This entry covers a “real example” of the usage of Faraday to manage a cybersecurity program. A sub-set of cybersecurity processes will be described, but the tool is not only useful for those. Please, be creative and use it to cover your needs :)

Asset Management (know what we have).

Asset management is, maybe, the most critical process which you must put in place to start a cybersecurity program. Knowing which assets you have and what are their values for the business is the key principle to applying “cost-benefit” security solutions. So, you can consolidate into Faraday all your main assets, using tags or even making some kind of “asset registration” you can describe the main information for proper cybersecurity management, like:

- Asset Owner
- IT Owner
- Security Owner
- Business Involved
- SLA

Another good approach would be defining a “RACI Matrix” to know “who is who” for cybersecurity responsibilities. With this RACI you can define who’s responsible, accountable, among other roles regarding different security processes, like patch management, incident response, hardening, etc.

The “tag” feature would increase the quality of data for your assets because you could describe topics like: B2C, PCI, HIPAA, etc.

For example, you can use your vulnerability scanning tool over the most critical assets and integrate the results into Faraday. This is a good approach to know “What could happen with our most critical assets?” :)

You could read more about this in the #CISControls CSC-1, but also this process is part of ISO, NIST, PCI, DSD 35 Top Mitigation Strategies, among others references.

Note: You should define a roadmap following your cybersecurity objective. This means increasing scope based on the value of the assets and the risk exposure.

Compliance Management

Reference	Section
CIS Controls	CSC 1 - Inventory of Authorized and Unauthorized DevicesCSC 2 - Inventory of Authorized and Unauthorized Software
Australia DSD Top 35 Mitigations Strategies	Application Whitelisting
PCI-DSS	2.4 Maintain an inventory of system components that are in scope for PCI DSS
ISO 27002	8.1 Responsibility for assets
NCSC Ten Steps for Cybersecurity	Secure Configuration

Security Hardening

Another security process which you can support with Faraday is regarding “Security Hardening”, because when you know which your assets are and how they need to run, you can apply a secure configuration. Security Hardening is the process which provides good secure configuration for your asset. For this purpose you can use a lot of references, for example CIS Benchmarks, but focused on Faraday, you can use the tool to identify if your assets are following your own rules. For example:

- Are we using insecure protocols like ftp, telnet, snmp, smbv1?
- Are we using default accounts like root, sa, sys, system, admin, etc?
- Are we using this port for this service? Are we sure that we need this port open?
- Were we involved for this new service available? Is it a new platform? Which is the project ID? Do we have a change request for this?

You can even connect Faraday with your “Compliance Management Tool” to obtain results and do proper follow-up. You can also create reports about insecure services, service by server, among other security KPI.

You could read more about this in #CISControls CSC-3, but also this process is part of ISO, NIST, PCI, DSD 35 Top Mitigation Strategies, among others references.

Compliance Management

CIS Controls	CSC 3 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and ServersCSC 9 - Limitation and Control of Network Ports, Protocols, and ServicesCSC 11 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Australia DSD Top 35 Mitigations Strategies	OS HardeningAPP Hardening
PCI-DSS	2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards2.3 Encrypt all non-console administrative access using strong cryptography
ISO 27002	9.4 System and application access control13.1 Network security management
NCSC Ten Steps for Cybersecurity	Secure ConfigurationNetwork Security
NCSC Ten Steps for Cybersecurity	Secure Configuration

Vulnerability Management

Security is a process, nothing you can do about this, so for this reason you must run continuous activities to know what is your exposure to new threats. So, as part of your vulnerability management process, you should define a security scan schedule (weekly, monthly, quarterly, etc). Faraday can support the most common security scan tools and also give you extra capabilities to do

this more transparently and automated with the consolidation of all the findings in one place :) So, you can run different tools, with the same or different scope, but use Faraday to review the results in one place. This will offer a better approach to have the “whole picture” for internal and external security scans.

A quick recap: if we know who is accountable for the security of an asset, we could assign the security issue to this person and give follow-up using Faraday. This means using “Asset Management” registers to improve Vulnerability Management. Faraday could be connected to the most common ticketing tools, so you can follow the progress from the same place where you have the findings.

Faraday can be integrated with the most common security scan tools to obtain the best approach regarding your exposure, in just one place. By the way, you can create reports based on results, for example, for:

- Top 10 Most Vulnerable Asset
- Top 10 Asset with Critical findings
- Top 10 Insecure Servers.
- Top 10 of Protocols.
- Platform which more vulnerabilities.

As always, you should define the reports based on your security objectives which are part of the cybersecurity program. This should be part of a security dashboard :)

You could read more about this in #CISControls CSC-4, but also this process is part of ISO, NIST, PCI, DSD 35 Top Mitigation Strategies, among others references.

Compliance Mapping

IS Controls	CSC 4 - Continuous Vulnerability Assessment and RemediationCSC 18 - Application Software Security
Australia DSD Top 35 Mitigations Strategies	Patch ApplicationsPatch Operating Systems
PCI-DSS	6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)
ISO 27002	9.4 System and application access control18.2 Information security reviews
NCSC Ten Steps for Cybersecurity	Secure ConfigurationNetwork Security

IS Controls	CSC 4 - Continuous Vulnerability Assessment and RemediationCSC 18 - Application Software Security
NCSC Ten Steps for Cybersecurity	Secure Configuration

Pentest Management

Pentesting is a “verification process”, which means you should use the pentest to verify if your project has followed the security rules (as part of your SDLC). The worst-case scenario would be waiting for the pentest to apply security measures, this is more expensive than including security from the beginning and would be a risk for the project to Go Live.

With Faraday you can consolidate all the results and use it to do appropriate follow-up. After remediation you can register the verification into the tool, as well. This means the entire lifecycle of the issue is in one place. You can also use tags to mark which is the pentest calendar which applies for each platform, for example: this year, next year, decommission, etc.

Another usage could be applying tags to match findings. For example, vulnerability over a PCI asset with CVSS between 7 to 10 means PCI Non-compliance situation. Or OWASP Top 10 issue would mean PCI Non-compliance, but these are just examples.

Pentest execution and follow-up was the main purpose of Faraday from past years, but now you can increase the value involving this process (pentest management) into your cybersecurity program also with other processes like the ones described in this article.

You could read more about this in #CISControls CSC-20, but also this process is part of ISO, NIST, PCI, among others references.

Compliance Management

Reference	Section
CIS Controls	CSC 18 - Application Software SecurityCSC 20 - Penetration Testing and Red Team exercises
PCI-DSS	6.5 Secure Coding considering OWASP TOP 1011.3 Implement a methodology for penetration testing
ISO 27002	12.6 Technical vulnerability management14.1 Security requirements of information systems14.2 Security in development and support processes18.2 Information security reviews
NCSC Ten Steps for Cybersecurity	Secure ConfigurationNetwork Security
NCSC Ten Steps for Cybersecurity	Secure Configuration

Some conclusions:

A cybersecurity program is something which you must adapt and maintain based on your business needs. A fixed plan for everyone is not possible, for this reason you must be close to your business, know the environment and its behaviour, know its risks and compliance requirements. Security is a

continuous process which needs training, time, effort, teamwork, support from the business, budget, and heart!

To be agile and offer a good performance you should use a tool or a sub-set of tools. Faraday is a great tool to support your cybersecurity program, with a lot of possible usages, features which are updated frequently, with support for the most common security platforms and with a very challenging roadmap of new features.