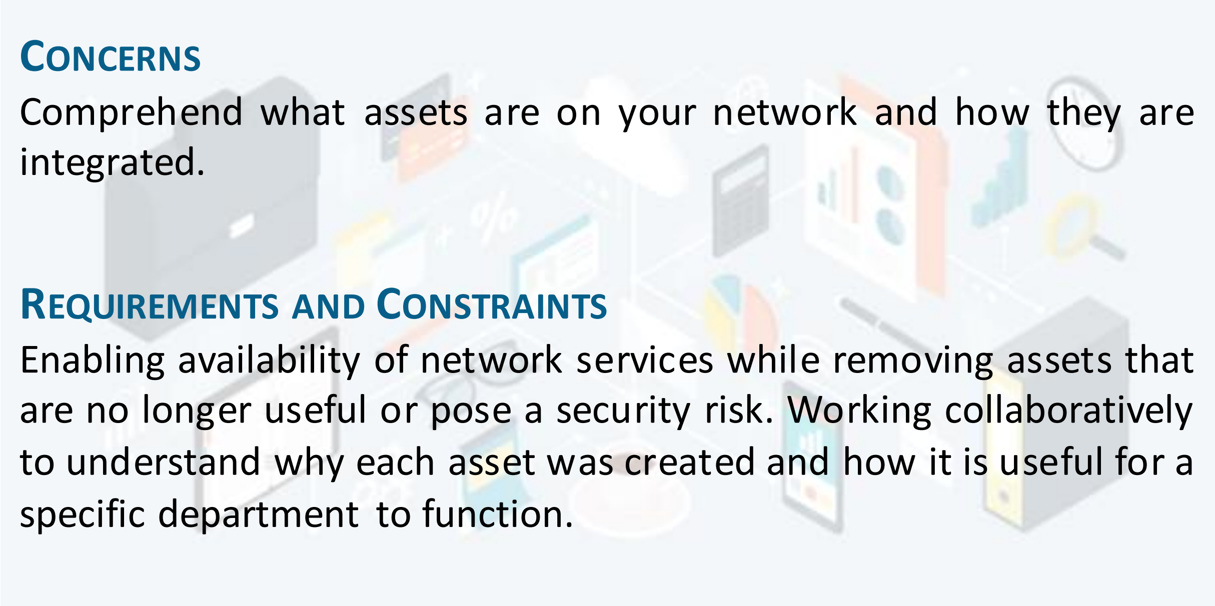
Opéra
CONSEIL

Use case Cybersecurity

Orchestrating efficiency, inspiring trust

Use case – Asset Management



Concerns

Comprehend what assets are on your network and how they are integrated.

Requirements and Constraints

Enabling availability of network services while removing assets that are no longer useful or pose a security risk. Working collaboratively to understand why each asset was created and how it is useful for a specific department to function.

Services provided

- Asset Tracking to identifying the asset, owner, and purpose.
- Assess maintenance requirements, vulnerabilities, value as a point of attack, and disposal if necessary of each asset.
- Adherence to security controls guided by industry standards such as ISO 27001
- Revise security controls to adapt to special use cases in organizational assets

What are the benefits for the organization?

Inventory of assets means that when an asset is involved in a security incident: the proper incident reporting and controls are already in place

Ownership of the assets will result in end users taking responsibility for mitigating risk and streamlining remediation

Facilitates security auditing and penetration testing during the planning phase

ISO 27001

Conform to industry security standards such as ISO 27001 to build trust with partner companies

Use case – Penetration Testing

First testing of your security should not be from a stranger !

A breach can cost millions, simulate an external attack during a penetration test to refine controls.

Steps of Penetration Testing

- Scope
- Reconnaissance
- Threat Modeling
- Exploitation
- Post Exploitation
- Analysis and Reporting

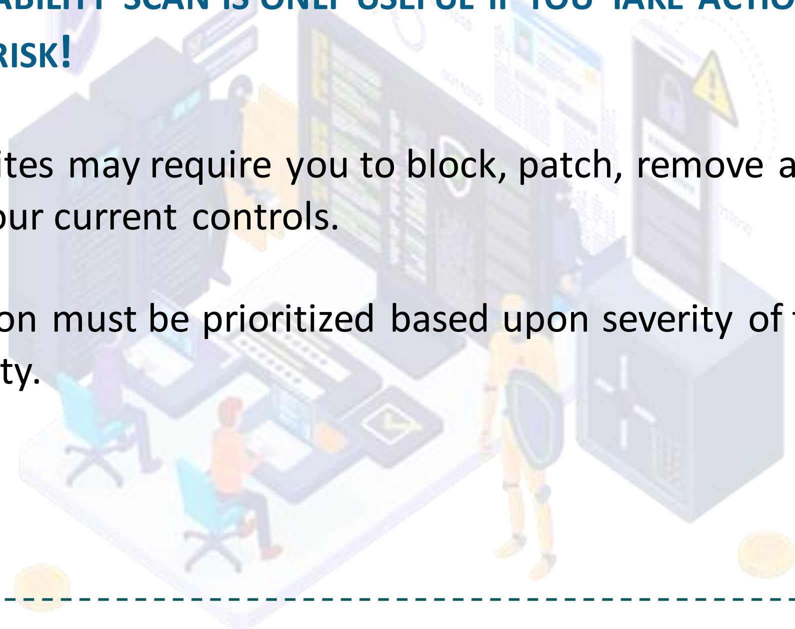
Bridge the gap between the security team and the penetration testers

- Build a scope that is both feasible to execute given the size of your organization and resources as well as effective in capturing highest priority assets.
- Manage the limitations of penetration testers to access resources while not inhibiting availability to end users
- Ensure that assets are restored to pre exploitation configurations and any vulnerabilities discovered are controlled
- Integrate entire security team to understand and communicate results of post exploitation reporting.

What are the benefits for the organization?

- Ensure vulnerabilities are identified before the next breach
- Accurately assess the value of assets to network security
- Minimize the cost of data breaches

Use case – Vulnerability Management



A vulnerability scan is only useful if you take action to mitigate risk!

Vulnerabilites may require you to block, patch, remove assets or address your current controls.

Remediation must be prioritized based upon severity of the vulnerability.

Stages of Vulnerability Management

- Identify
- Evaluate
- Remediate
- Report

Communicate a vulnerability report to enable leaders to make decisions

- Clear and concise prioritization of each vulnerability based upon the Common Vulnerability Scoring System (CVSS)
- Regular and repeated vulnerability scans using tools such as Nessus Vulnerability Scanner to conduct SCAP scans and ensure remediation is progressing as planned
- Scheduling remediation to enable end users to continue to be productive during peak hours
- Addressing and refining security controls based upon remediation efforts

What are the benefits for the organization?

- Ensure vulnerabilities are removed before the next breach
- Decrease downtime of services while maximizing security
- Documented controls based organization specific threats

Use case – Managed Detection & Response (MDR)

Concerns

Facilitate the active discovery of security incidences and executing response and reporting.

Requirements and Constraints

Providing MDR (Managed Detection and Response) through the use of XDR (Extended Detection and Response) without inhibiting the avaliability of services and operating within the resource constraints of the customer.

What are the benefits for the organization?

- Provide resources that are not organic to the organization
- Leverage AI to streamline a variety of security services
- Decrease the time the attack persists on your network

Services provided

- Assess and Refine
- Reduce the number of security tools you are forced to actively monitor, Integrate IDS/IPS with your other monitoring systems to catch suspicious traffic on Layer 2 through 7 of the OSI model
- Solve the problem of manpower and resource shortages
- Set clear and manageable goals to improve your security posture
- Regularly audit your incident reporting and response procedures
- Use AI and XDR tools to gather information in real time of potential attacks
- Use data driven by XDR to focus your teams efforts on the problem areas instead of hunting in the dark

Use case – Business Continuity Planning

Concerns

Develop Disaster Recovery Plan to restore services in the event of a data breach or complete shutdown of services

Requirements and Constraints

Building redundancy and sustainability within the confines of organizational resources

What are the benefits for the organization?

- Shorten downtime after a breach
- Reduce data loss by accessing incremental backups
- Build trust with your clients who know they will not lose access to your product in the event of a breach

Services provided

- **What is the cost if data is lost for your organization?**

The answer to this question should drive how much your organization is willing to spend to protect that data and how much it is willing to spend to build redundancy in order to maintain availability of that data.

- **What data requires restoration in the event of a data breach?**

Not all data must be restored immediately or at all. Deciding the value and prioritizing data can reduce the cost of data storage and the size of the infrastructure required to restore services.

- **What threats are realistic to your organization?**

Preparing for a tsunami when your data is stored in a desert may not be practical or useful. A DRP should be tailored to your organization’s needs.

- **How will you test your DRP?**

A regular test of your plan will ensure everyone is prepared to execute calmly during a crisis.

For any additional information on our offers

Géraldine BLED
Managing Partner / CEO
43, rue des Remparts d’Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Gsm: +33(0)6 12 04 36 01
Email :geraldine.bled@opera-conseil.com

Sébastien AKL
Director of Sales and Business Developement
43, rue des Remparts d’Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Gsm : +33(0)6 13 66 46 83
Email :sebastien.akl@opera-conseil.com

Matheus MENEZES
COO / Salesforce solution manager
43, rue des Remparts d’Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Gsm: +33 (0)6 09 06 95 54
Email :matheus.menezes-pinheiro@opera-conseil.com

Karine OUAINI
EPM/PPM solution manager
43, rue des Remparts d’Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Email :karine.ouaini@opera-conseil.com

Mathew DAVIS
Cyber Security manager
43, rue des Remparts d’Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Email :mathew .davis@opera-conseil.com