SecOps SPL - Functional diagram

SecOps SPL

Administration

Security Architects here define company's Monitoring Targets and relate these to MITRE ATT@CK, BAIT, KAIT etc.
Admin :: Monitoring Targets

Security Architects or CTA/SOC Analysts here define the conditions for alerts to get closed automatically.
Admin :: Auto-close Setting

Security Architects or CTA/SOC Analysts here define the conditions for alerts to be grouped to cases automatically.
Auto-grouping Settings

Security Architects or Risk Managers use this to administer the rules for automated UC Testing
Admin :: UC Testing Auto Replay Settings

This dialogue allows Security Architects to assign Use Cases to tenants and stages
Admin :: Alert states and staging

Security Architects or CTA/SOC Analysts assign Monitoring Targets, edit descriptions, enable / disable Use Cases or set new cron schedules
UC Factory :: Use Case Library

Health

Check indexes and sourcetypes for delayed/future events watch for missing important devices.
Health :: Data Integrity & Quality

Visualise runs and skips of Scheduled Searches, re-schedule, activate or deactivate if necessary.
Health :: Scheduled Searches and Distribution of start times

SOC

SOC Analysts work with Notables here
SOC :: Open Alerts Overview

SOC Analysts enter their Welcomelist Requests here.
SOC :: Welcomelisting Request Editor

Use Case Factory

Developers assign Monitoring Targets or edit descriptions
UC Factory :: Use Case Library

Developers here define the test events and testing parameters for their Use Cases
UC Factory :: UC Testing Process - Definitions and Test

CTA

Visualise attacks on internet-exposed SSH ports
CTA :: Attacks on SSH

Visualise attacks on internet-exposed web-servers
CTA :: Attacks on Webserver

CTA Team analyse Incidents here
CTA :: Open Incidents Overview

New requests will be accepted / rejected by CTA members or Risk Managers.
CTA :: Welcomelisting Request and Rule Administration

GOV

Study the rulesets here without the need for another tool
GOV :: Regulatory Rulesets and relevant Frameworks

Reporting

SecOps Basics

An overview of all indexes and sourcetypes used by your organisation
Report :: SecOps Indexes and Sourcetypes

Monitoring Targets

Learn about the Monitoring Targets defined in your company and how they are related to MITRE ATT@CK, BAIT, KAIT etc.
Report :: Monitoring Targets

Learn which UCs exist and how they are related to the Monitoring Targets defined in your company
Report :: Monitoring Targets and Use Cases

Alert Statistics

See how many alerts exist, had been closed and for which reasons by tenant and stage
Report :: Overall Alert Statisctics

An online report of all auto-closed alerts by date time, tenant, stage, reason, name and type
Report :: Auto-closed Alerts

Track the route of any alert in SecOps SPL by tenant and stage, therefore fulfilling auditor's dreams
Report :: Historical Alerts

Learn how often alerts had been triggered, separated by stage
Report :: Alert Trigger Statistics