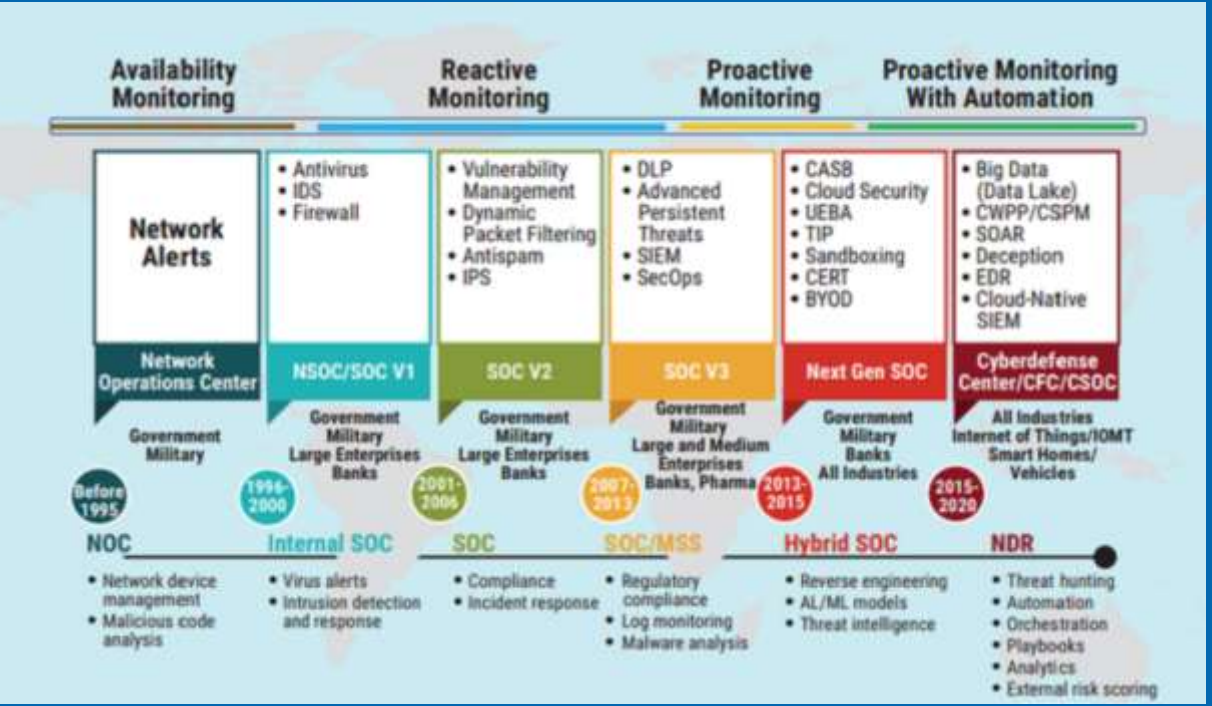
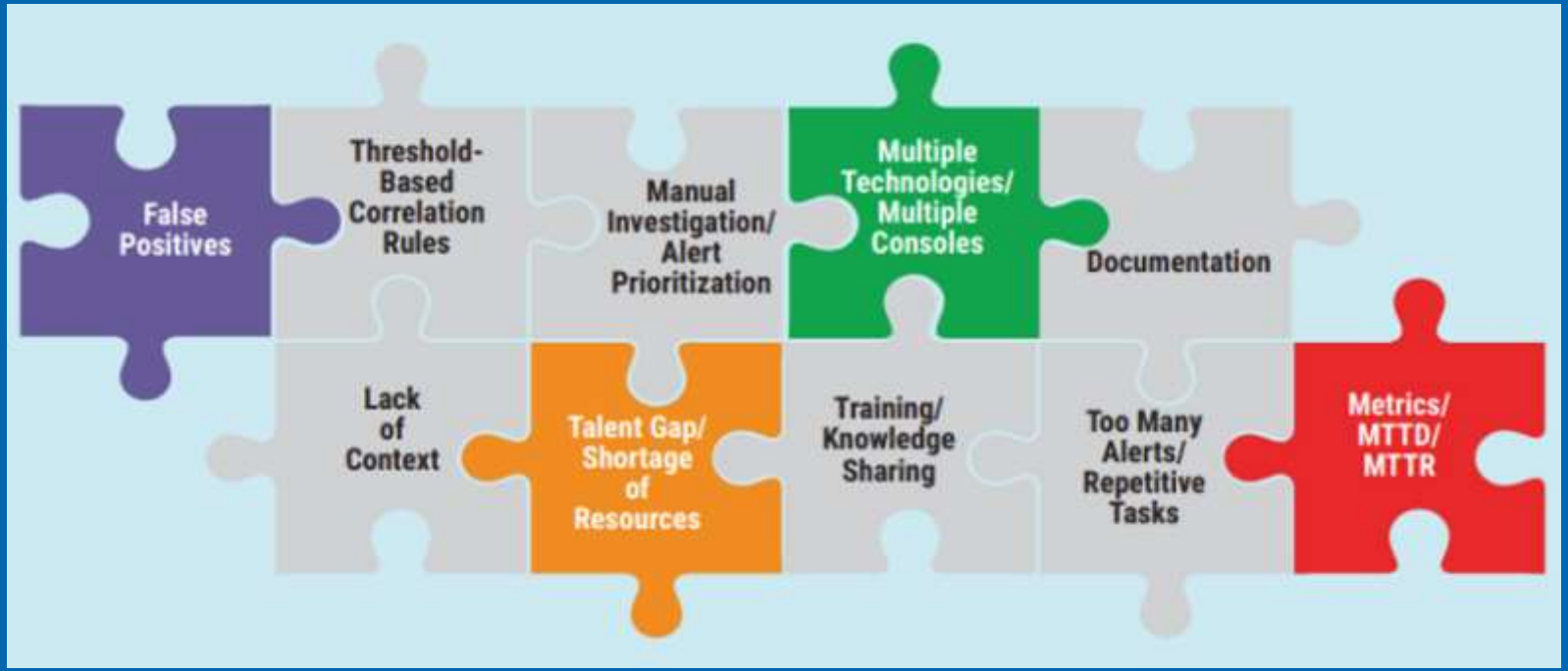

telelink
BUSINESS SERVICES
INTEGRATED CYBERSECURITY MONITORING
A PRACTICAL APPROACH

EVOLUTION OF THE SOC



Source: ISACA

SOC challenges



Platinum Business Partner IBM

telelink BUSINESS SERVICES

Source: ISACA

THE NEED FOR INTEGRATIONS

BETTER VISIBILITY

ENRICHMENT

REDUCE NUMBER OF OPEN CONSOLES

OPTIONS FOR CHANGES

IT DEPT VS. IT SECURITY MONITORING

Platinum Business Partner IBM

telelink BUSINESS SERVICES

COVERING THE NEEDS

HUGE NUMBER OF PARSERS FOR VARIOUS LOG SOURCES

UNIVERSAL PARSER/CUSTOM

THREAT INTEL INTEGRATIONS/APPs

APPS FOR INTEGRATION WITH EXTERNAL SYSTEMS

OPTIONS FOR CHANGES – APPs/SOAR

Platinum Business Partner IBM

telelink BUSINESS SERVICES

APPS FOR INTEGRATIONS

INTEGRATIONS WITH EDR

INTEGRATIONS WITH VA / VM

INTEGRATIONS WITH NDR

INTEGRATIONS WITH DAM

UBA

Platinum Business Partner IBM

telelink BUSINESS SERVICES

APPS FOR INTEGRATIONS

App exchange



Vulnerability



Endpoint



Network



User



Platinum Business Partner IBM

telelink BUSINESS SERVICES

APPS FOR INTEGRATIONS

Some of the functionalities and options

Threat Intelligence

- URL filtering and categorization
- IP reputation
- Download IOCs from collections
- Updated reference sets in near-real time
- Provides a visualized view for Advanced Threat Protection Feed by X-Force
- Option to pull in threat intelligence feeds using the open standard STIX and TAXII formats

Endpoint protections apps

- Get events and threats indicators
- See, detect, and take action upon endpoint activity from directly within the QRadar console
- Provide options to mitigate threats and to manage endpoints
- Additional dashboards and more.

Platinum Business Partner IBM

telelink BUSINESS SERVICES

APPS FOR INTEGRATIONS

Some of the functionalities and options

Vulnerability

- Provides data enrichment of Qradar offenses
- Ad-hoc scanning, and rule-based scanning
- Ingest your VM detections into Qradar\
- Visualize historical data

NDR

- Real-time, pre-correlated threat detections and host scores into the QRadar platform
- Enrich the context of real-time threat investigations.
- Pinpoint hosts with the highest risk to the network
- Visibility into threats across the kill chain

Platinum Business Partner IBM

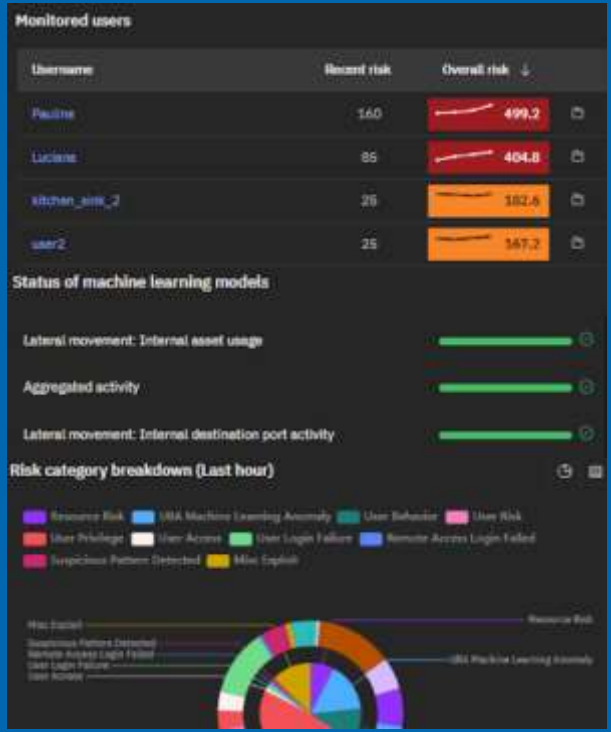
telelink BUSINESS SERVICES

APPS FOR INTEGRATIONS

Some of the functionalities and options

UBA

- Helps you to determine the risk profiles of users inside your network
- Machine Learning (ML) add-on tool
- Adding use cases that are based on custom rules
- Adding content packages
- Adding use cases for machine learning analytic
- Dashboards views



Platinum Business Partner

IBM

telelink BUSINESS SERVICES

OPTIONS FOR CHANGES AND ACTING

Reactive monitoring to Proactive Approach of Security Operations

SOAR

Acting through apps

Two-way integrations

Platinum Business Partner IBM

telelink BUSINESS SERVICES

OPTIONS FOR CHANGES AND ACTING

Reactive monitoring to Proactive Approach of Security Operations

- Manual or Automated escalation of offenses from QRadar to Resilient.
- Import of associated IOCs (IP addresses & other artifacts), plus automated updates over time.
- Quickly and easily create playbooks
- Seamlessly integrated analyst workflow speeding up investigations and response
- Reduce time to respond to and remediate

Platinum Business Partner IBM

telelink BUSINESS SERVICES

OPTIONS FOR CHANGES AND ACTING

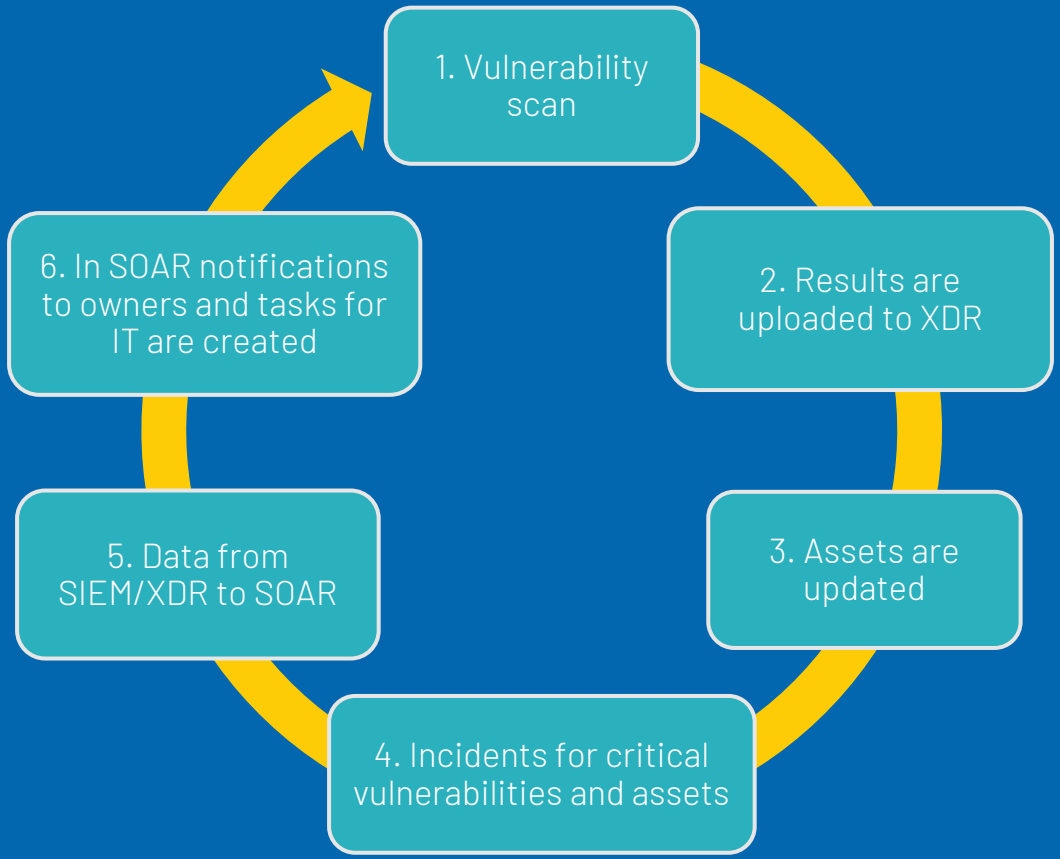
And some more…

- Assess and report on SOC performance
- Threat Intelligence feeds to automatically enrich and action Indicators of Compromise
- Bi-directional synchronization of notes and closed cases to ensure data integrity.
- The “Reference Set” functions manage and connect QRadar reference set items with Resilient incident artifacts.
- The “Search” function allows users to manually or automatically run QRadar Ariel queries directly from Resilient workflows after an incident is created.

Platinum Business Partner IBM

telelink BUSINESS SERVICES

EXAMPLE



Platinum Business Partner IBM

telelink BUSINESS SERVICES

WHAT CAN BE ACHIEVED



Unify workflows - Work without pivoting between tools

Eliminate silos - gain visibility across data sources

Automate work and go more pro-active



Disconnected tools

Poor visibility

Outdated detection

Platinum Business Partner IBM

telelink BUSINESS SERVICES


QUESTIONS &
ANSWERS
Platinum
Business
Partner
IBM
telelink
BUSINESS SERVICES


THANK YOU!
telelink
BUSINESS SERVICES