Revvelium. 12.3

CHANGE LOG

DATA ANALYTICS

4 MONTHS **80** USER-STORIES **41** BUGS **38** TECHNICAL TASKS

FEATURES (user-story)

Platform-wide usability enhancements

- Globally toggleable tooltips on the platform

Enhanced *alerts* management and UI improvements

- Filter with logical operators and persistence across pages
- UI overhaul of the ALERT MAPPING section

Improved *administration* features

- Dynamic group management (CRUD)

Streamlined *log collection* management

- Log source search and short table
- Removing mandatory fields when performing CRUD on a log source

New *SLA* Metrics and SOC KPIs

- New SLA (MTTD, MTTR, MTTT + SOC Manager KPIs)

New *Log loss detection* enhancements

Partner email template improvements

New *threat* management enhancements

- Mitre Att&ck Framework Table : tactics / techniques
- Filter using logical operators and restrict access by type
- Expandable list of threats
- Threat name editing
- Addition of an informational tutorial on the Mire (existing in V11)
- UX improvement of the TASK creation pop-up
- Polling improvement (no more manual refresh needed for notifications)

Advanced *SIEM rules* capabilities

- Rules import & testing
- Manage exceptions (whitelist) directly from the graphical interface
- Configuration options (threshold, severity score, TLP, PAP, etc.)
- Modification timeline for rules (who, what, when?)
- Enable/disable one or multiple rules (ON/OFF)
- Mitre attack coverage for each rule

SOAR innovations and integrations

- REV Copilot N1 (LLM)
- ITSM Interco

Other Technical Enhancements

- SOC report automation (API Metrics)

Improved deployment scripts

Switch to a new repository for COMMON rules

Updated *user documentation*

LEGEND IMPROVED 12.4 ISSUE 12.2 IMPRVNT PARTNER API ROUTE ACCOMPAGNEMENT & CONFORT

ITRUST.