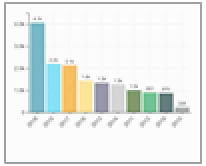


Operating System breakdown

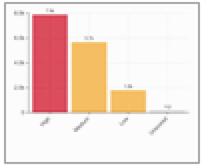


Vulnerability management

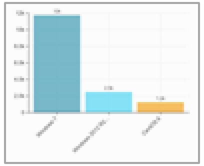
Vulnerabilities identified by year



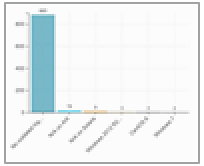
Vulnerabilities identified by severity



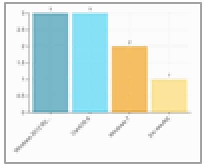
Vulnerabilities identified by OS



High Severity Vulnerabilities on Workstations

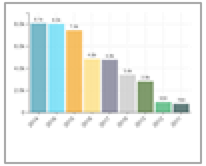


High Severity Vulnerabilities on Servers

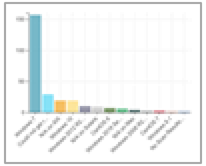


Patch management

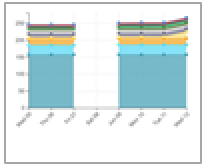
Missing Critical Patches identified by year



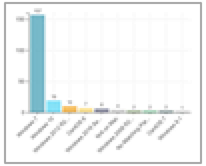
Workstations Missing Critical Patches



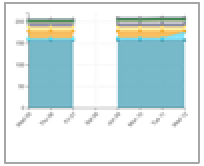
Workstations Missing Critical Patches - Historic



Servers Missing Critical Patches

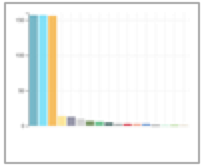


Servers Missing Critical Patches - Historic

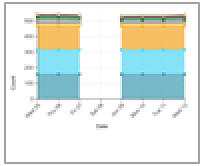


Software distribution

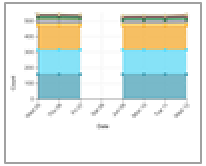
Software Update Eligible by OS



Workstation Software Update Eligible - Historic

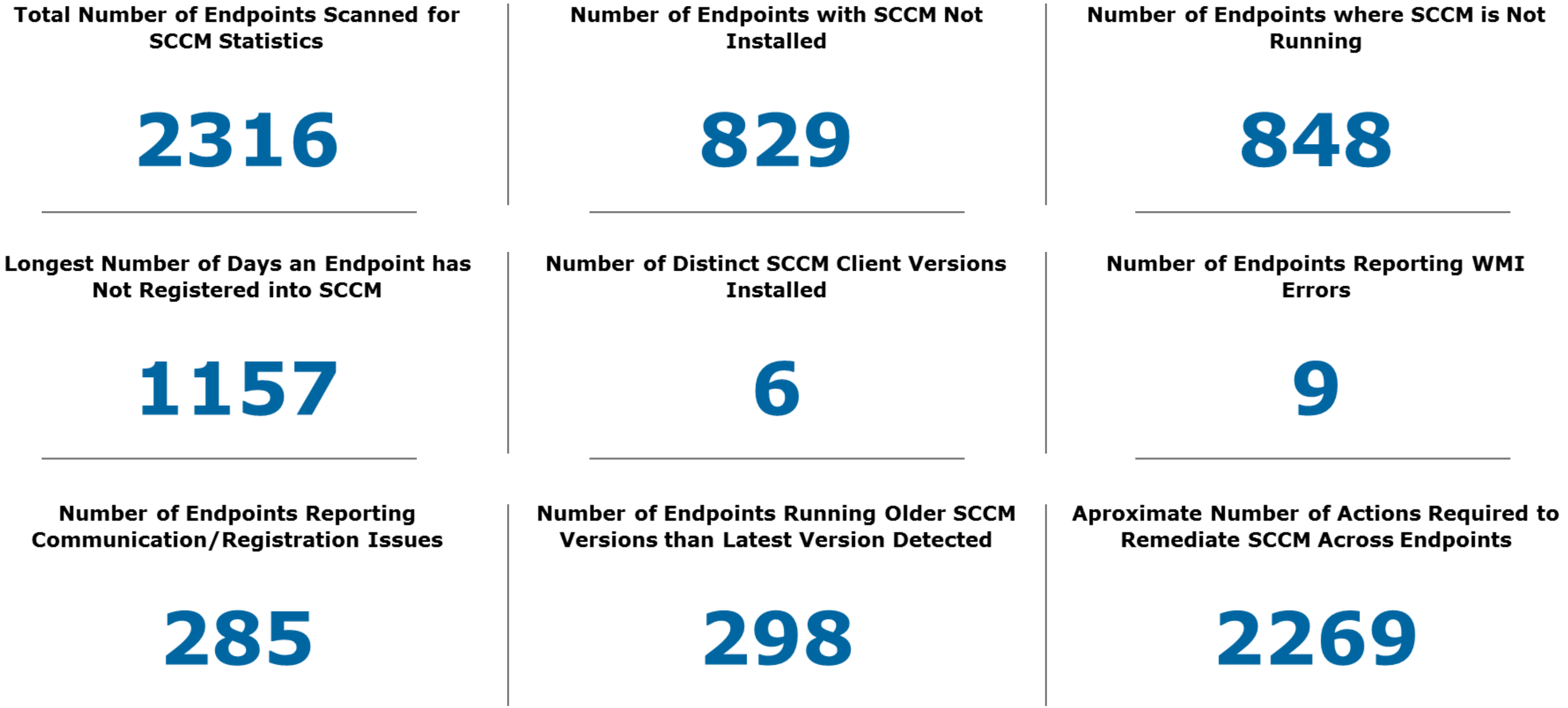


Server Software Update Eligible - Historic



Dashboard example 2/2

Zoom on SCCM statistics



Total Number of Endpoints Scanned for SCCM Statistics

2316

Number of Endpoints with SCCM Not Installed

829

Number of Endpoints where SCCM is Not Running

848

Longest Number of Days an Endpoint has Not Registered into SCCM

1157

Number of Distinct SCCM Client Versions Installed

6

Number of Endpoints Reporting WMI Errors

9

Number of Endpoints Reporting Communication/Registration Issues

285

Number of Endpoints Running Older SCCM Versions than Latest Version Detected

298

Aproximate Number of Actions Required to Remediate SCCM Across Endpoints

2269

IT Hygiene Assessment

Team & Price

- **Atos / Tanium team**
  - **1 Project Manager** (Atos)
  - **1 Security Architect** (Atos)
  - **1 Technical Expert** (Tanium)

- **Customer team**
  - **1 Sponsor**
  - **1 Architect/Technical lead**

- **Service scope**
  - Briefing / Kick-Off / Tech. Prerequisites
  - Platform setup / Endpoint agent deployment
  - Troubleshooting / 1st level of assessment / Custom KPIs
  - Data collection / Data analysis
  - High-level reporting + Details about metrics/findings

- **Service price**

Full scope	Representative scope (~30%)
21 000 € HT	**13 200 € HT**

Atos Cybersecurity

Atos Cybersecurity

Cybersecurity: Products & Services

Qualification/Certification ANSSI

PRODUCTS

Trustway

- Data security : **DataProtect**
- Secure smartphone : **HooX**
- Secure communications : **Chronos / TVPN**
- Hardware Security Module (HSM) : **Proteccio**

Evidian

- IAM : **Identity & Access Manager**
- Unified Authentication : **Authentication Manager**
- SSO : **Enterprise SSO**
- Access Federation : **Web Access Manager**

Horus

- **CardOS**
- PKI Infrastructures : **MetaPKI**
- Trusted services : **MetaSign/MetaTime/VericCert**

SERVICES

Consulting & Audits

- Consulting : **Strategy / Risks / Audit**
- Compliance : **EU-FR / ISO / ANSSI / Approval**
- Audits : **Compliance / Tech. PenTests / PASSI**

Integration & Expertise

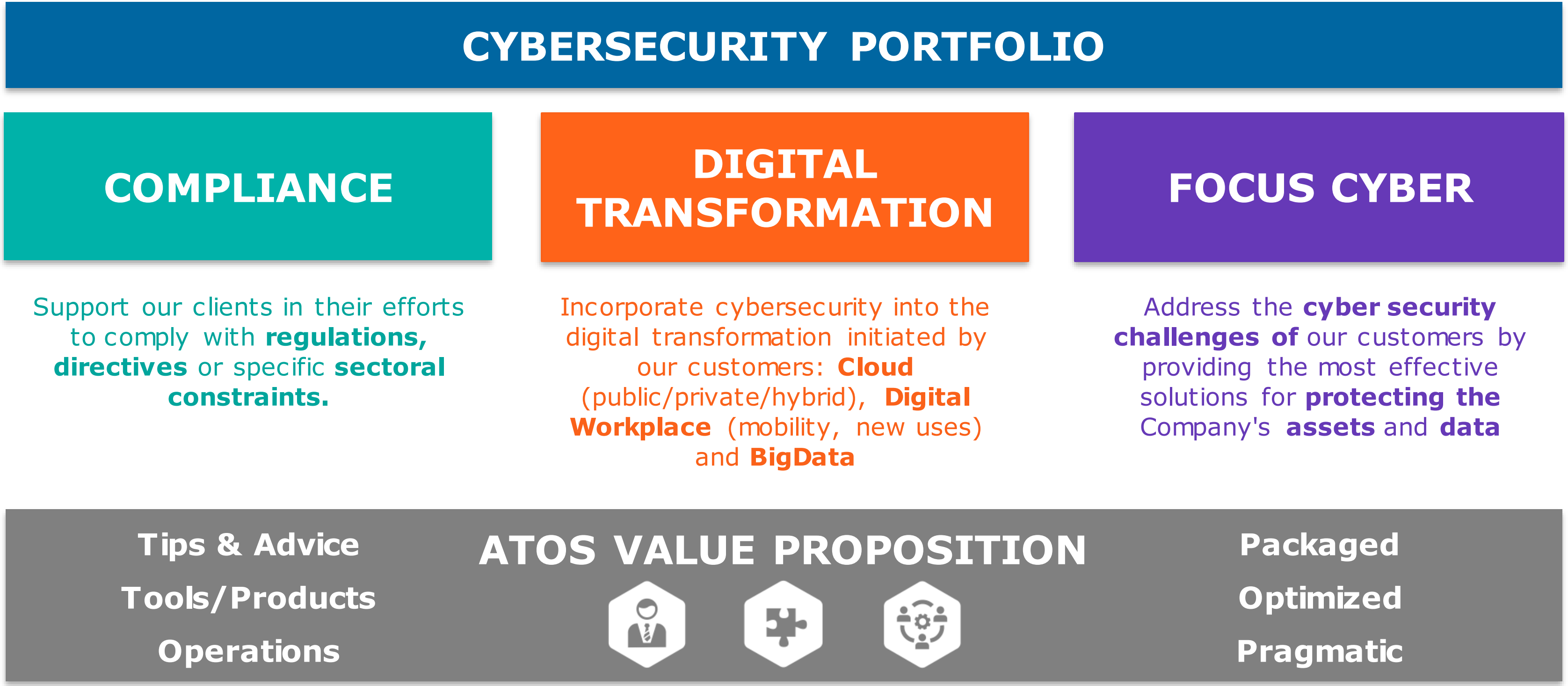
- Study & Design : **Design / Technical specifications**
- Integration : **DataCenter / Perimeter Security**
- Integration : **Endpoint Security (including Mobility)**
- Integration : **Data security & activities**

Managed Services

- Operations : **Internal/External/Hybrid**
- Specific : **On-call & Secure Sites**
- SOC : **SIEM / SOC PDIS aaS / MSSP / CSIRT**

Cybersecurity offers in France

A portfolio of offers structured into 3 families



CYBERSECURITY PORTFOLIO

COMPLIANCE

Support our clients in their efforts to comply with **regulations, directives** or specific **sectoral constraints.**

DIGITAL TRANSFORMATION

Incorporate cybersecurity into the digital transformation initiated by our customers: **Cloud** (public/private/hybrid), **Digital Workplace** (mobility, new uses) and **BigData**

FOCUS CYBER

Address the **cyber security challenges of** our customers by providing the most effective solutions for **protecting the** Company's **assets** and **data**

Tips & Advice

Tools/Products

Operations

ATOS VALUE PROPOSITION

Packaged

Optimized

Pragmatic

Cybersecurity offers in France

9 packaged offers responding to cybersecurity challenges 2018/2019

COMPLIANCE	DIGITAL TRANSFORMATION	FOCUS CYBER
GDPR / RGPD A tool-based process focused on **initialization and governance** (RT, DPIA) and on the control of **unstructured data**	**SECURED DIGITAL WORKPLACE** Securing the **new generation workstation** by adopting the **data-centric** approach	**ACCESS & DATA PROTECTION** **Governance** and **tools** for **classification** and data **protection** in all its forms.
LPM Services and technologies around **5 regulatory projects**: governance, architecture, access, administration and operations	**TRUSTED HYBRID CLOUD** Enhancing **security of cloud services** through a **risk** and **trust** driven approach	**ENDPOINT RESILIENCE** **Reinforcement of** workstation, mobile or server **protection against new threats**
NIS In search of the **compliance / business tradeoff** for SIE: governance, architecture, access, administration and operations	**SECURITY 4 CODEX** **Securing BigData capacities** (processing and storage) without affecting **system performance**	**COCKPIT 360°** **Recover control of your assets** through IS **observation** and **orchestration / automation of security services**

Atos Cybersecurity

Consulting/Audits Services & Projects

ISMS Consulting
Strategy & Organization
ISS support

Conformity
ISO & ANSSI standards
Regulations & Certification

Audits
Architecture/Code/Config.
Pen Tests/Vulnerabilities

Studies / Design
ISS architecture
Technological transition

Digital identities
Identity governance
Identity management & access
Single Sign On

Protection against PTAs
Forensic & Scan Agent
Sandboxing (host/net)

Perimeter protections
Firewall / Firewall NG
Web Application Firewall

Workstation
Antivirus / HIPS
Surface encryption
Hardening of the OS

Mobility
Mobile Device Management
Threat prevention

Perimeter protections
Anti-DoS, Anti-DDoS
Load Balancer NG
Proxy, Reverse Proxy

Flow decontamination
Email Antivirus
Anti-spam/Anti-malware
Signature/Encryption

Data protection
Data Leak Protection (DLP)
Manual classification
Data access control

Perimeter protections
VPN Gateway
Enhanced authentication
Administration bastion

SIEM
Concentration / Filters
Event correlation
SOCaaS base

Internal protection
Vulnerability scanning
Network partitioning
Securing virtual DCs

McAfee
ForeScout
DIGITAL GUARDIAN Formerly VERDASYS
WALLIX TRACE, AUDIT & TRUST
CROWDSTRIKE
paloalto NETWORKS
EGERIE SOFTWARE
gemalto security to be free
STORMSHIELD
SKYBOX SECURITY
VARONIS
TANIUM
RSA SECURITY
vmware
radware
CYBERARK

Thank you

For more information, please contact

Jean-Baptiste Voron
CTO Cybersecurity Atos France
M+ 33 6 72753597
jean-baptiste.voron@atos.net