PNNL-33190

FIC Threat Profile

Provided by Shamrock Cyber

July 2022

Josh Bigler
Angie Chastain
Paul Francik
Catie Himes
Danielle Nodine
Emma Lancaster
Patrick O'Connell
Aaron Phillips
Shawn Ricketts
Garret Seppala
Bianca Steele
Chance Younkin
Jacob Beaman
Angela Steinmetz

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, **makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from
the Office of Scientific and Technical
Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov**

PNNL-33190

FIC Threat Profile

Provided by Shamrock Cyber

July 2022

Josh Bigler
Angie Chastain
Paul Francik
Catie Himes
Danielle Nodine
Emma Lancaster
Patrick O'Connell
Aaron Phillips
Shawn Ricketts
Garret Seppala
Bianca Steele
Chance Younkin
Jacob Beaman
Angela Steinmetz

https://shamrockcyber.pnnl.gov

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Contents

Diagrams

Figures

Tables

Acronyms and Abbreviations

CIA	Confidentiality, Integrity, Availability
IDDIL-ATC	Identify Assets, Define the Attack Surface, Decompose the System, Identify Attack Vectors, List the Threat Actors, Analysis & Assessment, Triage, Controls
PNNL	Pacific Northwest National Laboratory
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TMT	Threat Modeling Tool

Acronyms from NIST 800-53:

AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity

Summary

The FIC team has engaged with PNNL's Shamrock Cyber Team to produce this Threat Profile. The Threat Profile provides the foundation for a thorough understanding of threats for development teams and stakeholders, and users of the system. The Threat Profile can be used as is, or as content to inform other reports tailored to a specific audience. It is intended to enable decision makers at all levels to improve the security posture of the system.

For the Threat Profile, threats to the FIC system were categorized, prioritized, and mapped directly to affected system components. The table below shows the number of threats per category and per priority.

Threat Type	High Priority	Medium Priority	Low Priority	Totals
Spoofing	0	6	0	**6**
Tampering	3	2	0	**5**
Repudiation	0	0	3	**3**
Information Disclosure	0	3	0	**3**
Denial of Service	1	0	2	**3**
Elevation of Privilege	4	0	0	**4**
GRAND TOTALS	***8***	***11***	***5***	***24***

This Threat Profile provides critical information for making threat-based decisions to increase security at a reasonable cost and to reduce risk. Readers can use the Threat Profile to decide whether to implement the given mitigations or to accept threats based on their impact to the system. Not all threats must be mitigated, and not all threats can be addressed in a cost-effective way. The Threat Profile does not make these determinations, but rather provides the threats and mitigations so that proper stakeholders may make those determinations. These are the status values for a given threat:

Implemented – threat is mitigated due to implementation of the mitigation within the system
Transferred – the threat risk has been transferred to a different entity and is out of scope
Accepted – the threat risk is accepted, and no mitigation will be implemented
Pending – the threat and its mitigation are being considered by the FIC team.

The table below shows status and totals for all mitigations in this Threat Profile.

Status	High Priority	Medium Priority	Low Priority	Totals
Implemented	3	8	1	***12***
Transferred	3	0	0	***3***
Accepted	0	0	1	***1***
Pending	**2**	**3**	**3**	***8***
GRAND TOTALS	***8***	***11***	***5***	***24***

Note that there are **8 pending** mitigations of 24 total threats in the Threat Profile. While it cannot be guaranteed that all threats, vulnerabilities, and risks will be found and mitigated, the Threat Profile shows the FIC team's due diligence in taking cybersecurity seriously. This effort leads to more secure systems and better-understood security.

1.0 Introduction

The FIC team is engaged with Pacific Northwest National Laboratory's (PNNL's) ***Shamrock Cyber*** Team to provide cybersecurity analyses of the FIC software. Shamrock offers several software services, as shown in Figure 1. These services are ultimately used together to inform business decision makers and minimize mission risk. Shamrock's threat-based analysis begins with ***Threat Models***, which are represented in a set of system diagrams. The next step is ***Threat Findings***, which consists of the threat models, use cases, and the threat findings. The final step is the ***Threat Profile*** (this document), which contains not only the Threat Findings, but also actionable mitigations that can be implemented against the threats, which is the ultimate objective of Shamrock threat-based analysis.

Consequence Based Analysis – analyzes the abuse, misuse, and hazards that determine risks of developing and deploying a system. The result is a Consequence Profile detailing the consequence-based analysis.

Threat Based Software Analysis – determines and prioritizes threats against the system and recommends mitigations. The result is a Threat Profile that contains a threat model, threat findings, and mitigations.

Vulnerability Based Analysis – analyzes a system from a vulnerability perspective and includes structural security analysis, operational security analysis, and security testing. The result is a Vulnerability Profile detailing the vulnerability-based analysis

Figure 1. Shamrock Cyber services.

1.1 Purpose of the Threat Profile

The Threat Profile establishes security requirements, justifies security measures, yields actionable controls, and effectively communicates risk. To that end, it can be effectively used by development teams, software architects, managers, and stakeholders. For stakeholders and managers, the Threat Profile shows what has been mitigated and what has not been mitigated, thus enabling decision makers to assess priorities based on the actual system and the threats against it. For development teams and software architects, the Threat Profile provides direct and actionable tasking that boosts the cybersecurity of the software product. In addition to providing information, the format of the Threat Profile maps mitigations to threats and threats to the diagram, making it clear where and how the controls are affecting and benefiting the system. This is advantageous compared to controls and vulnerability assessments that are not threat based and do not stem from system diagrams.

1.2 Categorizing and Prioritizing Threats

Categorizing threats helps identify, organize, and prioritize threats in any system—this holds true for FIC. To optimize the analysis process, streamline the engagements, and aid in mitigation, Shamrock Cyber utilizes Microsoft's STRIDE model (see Figure 2). There are many categorization models, but STRIDE best lends itself to Shamrock Cyber's processes, and tools are available to partially automate and expedite the initial analysis processes. Shamrock Cyber uses Microsoft's Threat Modeling Tool (TMT), which is based on the STRIDE model. The tool provides initial results, and the Shamrock Cyber team provides expertise to consolidate the threats.

Spoofing **–** when a process, file, website, network address, etc. is not what it claims to be
Tampering – the act of altering the bits in a running process, data in storage, or data in transit
Repudiation – involves an adversary denying that something happened
Information Disclosure – when the information can be read by an unauthorized party
Denial of Service – when the process or data store is unable to service incoming requests
Elevation of Privilege – when an adversary gains increased capability on a system or network

Figure 2. Microsoft's STRIDE model described.

Prioritizing threats is also critical to the process of developing a Threat Profile. With a list of mitigations, each with their own cost, level of effort, and consequences, it is necessary to understand which ones are most important and why. For a Threat Profile, priorities start with the standard CIA (Confidentiality, Integrity, and Availability) Triad, as used in Figure 3. The terms are defined simplistically as follows:

***Confidentiality* –** keep the data secret.

***Integrity* –** make sure the data is correct.

***Availability* –** make the data available.

These terms are important considerations when prioritizing threats, but using the triad necessitates that one of the three must be ranked as the most important. Figure 3 shows the FIC priorities for this Threat Profile.

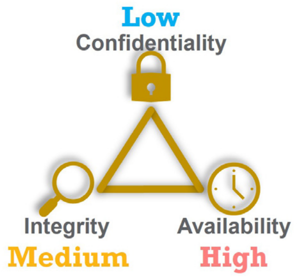


Figure 3. FIC priorities.

1.3 Types of Mitigation

Mitigations identified in this Threat Profile fall into three categories:

Physical – This is the traditional type of security in which valuable assets are guarded with guns, guards, and gates. However, physical security is becoming blended with cybersecurity in many ways because computers and networks are linked with gates, locks, and other access protection devices.

Technical – This refers to cybersecurity technology that is applied to typically (but not always) digital assets. Multi-factor authentication is a good example of a technical mitigation for access control.

Operational/Administrative – This is a method of following policy or procedural practices to implement security.

While these three types are not identified directly in the Threat Profile, it is important to note that most of the mitigations fall into the technical category, although both physical and operational do occur.

2.0 Threat Model

A Shamrock Cyber threat model is a set of use cases, a set of abuse cases, and a set of system diagrams. Use cases are descriptions of how the system operates from a user's viewpoint. They are invaluable for deriving system diagrams, which are the framework for Threat Findings and the Threat Profile. Abuse cases are just like use cases, but from the perspective of an adversary, abuse cases are used primarily to help derive and understand mitigations.

2.1 User Roles

User roles are descriptions of each user role and how that role interacts with the system from that user's viewpoint. They are invaluable for deriving system diagrams, which are the framework for Threat Findings and the Threat Profile. The following are typical users and their corresponding interactions with the system.

System Administrator. System administrators are the privileged administrator accounts for the FIC site. They have access to all the functions in the FIC site, as well as the ability to identify and establish configuration, and specify access authorizations for users.

General User. General users are those who visit the site for the purpose of browsing, reporting violations, applying for permits, etc.

2.2 Threat Diagrams

The diagram(s) in this section represent the FIC system and were derived through engagements between the Shamrock Cyber team and the FIC team. They contain some assumptions based on a mutual understanding about how the system will be designed and implemented.

2.2.1 Understanding Trust Boundaries

The most important aspect of performing threat-based analysis is knowing what trust boundaries are and where they are located. Interactions that cross trust boundaries are the most likely place for an adversary to inflict damage on a system. Figure 4 shows the FIC trust boundaries and explains what they are and where they are. The hierarchy of trust boundaries depicted in Figure 4 are maintained throughout the threat diagrams.

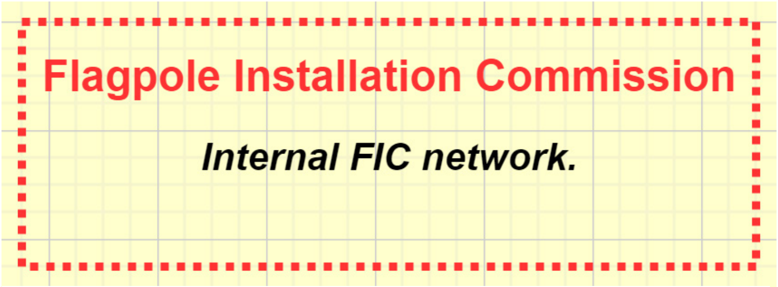
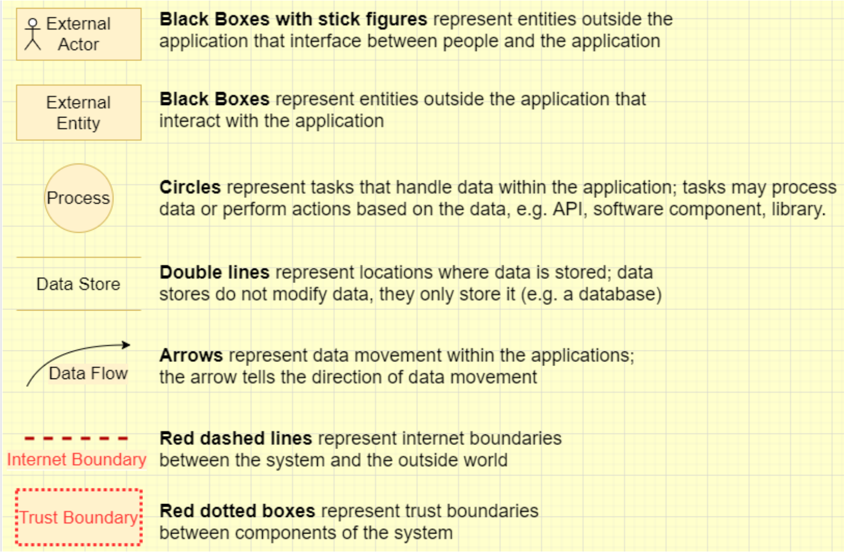


Figure 4. Trust boundaries defined.

The conventions used in the threat diagrams below help distinguish and categorize the different components of the system as follows:



Black Boxes with stick figures represent entities outside the application that interface between people and the application

Black Boxes represent entities outside the application that interact with the application

Circles represent tasks that handle data within the application; tasks may process data or perform actions based on the data, e.g. API, software component, library.

Double lines represent locations where data is stored; data stores do not modify data, they only store it (e.g. a database)

Arrows represent data movement within the applications; the arrow tells the direction of data movement

Red dashed lines represent internet boundaries between the system and the outside world

Red dotted boxes represent trust boundaries between components of the system

Figure 5. Legend for threat model diagrams.

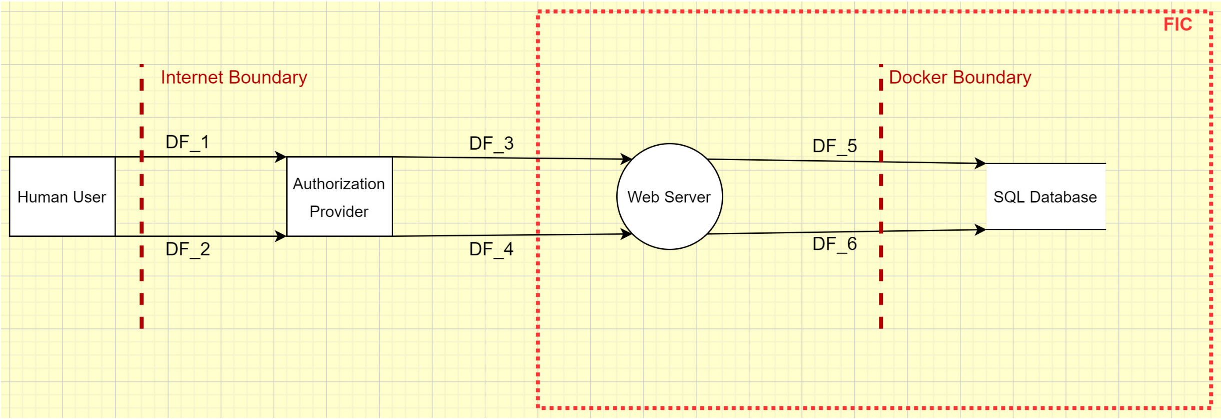


Diagram 1. FIC system diagram.

3.0 Threat Profile Table

The details for all the threats, the mapping of those threats to categories, example threats, and associated mitigations are documented here. Mitigations are the main objective and describe what will be done to prevent, deter, or minimize the threat.

3.1 Interpreting the Labels

The labels captured in parentheses in the Threat column of the Threat Profile Table below refer to the diagrams above. The label refers to an interaction (arrow) in the diagram, thus showing which interaction and which components the threat corresponds to. For example, a label such as `D1_I15` refers to Diagram 1, Interaction 15. If you find Diagram 1 above, the arrow labeled `D1_I15` will be the interaction corresponding to the threat. This strategy enables tracking of a mitigation, the threat it addresses, and the area of the diagram where the threat could occur. Thus, the table provides complete traceability from mitigation to threat to interactions between components.

3.2 Status of Mitigations

This Threat Profile provides critical information for making threat-based decisions to increase security at a reasonable cost and to reduce risk. Readers can use the Threat Profile to decide whether to implement the given mitigations or to accept threats based on their impact to the system. Not all threats must be mitigated, and not all threats can be addressed in a cost-effective way. The Threat Profile does not make these determinations, but rather provides the threats and mitigations so that proper stakeholders may make those determinations. For a given threat (a row in the table below), a status is assigned to that threat to indicate what is or should be done. These are the status values for a given threat:

Implemented – threat is mitigated due to implementation of the mitigation within the system
Transferred – the threat risk has been transferred to a different entity and is out of scope
Accepted – the threat risk is accepted, and no mitigation will be implemented
Pending – the threat and its mitigation are being considered by the FIC team.

Note that ***Pending*** mitigations are potential issues that should be addressed and assigned one of the other three values. The description provides the detail to explain the situation for the purposes of due diligence, traceability, or risk management.

3.3 NIST Standards

The mitigations provided in this threat profile have been mapped to the ***Security and Privacy Controls for Federal Information Systems and Organizations, commonly referred to as SP 800-53 Rev. 4***[1]. The publication was released by the National Institute of Standards and Technology (NIST). The Shamrock Cyber team has mapped the mitigations in order to readily show compliance with NIST recommendations. For each mitigation in the threat profile table, the corresponding NIST standards are listed. Keep in mind that some mitigations map to more than one standard in the SP 800-53 document.

[1] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

3.4 The Detailed Threat Profile Table

Table 1 below lists the threat type, threat, and mitigation. The table is arranged in order of priority.

Table 1. Threat Profile table.

#	Threat Type	Threat	Diagram Location	Mitigation	Mitigation Status	NIST
HIGH						
1	Tampering	Adversaries may inject SQL statements (malicious code) that are later passed to an instance of the SQL Server for parsing and execution. This could give an adversary the ability to read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system, and in some cases issue commands to the operating system	D1_I5	Use Prepared Statements (with Parameterized Queries); Use properly constructed stored procedures; Allow-list input validation; and or escaping all user-supplied input	Pending	SI-15, SI-4
2	Tampering	Data flowing across DF_3 may be tampered with by an attacker. This may lead to a denial-of-service attack against the Web Server, an elevation of privilege attack against the Web Server, or an information disclosure attack against the Web Server. Failure to verify that user input is as expected is a root cause of a very large number of exploitable issues	D1_I3	FIC IT authorizes users on behalf of the FIC app	Transferred	SI-15, SI-4

3	Tampering	Data flowing across DF_5 may be tampered with by an attacker. This may lead to corruption of the SQL Database	D1_I5	Access is restricted via FIC IT incorporating the use of Docker	Implemented	SI-15, SI-4
4	Denial Of Service	An external agent may prevent access to a data store on the other side of the trust boundary	D1_I5, D1_I6	Access is restricted via FIC IT incorporating the use of Docker to the VM	Implemented	AC-2, SC-5
5	Elevation Of Privilege	An attacker may pass data into the Web Server to change the flow of program execution within the Web Server to the attacker's choosing	D1_I3, D1_I6	The application is written in Node.JS and located within a Docker container	Implemented	AC-3
6	Elevation Of Privilege	Authorization Provider may be able to remotely execute code for Web Server	D1_I3	FIC IT authorizes users on behalf of the FIC app	Transferred	AC-3
7	Elevation Of Privilege	Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.	D1_I1, D1_I4	Handled by FIC IT	Transferred	
8	Elevation Of Privilege	SQL Database may be able to remotely execute code for Web Server	D1_I6	Validate user input, use parameterized queries, and disable unused functions	Pending	SI-15
MEDIUM						
10	Spoofing	The authorization Provider may be spoofed by an attacker, and this may lead to data being sent to the attacker's target instead of the Authorization Provider.	D1_I4	A standard authentication mechanism to identify the external entity was implemented	Implemented	CA-6, SC-7, IA-2

11	Spoofing	Authorization Provider may be spoofed by an attacker, and this may lead to unauthorized access to the Web Server.	D1_I3	A standard authentication mechanism to identify the external entity was implemented	Implemented	CA-6, SC-7, IA-2
12	Spoofing	SQL Database may be spoofed by an attacker, and this may lead to data being written to the attacker's target instead of SQL Database.	D1_I5	A standard authentication mechanism to identify the destination data store was implemented	Implemented	CA-6, SC-7, IA-2
13	Spoofing	SQL Database may be spoofed by an attacker, and this may lead to incorrect data delivered to the Web Server.	D1_I6	A standard authentication mechanism to identify the data store source was implemented	Implemented	CA-6, SC-7, IA-2
14	Spoofing	The web Server may be spoofed by an attacker, and this may lead to information disclosure by Authorization Provider.	D1_I3	A standard authentication mechanism to identify the destination process was implemented	Implemented	CA-6, SC-7, IA-2, AU-13
15	Spoofing	The web Server may be spoofed by an attacker, and this may lead to information disclosure by SQL Database.	D1_I6	A standard authentication mechanism to identify the destination process was implemented	Implemented	CA-6, SC-7, IA-2, AU-13

16	Tampering	The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input	D1_I3, D1_I6	Ensure that all variables go through validation and are then escaped or sanitized; Implement the use of output encoding when you need to safely display data exactly as a user typed it.	Pending	SI-10
17	Tampering	The web server 'Web Server' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'SQL Database' inputs and output	D1_I6	Ensure that all variables go through validation and are then escaped or sanitized; Implement the use of output encoding when you need to safely display data exactly as a user typed it.	Pending	SI-10, SI-15
18	Information Disclosure	Data flowing across DF_3 may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations	D1_I3	Has already implemented a reverse proxy on the box with FIC signed certs	Implemented	SC-8.1

19	Information Disclosure	Data flowing across DF_5 may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations	D1_I5	Has already Implemented a reverse proxy on the box with FIC signed certs	Implemented	SC-8.1
20	Information Disclosure	Improper data protection of SQL Database can allow an attacker to read information not intended for disclosure.	D1_I6	1. Has reviewed authorization settings ; 2. Protect against SQL injection attacks by using Prepared Statements (with Parameterized Queries); Use properly constructed stored procedures; Allow-list input validation; and or escaping all user-supplied input -; 3. Implement Input validation, accepting only characters from a list of safe values, or identify and escape a deny list of potentially malicious values	1. Implemented 2. Pending 3. Pending	SI-15, SI-10, SC-28

LOW						
21	Repudiation	The Authorization Provider could lie and claim that it did not receive data from a process on the other side of the trust boundary.	D1_I1, D1_I4	FIC IT will cover logging, as they own the Authorization box	Implemented	AU-2, AU-16
22	Repudiation	The web Server could lie and claim that it did not receive data from a source outside the trust boundary	D1_I3, D1_I6	Ensure the use of logging or auditing to record the source, time, and summary of the received data.	Pending	AU-2
23	Repudiation	The SQL Database could lie and claim that it did not write data received from an entity on the other side of the trust boundary.	D1_I5	Verify that logging is happening appropriately.	Pending	AU-2, AU-9
24	Denial Of Service	Failure to limit resource consumption can lead to DoS attacks that can be hard to deal with.	D1_I5	Verify that your resource requests don't deadlock, and that they do timeout. Rate limit traffic on the app. Create an upper limit on the size of the requests.	Pending	SC-5, SC-5(2)
25	Denial Of Service	An external agent can interrupt data flowing across a trust boundary in either direction.	D1_I1, D1_I3, D1_I4, D1_I5, D1_I6	This resource needs to be accessible nationwide	Accepted	SC-5, SC-5(3)

4.0 Conclusion

This FIC Threat Profile identifies threats that are mapped to specific system components. It also provides mitigations for each distinct threat–asset pairing. The outputs are actionable controls and facilitate an understanding of risk that informs decision makers who are most concerned with optimizing impact or cost. The contents of this Threat Profile inform threat-based decisions for increasing security at a reasonable cost and for reducing risk.

This threat-based software analysis illustrates the due diligence of the FIC team. In seeking an external analysis of their software, the team is assuring that FIC provides a secure and reliable capability in its operating environment.

The FIC Threat Profile provides a foundation for a thorough understanding of possible threats for the development team, the testing team, management, stakeholders, and partner stakeholders of FIC. It enables decision makers at all levels to improve the security posture of the system. This effort leads to more secure software and better-understood security. The FIC team is to be commended for their rigorous approach to employing cybersecurity throughout the development life cycle of their products.

Appendix A Terms of Reference

Term	Definition	Examples
Abuse Case	A product of consequence analysis that focuses on how systems can be abused and the consequences when a potential adversary takes an intentional hostile action against an organization's operations. An abuse case consists of three elements: Functional Use Element (FUE), Technical Abuse Element (TAE), and Functional Abuse Element (FAE) that combine to achieve a malicious outcome of effect that is intended to support an adversary's motives. NOTE: An abuse case is a single pass through the sets of FUEs, FAEs, TAEs	
Adversary	An entity whose intentions are hostile to an organization or its stakeholders	• *Hacktivist* – see relevant entry for definition • *Industrial espionage actor* – see relevant entry for definition • *Nation state actor* – see relevant entry for definition • *Organized crime actor* – see relevant entry for definition • *Script kiddie* – see relevant entry for definition • *Terrorist actor* – see relevant entry for definition • *Traditional hacker* – see relevant entry for definition
Adversary Context	A cybersecurity and risk management analysis perspective that emphasizes consideration of the actions and motives of potential adversaries when vetting and prioritizing potential risks.	
Adversary Dossier	An analytic report that presents risks, threats, or consequences of an adversary's actions and based on that adversary's capabilities, accesses, and motives	
Asset	"anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards)." – NIST IR 7693	
Availability	Ensuring timely and reliable access to and use of information – NIST	
Capability	The means by which harm is inflicted by an adversary using an arsenal of exploits, techniques, and tactics. An adversary's capabilities are dependent upon their levels of technical competence, funding, and resolve to act.	
Campaign	An agreed upon effort between a customer and the SSC team, includes one or more of the services offered by SSC.	

CIA Triad	A common cyber security model that identifies the three essential characteristics of information to be Confidentiality, Integrity, and Availability. This model is used to support the assessment of threats and vulnerabilities and for developing security strategies. The three elements of the CIA Triad are: • *Confidentiality* – see relevant entry for definition • *Integrity* – see relevant entry for definition • *Availability* – see relevant entry for definition	
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information – NIST	
Consequence	Harmful impact to a system, its operations, its mission outcome, or its stakeholders' equities through the realization of risk. Realized risk can be the result of an adversary's actions (Abuse Case risk), unintended misuse of the system (Misuse Case risk), or by a hazard acting on the system (Hazard Case risk).	
Consequence Based Analysis	The cumulative process of generating or identifying specified conditions which produce harm to a system, operations, mission outcomes, or stakeholder equities. The product/outcome of consequence-based analysis are Abuse Cases, Misuse Cases, or Hazard Cases.	
Dossier	An analytic report that organizes the results and findings as details about or related to a specific entity or subject	• *Adversary dossier* – see relevant entry for definition • *Others to come later* – relevant entries to be added
Denial of Service	When the process or data store is unable to service incoming requests	
Dynamic Application Security Testing (DAST)	An assessment of applications for indications of security vulnerabilities conducted while the software is in a running (dynamic) state	
Elevation of Privilege	When an adversary gains increased capability on a system or network	
Exploit/Weapon	"The means through which a vulnerability can be leveraged for malicious activity by hackers" – Rapid7	
Functional Abuse Element (FAE)	Part of the Abuse Case analysis methodology that specifically details an undesirable physical or logical capability of the system being analyzed. This is the consequence or effect that an adversary desires to accomplish in an Abuse Case.	

Functional Use Element (FUE)	Part of the Abuse Case analysis methodology that specifically details a physical or logical capability of the system being analyzed. FUEs include both the operationally intended functions of the system, and any other capabilities that extend beyond the intended use of the system.	
Hacktivist	A cyber threat adversary who utilizes illicit cyber-based techniques as a form of protest or civil disobedience to promote political or ideological goals.	
Hazard	A non-anthropogenic event in a system's operational environment with the potential to inflict harm or generate a negative consequence for the system's stakeholders.	
Hazard Case	A product of consequence analysis that focuses on the consequences of a non-anthropogenic event inducing harm to a system. A Hazard Case will also consist of three elements that are analogous to those in an Abuse Case.	
Industrial Espionage Actor	A cyber threat adversary whose primary motivation is business or industry related (e.g., theft of intellectual property, trade secrets or other sensitive/secret data; damaging business reputation; etc.)	
Information Disclosure	When the information can be read by an unauthorized party	
Integrity	Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity – NIST	
Misuse	A user action or activity with the potential to unintentionally inflict harm or generate a negative consequence for the system's stakeholders.	
Misuse Case	A product of consequence analysis that focuses on the consequences of a system operator or user inducing harm unintentionally through incorrect use of the system or its environment. A Misuse Case will also consist of three elements that are analogous to those in an Abuse Case.	
Mitigation	A mitigation involves implementing technical or procedural measures/controls to counteract specific vulnerabilities. Types of mitigations include physical, technical, and operational/administrative.	• *Implemented* – threat is mitigated due to implementation of the mitigation within the system • *Transferred* – the threat risk has been transferred to a different entity and is out of scope • *Accepted* – the threat risk is accepted and no mitigation will be implemented • *Pending* – the threat and its mitigation are being considered by the project team
Motive	The reason an adversary desires to enact a specific malicious effect on a system or organization	

Nation State Actor	A cyber threat adversary that is acting on behest of and/or with the financial and technological backing of a nation state.	
Organized Crime Actor	A cyber threat adversary working as part of or an extension of a criminal group and who's illegal cyber activities provide material support or revenue for that group	
Operational Context	A cybersecurity and risk management analysis perspective that emphasizes system operations, interactions, and the operational environment when vetting or prioritizing potential risks.	
Profile	An analytic report that is the result of a process that lays out addressable issues and lists mitigations for each of those issues	• *Threat Profile* – see relevant entry for definition • *Vulnerability Profile* – see relevant entry for definition • *Abuse Profile* – see relevant entry for definition • *Adversary Profile* – see relevant entry for definition • *Consequence Profile* – see relevant entry for definition
Script Kiddie	A cyber threat adversary that lacks the programing skill to develop their own cyberattack tools and instead relies on previously developed programs, software, and tools. Script kiddie is generally a pejorative term for the lowest-tier level of hackers. However, history has shown that script kiddies have launched devastating attacks.	
Security Based Development	The process of applying security principles, profiles, and dossiers to the design, development, and deployment of a system	
Repudiation	Repudiation involves an adversary denying that something happened (usually involves policy, as in getting a lawyer); involves evidence of origination, submission, and receipt	
Risk	The possibility of a negative, consequence-based event occurring in the context of the: • Asset being protected • Stakeholder equities • Abilities of the adversary • Motives or intentions of the adversary • Vulnerabilities that can be exploited • Harm that can be inflicted	
Spoofing	When a person, process, file, website, network address, etc. is not what it claims to be	

Static Application Security Testing (SAST)	Assessment of source code and binaries for indications of security vulnerabilities conducted from the inside out while the software is in a nonrunning (static) state	
STRIDE Model	A Microsoft methodology of characterizing cybersecurity threats into six categories, with STRIDE being the mnemonic for remembering those categories, which are as follows: • ***S**poofing* – see relevant entry for definition • ***T**ampering* – see relevant entry for definition • ***R**epudiation* – see relevant entry for definition • ***I**nformation Disclosure* – see relevant entry for definition • ***D**enial of Service* – see relevant entry for definition • ***E**levation of Privilege* – see relevant entry for definition	
Tampering	The act of altering the bits in a running process, data in storage, or data in transit	
Technical Abuse Element (TAE)	Part of the Abuse Case analysis methodology that details some manner in which an adversary can have an effect on a system. TAEs include such things as system vulnerabilities, exploits, attack vectors, etc.	
Terrorist Actor	A cyber threat adversary whose activities are conducted in support of the ideological/political goals, actions, and/or messaging of a terrorist organization and is funded and technologically supported by that organization; or acts to promote or otherwise promote terrorism even without formal financial, coordination, or support ties to a specific organization (e.g., lone wolf)	
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (https://csrc.nist.gov/glossary/term/threat)	
Threat Based Analysis	The cumulative process of generating Threat Models, Threat Findings, and a Threat Profile for a given system. The product/outcome of a Threat Based Analysis is a Threat Findings document with categorized and prioritized threats (from task overview table in SSC Engagement Playbook).	
Threat Profile	The result of a systematic process including system decomposition, abuse case modeling, asset characterization, STRIDE threat modeling, and risk	

	reduction through mitigation development. The threat profile document itself gives an overview of these activities and guides the system owners on how to proceed in risk reduction.	
Trust Boundaries	In the context of Threat Modeling, trust boundaries are locations on the data flow diagram where data changes its level of trust. Any place where data is passed between two processes is typically a trust boundary. All sub-systems and data within distinct boundaries share trust levels and thus trust each other. Boundaries nested within existing boundaries have a stricter trust level, where the external system and components will trust all sub-systems from within the nested boundary, but not necessarily the other way around.	
Threat Category	A class or division of threats regarded as having shared characteristics. The threat category of a given threat is namely determined by the system property in jeopardy of being violated by said threat. Examples of threat categories include the STRIDE categories and their respective properties of Authenticity, Integrity, Non-repudiability, Confidentiality, Availability, Authorization. (see entry for STRIDE Model)	
Threat Findings	A list of threats found against a system, including a short description, their categorization, and project-based prioritization.	
Threat Modeling	A structured approach of identifying and prioritizing potential threats to a system and determining the value that potential mitigations would have in reducing or neutralizing those threats. Threat modeling is also a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.	
Threat Model	A set of one or more diagrams representing system components, their connections, and possible attack points within the diagram.	
Traditional Hacker	A cyber threat adversary whose illicit cyber behaviors are primarily motivated by curiosity, achieving notoriety, and overcoming technical challenges.	
Threat Modeling	A structured approach of identifying and prioritizing potential threats to a system and determining the value that potential mitigations would have in reducing or neutralizing those threats. Threat modeling is also a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.	
Threat Model	The model of a system representing the information gathered through the threat modeling process.	

Traditional Hacker	A cyber threat adversary whose illicit cyber behaviors are primarily motivated by curiosity, achieving notoriety, and overcoming technical challenges.	
Usage Description	Capability-based descriptions of how the system operates from a user's viewpoint. They are invaluable for deriving system diagrams, which are the framework for Threat Based Analysis.	*System Administrator*: Responsible for deployment and maintenance of the system. System administrator will administer deployments in actual deployment environments. For example, a system administrator is responsible for deploying VOLTTRON and its agents into all the buildings in the campus. This person will have access to full system.
Usage Narrative	A single, highly specific, real-world example of actual characters interacting with something to achieve some objective.	Myrtle and Sam sit down on the couch together after supper to relax. Sam suggests they get out their WooptiDo to call their daughter Mary and her husband Bob. They haven't talked for a while and want to look at pictures of Ray, their new grandson. Sam touches the phone book in the upper left corner of the WooptiDo screen. Up pops a browser of names that have been stored on the WooptiDo. Myrtle rolls her eyes and simply says "Call Mary." The WooptiDo responds by dialing Mary's number and soon there is a ringing sound on the WooptiDo speaker… Meanwhile, Mary is cooking in the kitchen and Bob is in his favorite chair, puffing his pipe and watching the game on his WooptiDo. He's startled when suddenly the WooptiDo softly says, "Myrtle and Sam are calling…" Bob is enjoying the game and considers activating the "busy" signal, but he decides to answer the call. He hollers at Mary, who powers up her WooptiDo and joins the conversation. They all chat a while, although Bob is secretly eying the game in mini mode. After a while, Sam says he wants to see the pictures of Ray. Mary browses her WooptiDo folders, finds some pictures, and starts a "Slide show." A slide show immediately pops up on everyone's WooptiDo. Mary controls the show while everyone else watches. Bob has Myrtle and Sam on screen along with the slide show, but his attention is on the game. Suddenly, Myrtle asks to take control of the slide show. Mary reluctantly assigns the "Slideshow Driver" to Myrtle, giving her control of what everyone sees. Bob completely loses interest at this point, puts the call in mini mode, and brings the game

		back to full screen. Finally, after an hour, Myrtle ends the slide show, and everyone says their goodbyes. Myrtle and Sam put down their WooptiDos and smile. Mary turns off her WooptiDo and glares at Bob, which turns off Bob. Clearly, the game remains turned on. Everyone is pleased with their WooptiDo, although Mary ponders the usefulness of a “send-instant-shock” feature.
Use Case	A system analysis product that consists of assembling sequences of events and interactions between (and within) systems and their users in order to achieve particular goals (use)	
Vulnerability	The susceptibility of a system or component to intentional or unintentional sources of harm.	
Vulnerability Profile	The result of a systematic process including a static source code scan which highlights vulnerabilities at a line-by-line level, an analysis of the vulnerabilities found, and risk reduction through mitigation development. The vulnerability profile document gives an overview of these activities and guides the system owners on how to proceed in risk reduction.	

Appendix B Brief on Consequence Based Analysis

The Shamrock Cyber Team uses Consequence-Based Analysis (CBA) to assess risk to mission or business operations. Figure 6 shows the three categories of CBA, each of which is composed of three elements: a system function, a negative outcome, and a technical capability that, through the system function, enables the negative outcome. The elements, when present and combined in a system have the potential to impart harm to some part of the system, its operation, its mission, or its stakeholders. The negative outcome is a plausible consequence of something going wrong with the system or its operation. The technical element is the link that could transform normal operations into the identified negative outcome. Each of these cases is constructed as follows:

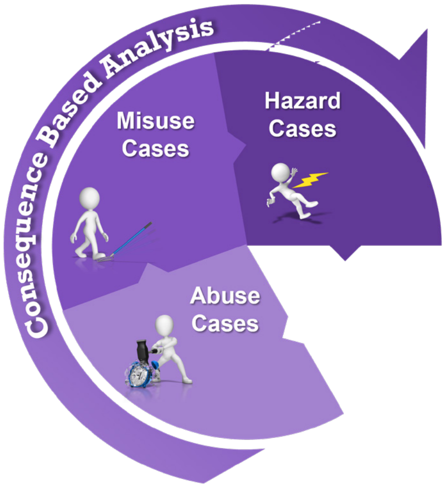


Figure 6. The CBA leaf of Shamrock Cyber.

Abuse Case – damage caused by intentional acts of an adversary

- Adversaries and their Motives (A&M) – who wants to do damage and why
- Functional Use Element (FUE) – what the system does
- Functional Abuse Element (FAE) – the harmful outcome
- Technical Abuse Element (TAE) – how the system can be "hacked" intentionally

Misuse Case – damage caused by unintentional acts and human error
Mistakes and Misbehavior (M&M) – foreseeable user mistakes or misuse
Functional Use Element (FUE) – what the system does
Functional Misuse Element (FME) – the harmful outcome
Technical Misuse Element (TME) – how the system errors when misused

Hazard Case – damage caused by non-human events in the system's operating environment

- Environmental Events (EE) – something that occurs naturally in the environment
- Functional Use Element (FUE) – what the system does
- Functional Hazard Element (FHE) – harmful outcome)
- Technical Hazard Element (THE) – how the system could malfunction due to a hazard

The Shamrock Cyber team engages with customers (owners, operators, and other stakeholders) to understand system operations, use cases, and missions. The team also gathers stakeholders' unacceptable mission outcomes and conditions. From this, plausible scenarios are derived that could lead to unacceptable consequences. Assessments for threats and vulnerabilities are then either gathered or performed and used to build the various "cases." The Shamrock Cyber team engages customers as needed throughout the process.

When analysis is complete, narratives such as ***Adversary Dossiers*** are developed to explain in simple, non-technical terms, the risks and consequences those risks can have on stakeholder equities. This allows greater stakeholder access to risk assessment and management processes and discussions. At the same time, each case is directly linked to one or more technical elements which directs system security and defense personnel in the identification, design, and implementation of security controls, vulnerability remediations, or risk mitigations.

Appendix C Brief on Vulnerability Based Analysis

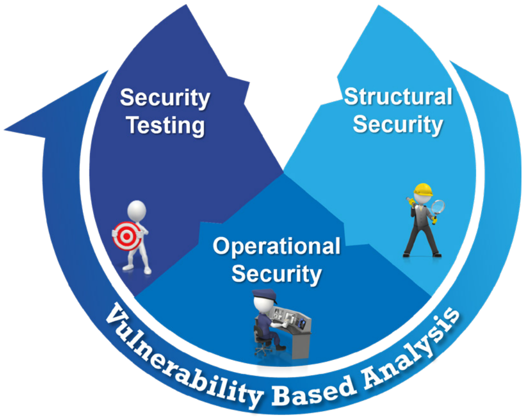


Figure 7. The VBA leaf of Shamrock Cyber.

The Shamrock Cyber Team is establishing Vulnerability Based Analysis (VBA) in the areas depicted in Figure 7. Shamrock Cyber VBA focuses on ***Structural Security***, ***Operational Security***, and ***Security Testing***. Structural Security involves vulnerability assessments on the construction of the system, which for software is Static Application Security Testing (SAST). Operational Security focuses on analyzing the behavior of a system while in operation, which for software is Dynamic Application Security Testing (DAST). Open-Source Analysis (OSA) is a software-focused analysis of third-party software and can be part of SAST or DAST.

When it comes to software, the objective of Shamrock Cyber VBA is to perform an analysis that eliminates false positives, summarizes the vulnerabilities, and makes recommendations. The result of this analysis enables the development team to prioritize vulnerabilities and address them in order of priority.

Shamrock Cyber makes use of Checkmarx, a commercial software scanning tool adopted by PNNL, that performs both SAST and OSA scanning. The Shamrock process is a straightforward set of steps:

1. ***Receive source code***

   The source code comes from the customer development team in the form of a zip file or a URL to a code repository The source code will be used as input to the Checkmarx scanner.

2. ***Execute a Checkmarx SAST scan***

   Every file contained in software (from the repo or the zip file) will be scanned and the results form the foundation for Shamrock Cyber analysis.

3. ***Execute a Checkmarx OSA scan***

   Dependency libraries will be scanned by Checkmarx, and vulnerable libraries along with out-of-date libraries will be documented, forming the foundation for Shamrock analysis.

4. ***Analyze SAST scan results***

   The results of Shamrock analysis of SAST go into the final report.

5. ***Analyze OSA scan results***

   The results of Shamrock analysis of OSA go into the final report

When this process is complete, the Shamrock Cyber team organizes the information into the final product, the ***Shamrock Cyber Vulnerability Profile***.

Appendix D Brief on Threat Based Analysis

The Shamrock Cyber team combines three stages of Threat-Based Analysis (TBA), as shown in Figure 8. TBA utilizes portions of Lockheed Martin's IDDIL-ATC methodology (Figure 9) to perform threat analysis. Shamrock optimizes IDDIL-ATC for more cost-effective, time-efficient results that lead to immediately actionable controls. Using the Lockheed Martin nomenclature, Shamrock actually begins with ***Decompose the System***. To accomplish this, Shamrock often requests that ***Usage Narratives*** be written by members of the project team. The narratives provide the Shamrock team with valuable context in simple, non-jargon terms. With this context, the next step is to develop a set of use cases and data flow diagrams that represent the system. Generally, the assets and the attack surface can be identified using these diagrams, thus addressing the ***Identify Assets*** and ***Define the Attack Surface*** steps. From there, Shamrock attempts to ***List Threat Actors***, but this is not yet a rigorous exercise. The use cases, abuse cases, and data flow diagrams represent the ***Shamrock Cyber Threat Model***, which is the foundation for developing the Threat Profile.

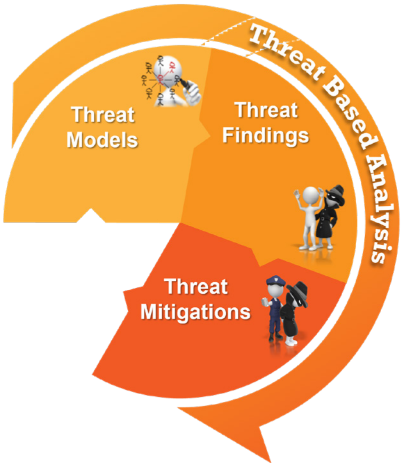
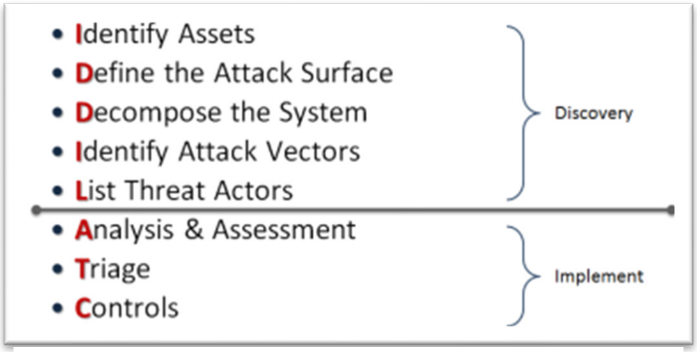


Figure 8. The TBA leaf of Shamrock Cyber.


- Identify Assets
- Define the Attack Surface
- Decompose the System
- Identify Attack Vectors
- List Threat Actors

Discovery

- Analysis & Assessment
- Triage
- Controls

Implement

Figure 9. Lockheed Martin's methodology.

Shamrock asks the project team to set an initial expectation of threat priority based on Confidentiality, Integrity, and Availability (CIA). The CIA Triad (see Figure 10) is a commonly used cybersecurity model.

The Shamrock Cyber team uses the data flow diagrams as input to Microsoft's Threat Modeling Tool (TMT). The TMT is a free download that comes with standard threat templates used by Shamrock. The TMT reads the diagrams and uses the templates to provide initial ***Analysis and Assessment*** as well as ***Triage*** results. The TMT also uses Microsoft's STRIDE model to categorize threats. The initial results from the TMT are then analyzed by Shamrock subject matter experts to complete the ***Shamrock Cyber Threat Findings*** for review by the project team.

Confidentiality
Integrity
Availability

Figure 10. The CIA Triad.

With the Threat Findings in hand, Shamrock goes back to the project team to collaboratively analyze and determine mitigations (***Controls***). When this exercise is complete, the Shamrock Cyber team organizes the information into the final product, the ***Shamrock Cyber Threat Profile***.

Pacific Northwest
National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov