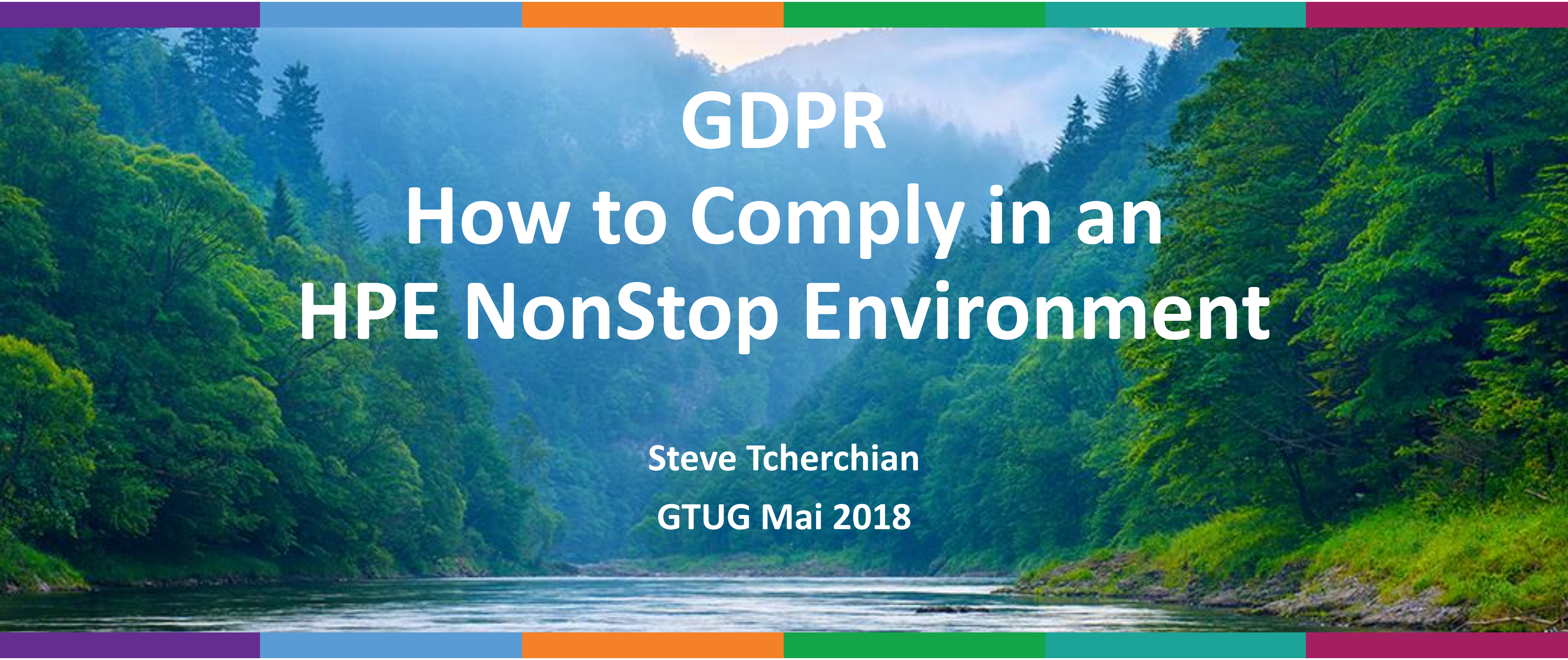


GDPR
How to Comply in an HPE NonStop Environment

Steve Tcherchian

GTUG Mai 2018

XYPRO®

Agenda

- About XYPRO
- What is GDPR
- Data Definitions
- Addressing GDPR Compliance on the HPE NonStop

About XYPRO

Inc. Magazine 2017 Award for Best Workplaces

- Solutions and expertise in NonStop cyber security, compliance, and database management
- XYGATE security solution suite
- Merlon NonStop database management solutions
- Background
    - Founded in 1983 and based in California, USA
    - Over 100 employees around the world
    - Globally-based sales, support and services
    - Strong partnership with HPE
    - Acquired Merlon Software in March 2017

XYPRO Technology Corporation
HP NonStop Server Security
A Practical Handbook
Securing the HP Non Stop Server in the Open Systems World

2013 HP AllianceOne Partner of the Year

Security Category

XYGATE and Merlon Solutions

Comprehensive NonStop security and database management

Security Intelligence

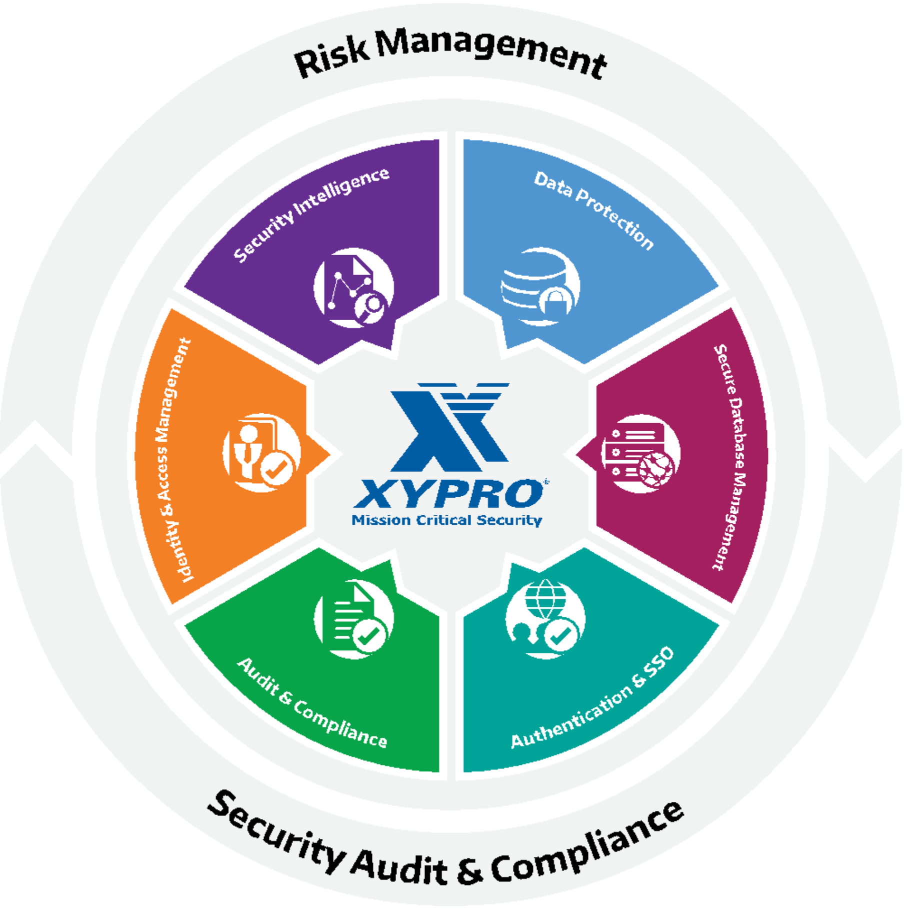
Reduce Mean Time to Detection

Identity & Access Management

Manage Access to Information

Audit & Compliance

Leverage Audit Data



Risk Management
Security Intelligence
Data Protection
Secure Database Management
Authentication & SSO
Audit & Compliance
Identity & Access Management
XYPRO
Mission Critical Security
Security Audit & Compliance

Data Protection

Protect Your Data

Secure Database Management

Manage Data Effectively

Authentication & SSO

Authenticate Securely

Disclaimer

This presentation is a commentary on the GDPR, as XYPRO interprets it, as of the date of publication. We've spent a lot of time with GDPR and have been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well prescribed.

As a result, this presentation is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

XYPRO MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN PRESENTATION.

What is GDPR?

GDPR enforcement begins 25 May 2018

- General Data Protection Regulation
- European Union’s new Data Protection Law
- Replaces the Data Protection Directive

GDPR gives individuals greater control over their personal data and imposes many new obligations on organizations that collect, handle, or analyze personal data. The GDPR also gives national regulators new powers to impose significant fines on organizations that breach the law.

Introduction to GDPR

GDPR enforcement begins 25 May 2018

- Tough Penalties - Fines up to 4% of global turnover
- Applies to EU and non-EU companies that collect and process personal data of subjects in the EU
- Breach notification within 72 hours
- Privacy by Design
- Right to be Forgotten, Data Portability
- Mandatory Data Protection Officers
- GDPR is NOT a directive. It will supersede national laws

© POST TYPOGRAPHY ← PLEASE CREDIT AND LINK TO → POSTTYPOGRAPHY.COM

GDPR Personal Data Definition

GDPR enforcement begins 25 May 2018

“…any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier”

Examples

- Name
- Identification Number (e.g. SSN)
- Location Data
- Online Identifiers
- Genetic Data
- Biometric Data

GDPR Data Definitions

GDPR enforcement begins 25 May 2018

Controller: a body which determines the purposes and means of the processing of personal data;

Processor: a body which processes personal data on behalf of the controller.

Processing: any set of operations which is performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information

Filing system: any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

GDPR Key Principles

GDPR enforcement begins 25 May 2018

- Transparency, fairness and lawfulness
- Limiting the processing of data to specified, explicit and legitimate purposes
- Minimizing the collection of data
- Ensuring accuracy
- Enabling data to be erased
- Limit the storage of data

Current state of cyber security

Mandiant M-Trends 2017 Report

99+
Days

For organizations to discover a compromise

47%

Of organizations learn about breach from an external entity

84%

Of successful breaches compromise app vulnerabilities

100%

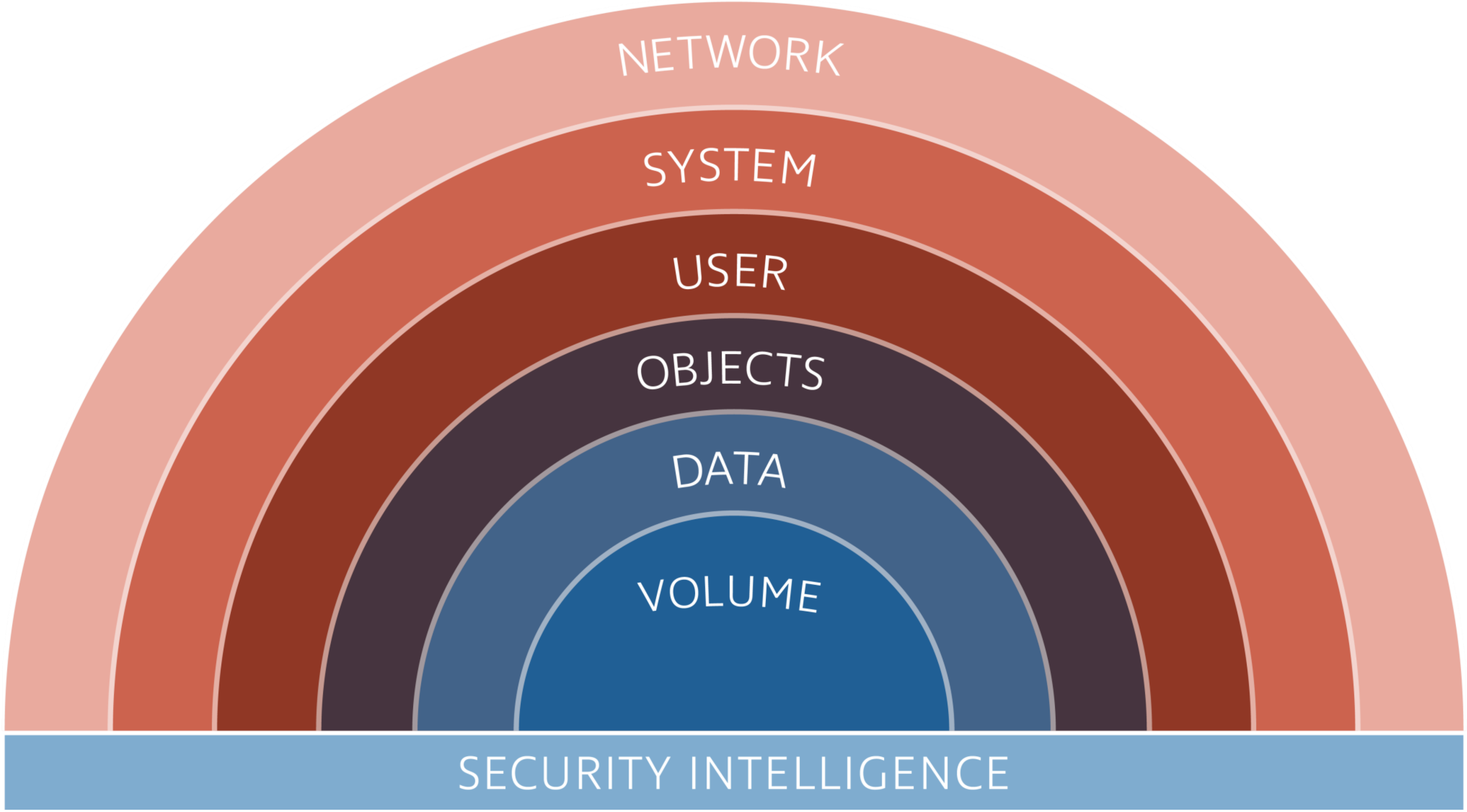
Had Firewalls, IPS, SIEMs and other solutions deployed in their environment

Identifying threats is harder than ever

Cyber security needs to adapt

- Attacker objectives and methods have changed
  - Focusing on theft of user credentials
  - Hackers spending 90% of their time on reconnaissance
  - Using “low and slow” techniques
- Cyber crime affects every industry, every platform
- Attacks are coming from all sides
- Increase in data, connectivity and globalization

NonStop Security Layers



Article 32

Article 32 of the GDPR states *"the data controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk"*. Further, Article 32 requires *"the data controller or data processor must take steps to ensure that any natural person with access to personal data does not process the data except on instruction of the controller, processor, European Union law, or member state law"*.

This means ensuring proper **authentication, access control**, and **identity management** are in place to ensure a level of security appropriate to the risk.

Authentication and Access Control

Authentication & SSO

- XYGATE User Authentication (XUA)
  - Flexible authentication processes
  - Multi-factor authentication
    - Note increased requirement with PCI 3.2
  - Single sign-on
  - LDAP and Active Directory support
  - Support for RSA SecurID and RADIUS

Identity & Access Management

- XYGATE Access Control (XAC)
  - Individual accountability
  - Role-based access control
  - Granular access control
  - Keystroke logging
  - Audit privileged user activity

Article 32 continued

Article 32 also references Security of processing: *"The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including… the pseudonymization and encryption of personal data;"*

This boils down to **encryption and masking of personal data.** Encryption is supported on the HPE NonStop at most layers – from network to data. Article 32 requires processors working with EU citizens' personal data to use it.

Article 33

Article 33 requires prompt breach notification: *“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.”*

Records of all activity that touch that data need to be collected and organized to make it possible to detect and report on all unauthorized access. For NonStop systems, this means **audit everything associated with GDPR-defined personal data** – or as much possible to address the risk.

Auditing and Alerting

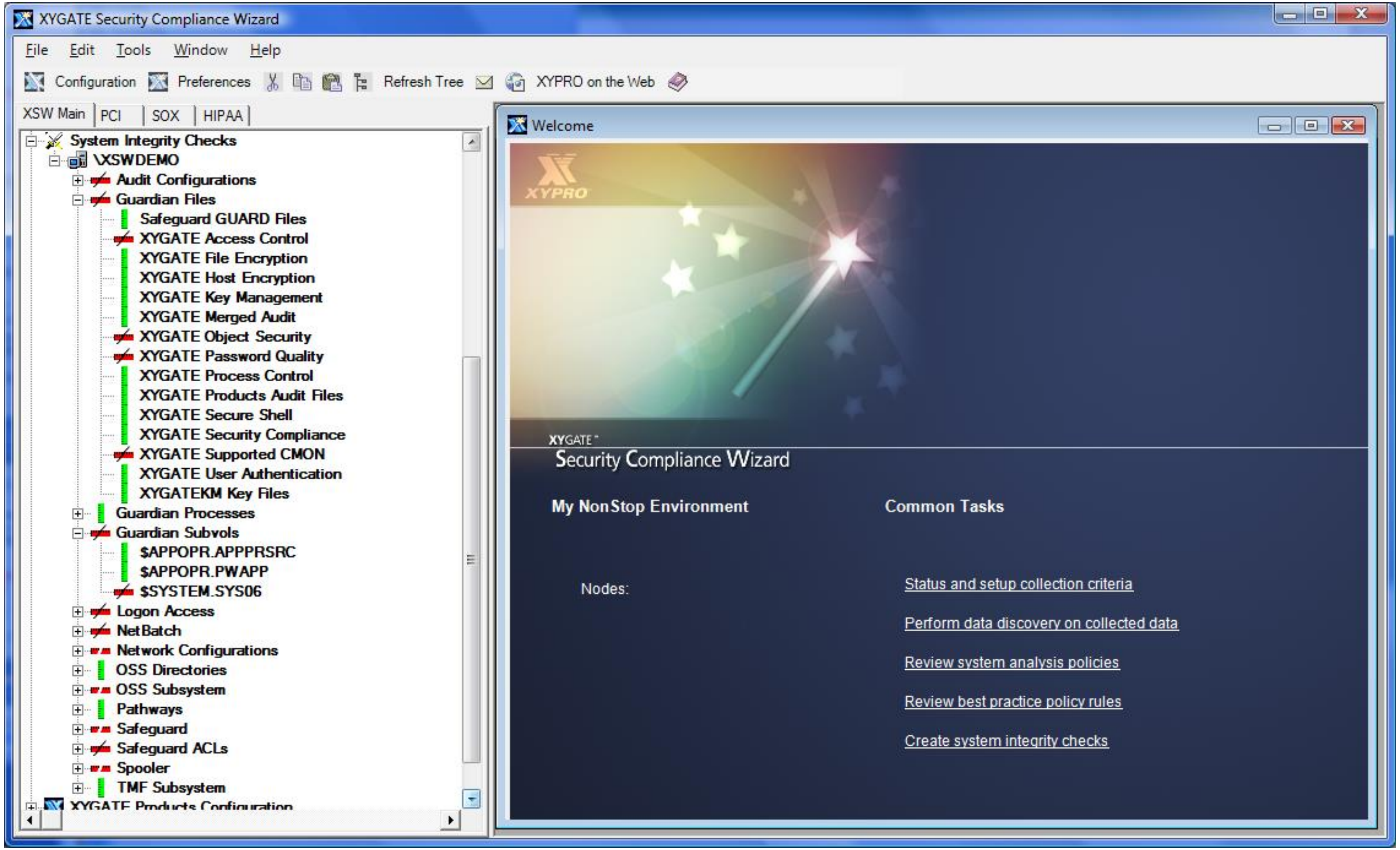
Audit & Compliance

- XYGATE Merged Audit (XMA)
  - Single repository for audit data
  - Audit and compliance reports
  - Integration with SIEMs
  - Plugins for BASE24 and BASE24-eps

Audit & Compliance

- XYGATE Compliance PRO (XSW)
  - PCI DSS, best practices, industry regulations and company policy
  - Integrated compliance and analysis
  - File and system integrity checks
  - PCI reporting

Monitoring with Compliance PRO



- System Integrity Checks
  - \XSWDEMO
    - Audit Configurations
    - Guardian Files
      - Safeguard GUARD Files
      - XYGATE Access Control
      - XYGATE File Encryption
      - XYGATE Host Encryption
      - XYGATE Key Management
      - XYGATE Merged Audit
      - XYGATE Object Security
      - XYGATE Password Quality
      - XYGATE Process Control
      - XYGATE Products Audit Files
      - XYGATE Secure Shell
      - XYGATE Security Compliance
      - XYGATE Supported CMON
      - XYGATE User Authentication
      - XYGATEKM Key Files
    - Guardian Processes
    - Guardian Subvols
      - $APPOPR.APPPRSRC
      - $APPOPR.PWAPP
      - $SYSTEM.SYS06
    - Logon Access
    - NetBatch
    - Network Configurations
    - OSS Directories
    - OSS Subsystem
    - Pathways
    - Safeguard
    - Safeguard ACLs
    - Spooler
    - TMF Subsystem
- XYGATE Products Configuration

My NonStop Environment

Nodes:

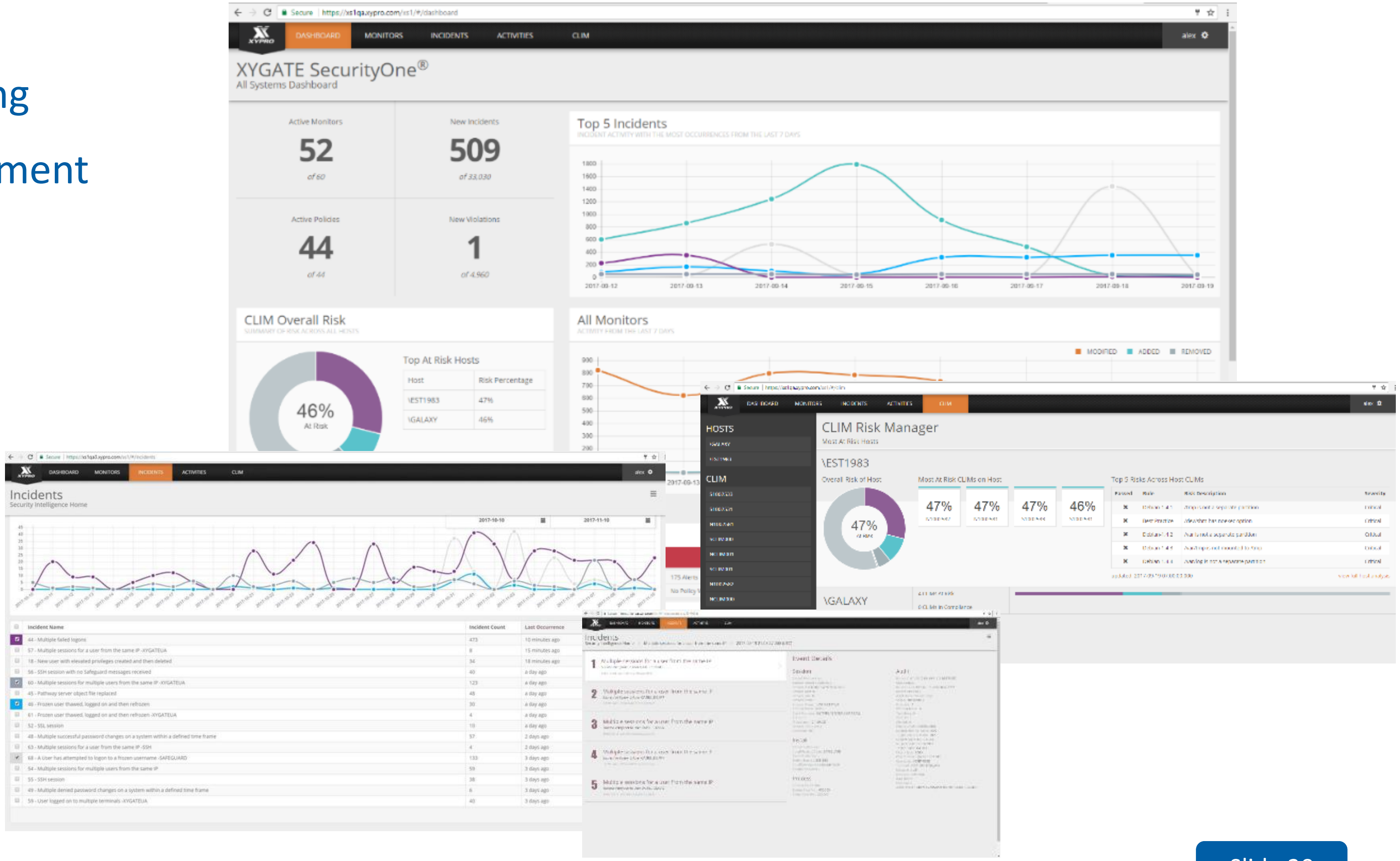
Common Tasks

- Status and setup collection criteria
- Perform data discovery on collected data
- Review system analysis policies
- Review best practice policy rules
- Create system integrity checks

XYGATE SecurityOne (XS1)

Security intelligence and analytics

- Unified dashboard
- Intelligent integrity monitoring
- Compliance and risk management
- Machine learning
- Anomaly detection
- Correlation and context
- CLIM Risk Manager



☐	Incident Name	Incident Count	Last Occurrence
☑	44 - Multiple failed logons	473	10 minutes ago
☐	57 - Multiple sessions for a user from the same IP -XYGATEUA	8	15 minutes ago
☐	18 - New user with elevated privileges created and then deleted	34	18 minutes ago
☐	56 - SSH session with no Safeguard messages received	40	a day ago
☑	60 - Multiple sessions for multiple users from the same IP -XYGATEUA	123	a day ago
☐	45 - Pathway server object file replaced	48	a day ago
☑	46 - Frozen user thawed, logged on and then refrozen	30	a day ago
☐	61 - Frozen user thawed, logged on and then refrozen -XYGATEUA	4	a day ago
☐	52 - SSL session	10	a day ago
☐	48 - Multiple successful password changes on a system within a defined time frame	57	2 days ago
☐	63 - Multiple sessions for a user from the same IP -SSH	4	2 days ago
☑	68 - A User has attempted to logon to a frozen username -SAFEGUARD	133	3 days ago
☐	54 - Multiple sessions for multiple users from the same IP	59	3 days ago
☐	55 - SSH session	38	3 days ago
☐	49 - Multiple denied password changes on a system within a defined time frame	6	3 days ago
☐	59 - User logged on to multiple terminals -XYGATEUA	40	3 days ago

GDPR Compliance on HPE NonStop

- Understand your current data processing activities
- Assess your current compliance and identify gaps
- Prioritize remediation actions based on risk and resources
- Implement an actions plan
- Let XYPRO help

XYPRO®

merlon software corporation
a XYPRO company

Thank You!

@SteveTcherchian
steve@xypro.com