INL/EXT-14-31522

ReACT Methodology Proof of Concept Final Report

Bri Rolston
Sarah Freeman

March 2014

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-14-31522

ReACT Methodology Proof of Concept Final Report

Bri Rolston
Sarah Freeman

March 2014

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Abstract

The Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE-OE) funded INL Researchers to evaluate a novel process for assessing and mitigating cyber security risks. The proof of concept level of the method was tested in an industry environment. This case study, plus additional case studies will support the further development of the method into a tool to assist industry in securing their critical networks. This report provides an understanding of the process developed in the Response Analysis and Characterization Tool (ReACT) project. This report concludes with lessons learned and a roadmap for final development of these tools for use by industry.

Executive Summary

The Response Analysis and Characterization Tool (ReACT) provides companies and practitioners with a standardized, methodical approach for assessing and mitigating cyber security risks. The process is designed to understand cyber security architecture and risks from the user's perspective, not the attacker's. ReACT is a proof of concept Frontier project funded by the Office of Electricity Delivery and Energy Reliability in the Department of Energy (DOE-OE). The team at the Idaho National Laboratory (INL) National and Homeland Security Critical Infrastructure Protection performed the work in partnership with an asset owner and refinement by DOE-OE experts.

Energy sector industries face an ever changing cyber threat environment with a constant flood of emerging threat information that is not specific to their implementation. Past threat sharing events with these asset owners in the energy sector has shown that there is no single approach which can be applied across the board. Mitigations for vulnerabilities and exploits along with incident response are static while the threat is dynamic due to the changing techniques of the attackers. Understanding and mitigating these threats with process improvement adds value to the business process of industry.

ReACT includes identifying methods to understand the asset owner's implementation, protection capabilities, and impacts to a cyber-threat. The three main areas of effort for the ReACT methodology include a functional overview, ReACT assessments and a strategy for process improvements after incident response. The methodology results in several products including a Functional Baseline Chart, and Communications Map to understand the functional overview; a Security Posture Analysis and Attack Surface Analysis for the assessment of cyber-threat; and finally a Root Cause Failure Analysis and ReACT Response Plan for threat incident response to feed into process improvements.

The ReACT methods were tested at an asset owner utility. This industry partner is an active participant in the protection of critical infrastructure specific to the energy sector and is advanced in their protection and incident response capabilities. The sophistication of this industry partner allowed the INL team to model the ReACT process quickly with minimal effort spent on identifying critical workflow or core systems.

This industry partner had a favorable impression to the ReACT proof of concept. In particular, the industry partner identified the primary benefit of the methodology as providing groups with an organized approach based on the functional security layers (FSL) within the Functional Security Matrix (FSM). The industry partner found value in the process improvement and dynamic approach to the cyber-threat as a step change in protection from the static vulnerability/exploit mitigations. During the assessment with the industry partner, feedback on the methods and process were identified along with lessons learned. The ReACT process is most successful when implemented in a team environment. During the case study, the project drew from both internal analysts and external SMEs. For example, the asset owner brought knowledge regarding the functional requirements and security posture, while the INL team brought their understanding of attack methods and cyber-threat incident response. Most of the recommendations promote asset owner involvement in cyber-threat analysis.

Future directions identified through asset owner partnerships include the need for additional case studies, the development of additional training materials on how to use the ReACT process, the development of a security controls catalog to understand the defense strategies, automation of the process, and provision near real-time threat sharing.

Acknowledgement

DOE-OE funded this Frontier project based on a concept presented during the FY13 annual operating plan teleconference. Response Analysis and Characterization Tool (ReACT) was funded along with other frontier concepts. Working with DOE-OE experts, INL staff refined the concept from root cause analysis to a standard method for assessing and mitigating cyber security risks with root cause analysis as one of the tools. ReACT represents this cooperation between DOE-OE subject matter experts, asset owner partnerships and INL staff.

CONTENTS

Acronyms

ATAC	Attack Technology, Analysis and Characterization
ASA	Attack Surface Analysis
CIP	Critical Infrastructure Protection
DOE-OE	Department of Energy Office of Electricity Delivery and Energy Reliability
EMS	Energy Management System
FSL	Functional Security Layers
FSM	Functional Security Matrix
NHS	National and Homeland Security
IDRA	Impact Driven Risk Analysis
INL	Idaho National Laboratory
ReACT	Response Analysis and Characterization Tool
RCFA	Root Cause Failure Analysis
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
UR&R	User Roles and Responsibilities

1. Introduction

The Response Analysis and Characterization Tool (ReACT) provides companies and practitioners with a standardized, methodical approach for assessing and mitigating cyber security risks. A team of Idaho National Laboratory (INL) National and Homeland Security (NHS) Critical Infrastructure Protection (CIP) experts performed this work focusing on cyber security risks to control systems. The process is designed to understand cyber security architecture and risks from the user's perspective, not the attacker's. This ReACT proof of concept report fulfills the milestone *ReACT Final Report*, number 2.5.8.

1.1 Background

Since the Department of Energy Office of Electricity Delivery and Energy Reliability's funding of the National SCADA Test Bed in 2003, INL's work in CIP has focused on the cyber security of control systems supporting the energy sector. INL's direction continues to support work with vendors of control systems and asset owners who manage and operate controls for the energy sector. Based on these past relationships, INL understood the challenges associated with the consumption of threat information and its applicability to industry. Based on significant experience in cyber security vulnerabilities of control systems, exploits, and incident response, INL was able to identify the issue of addressing the static, one time, vulnerability in a dynamic threat environment defined by an attacker's changing tools, techniques, and procedures. The ReACT proof of concept provides a standard method to analyze and mitigate the threat portion of the risk equations with specifics to implementation and business goals.

1.2 Scope

The scope of ReACT includes identifying methods to understand the asset owner's implementation, protection capabilities, and impacts to a cyber threat. Three main areas of effort include a) the identification of the functional overview, b) the completion of the ReACT assessments through the completion of the functional baseline, communication paths, security posture and attack surface analysis and c) the identification of a response strategy to include process improvements. The development of ReACT included collaboration with an asset owner, which allowed for a test of the proof of concept.

1.2.1 Basis for Development

INL researchers evaluated the concepts and assumptions which form the foundation of cyber security management. By working with an industry partner during product development a number of issues were identified:

1. A group's incident and risk remediation strategies may not consider business requirements or how technology is deployed within the organization.
2. Most cyber security incident and risk management work focuses upon solving short-term, technology issues identified through the review of technical security data. For example, vulnerabilities are managed in reaction to either patch releases by the vendors or the discovery of new malware.
3. A lack of root cause failure analysis (RCFA) typically impedes an organization's evolution toward more proactive incident and risk management processes.
4. Security teams are seen within their organizations as extremely punitive; in short, doing security to them, rather than with them.

From this collaborative work, INL researchers developed a framework to provide the foundational analysis, information architecture, and relationship correlation necessary to address the obstacles previously identified.

1.3 Purpose

The ReACT methodology provides energy-sector members with an organized approach to characterize cyber-based risks to their critical infrastructure. This characterization can then serve as the basis for developing a cyber-security metrics program for critical infrastructure. Once cyber risk has been characterized, organizations can begin to address threat more proactively.

Industry, much like other members in the public and private sectors, face an ever changing cyber threat environment. However the security efforts of these organizations do not suffer from a dearth of threat data, but rather the constant flood of emerging information. Against this backdrop, industry partners need a consistent, organized approach for evaluating publically available threat information.

The challenge of threat intelligence consumption is compounded by variations in focus, methods, and goals, across sectors and industries. There is no single approach which can be applied across the board. However, personalized approaches will fail if these efforts ignore the business goals of an organization.

1.3.1 ReACT Proof of Concept Objective

The INL team sought to create methods to provide industry the foundational analysis, information architecture, and relationship correlation necessary to address the obstacles previously identified. In order to properly evaluate the feasibility of this approach, INL developed the ReACT proof of concept project (in conjunction with the Attack Technology, Analysis and Characterization (ATAC) proof of concept project). Central to both these projects was an onsite assessment with an industry partner, during which INL worked closely with the local core system management team. By working with this industry partner, INL researchers developed a plan for further development.

1.3.2 Objective of ReACT

ReACT provides companies and practitioners with a standardized, methodical approach for assessing and mitigating cyber security risks. Specifically, ReACT is intended to lessen the probability that a critical event will occur, thereby lowering an organization's risk. The process is intended to approach secure cyber architecture development and risk management from an organizational perspective. Such a focus ensures that ReACT provides its users with a security model that not only protects the organization but also takes into consideration the way people use software and systems. This people-based approach ensures an effective security plan that will receive wide acceptance throughout the organization.

2. ReACT Methodology Summary

ReACT is a data organization and analysis framework that facilitates efficient aggregation and evaluation of cyber-risk related information. The results of a ReACT assessment can be used to feed existing risk management processes, ensuring cyber risk is considered equivalently to other types of risk (such as legal, financial, or regulatory risk).

After the identification of critical workflow components, the ReACT process can be broken down into three basic steps, which will be discussed in greater detail later in this document depicted in Figure 1.

1. ***Development of the Functional Overview*—**The evaluation of an organization's technology requirements including the identification of core systems and critical impact;
2. ***ReACT Assessment*—**A multi-step process which includes the development of a functional baseline and communications map, identification of existing security posture, attack surface analysis (ASA), and RCFA;
3. ***ReACT Response Plan*—**The creation of a response strategy to address issues identified during the ReACT assessment, including root cause failures.

ReACT assessments amass information about an organization's core cyber components, their functional configuration, their communication capabilities, and their existing security posture. One of the advantages of the ReACT process is the relative ease of information collection. System administration, security, and process operations already collect most of the necessary information required for a ReACT assessment.

3. Assumptions

The ReACT team worked with the DOE-OE experts on understanding the assumptions, and products prior to finalizing the methods developed. Asset owner partnerships validated these assumptions.

1. Cyber events, whether functional or security-related, affect the likelihood (or probability) of an impact occurring. Put another way, cyber security information feeds probability calculations, and not impact assessments. This means that organizations minimize enterprise risk by decreasing the probability a cyber event results in critical impact.
2. In order to calculate risk effectively, groups must understand the relationship between the likelihood a cyber event will occur and whether or not it could result in critical impact.
3. Many operations and process teams use root cause failure analysis or Quality Assurance (QA) in order to improve their reliability or increase their resiliency. However, these concepts are not commonly used by cyber security teams.
4. Businesses seek to maximize their performance through technology. Effective cyber security architecture and risk mitigation efforts need to take these business practices into account in order to be relevant to the asset owner.

4. Products of the ReACT Assessment

Standard methods and steps have been defined for the three methods identified in the ReACT methodology (Functional Overview, ReACT Assessment and ReACT Response plan). An overview of the critical workflow components is depicted in Figure 1. A detailed description of the ReACT methodology can be found in Appendix I.

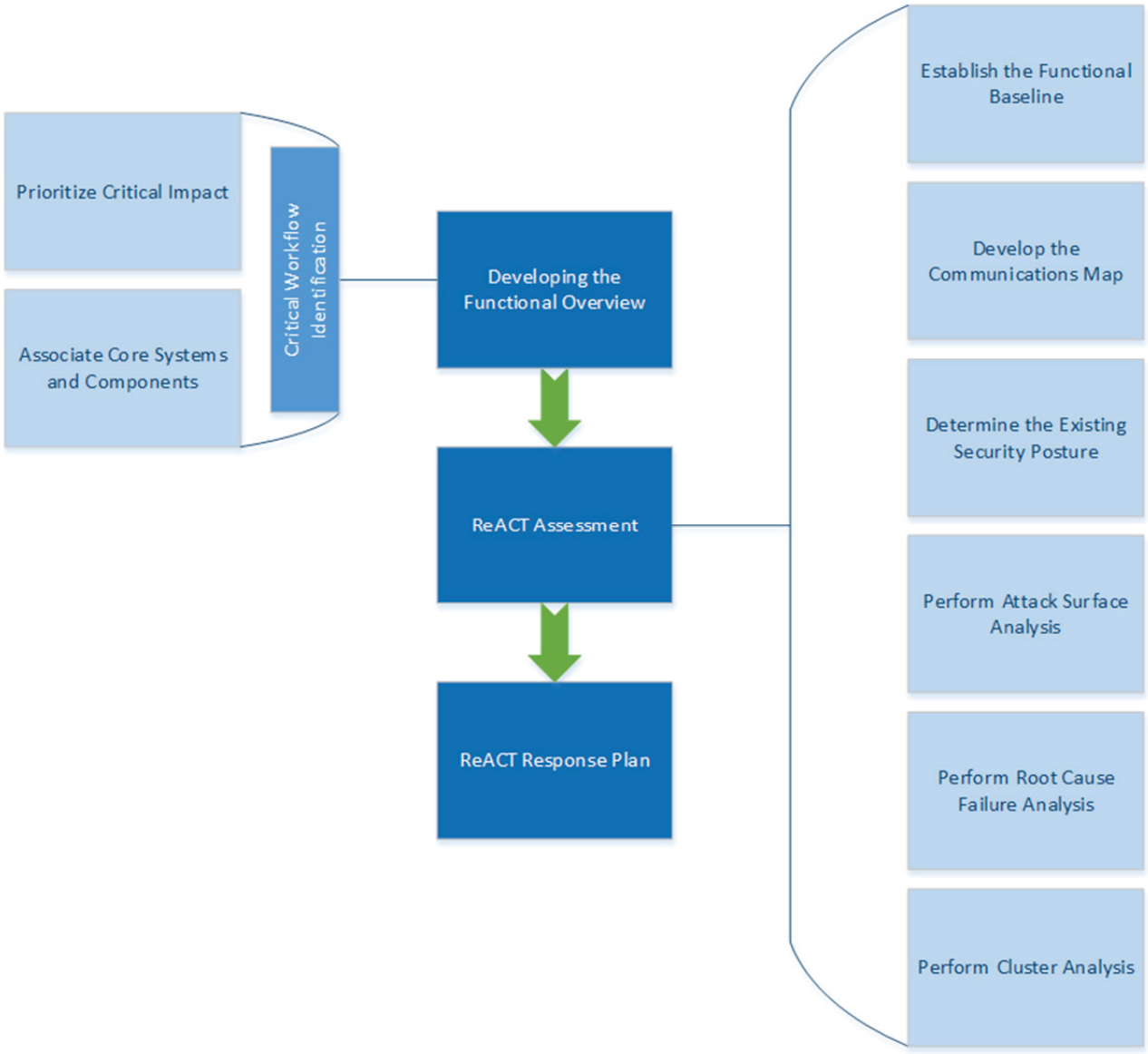


Figure 1. An overview of the ReACT process. The ReACT process can be broken down into three basic steps, included above in dark blue.

ReACT characterizations amass information about an organization's core cyber components, their functional configuration, their communication capabilities, and their existing security posture. One of the advantages of the ReACT process is the relative ease of information collection. System administration, security, and process operations already collect most of the necessary information required for a ReACT assessment.

After this information is collected, the data is organized and examined in order to generate the following products:

1. ***Functional Baseline Chart***
2. ***Communications Map***
3. ***Security Posture Analysis***
4. ***Attack Surface Analysis (ASA)***
5. ***Root Cause Failure Analysis (RCFA)***
6. ***ReACT Response Plan***

Many of the products mentioned above are incorporated into the Functional Security Matrix (FSM). The FSM is an information schema which maps relationships between different kinds of technical security data. Appendix IV includes a FSM template.

4.1 The Functional Baseline FSL Chart

The first step in a ReACT characterization is establishing the functional baseline. The functional baseline is a comprehensive software, service, and user inventory of the core systems. It is expressed in terms of the functional security layers (FSL), a fundamental component of ReACT.[1] Included in this document is an example Functional Baseline FSL Chart (Figure 2). It should be noted that the Functional Baseline FSL Chart is the second column of the FSM in Appendix IV. The organized approach included here lessens the possibility that individual components (and later on, attack vectors) will be overlooked.

[1] The FSL are simply a data schema that allows large amounts of technical data to be gathered methodically and represented in an easily-understood format. Additional information is included in Appendix II.

Functional Security Layer	**Functional Baseline**
UR&R	**Local accounts (user, service, machine)**
	Domain accounts (user, service, machine)
Network	**TCP/IP**
Firmware	**N/A**
Operating System	**Windows Server 2003 R2**
Virtualization	**N/A**
Applications	**.Net framework**
	IIS web server
	Microsoft SQL server
Cloud, hosted, or vendor services	**N/A**
Custom code	**Content Management System (CMS)**
Data & Data Stores	**N/A**

Figure 2. An example of a completed Functional Baseline FSL chart. As shown the core components being analyzed are part of the functional baseline of a fictional company's Microsoft web server on their extranet. New additions to the FSM are bolded.

Functional Security Layer	Functional Baseline	Communications Map		
		Protocol	Services	Ports
UR&R	Local accounts (user, service, machine)	**N/A**		
	Domain accounts (user, service, machine)	**N/A**		
Network	TCP/IP	**All**	**All**	**All**
Firmware	N/A			
Operating System	Windows Server 2003 R2	**TCP**	**RPC**	**135**
			RPC	**137**
			RPC	**139**
Virtualization	N/A			
Applications	.Net framework	**TCP**	**HTTP**	**80**
			HTTPS	**443**
			Alternate HTTP	**8080**
	IIS web server	**TCP**	**HTTP**	**80**
			HTTPS	**443**
			Alternate HTTP	**8080**
	Microsoft SQL server	**TCP**	**HTTP**	**80**
			HTTPS	**443**
			Alternate HTTP	**8080**
Cloud, hosted, or vendor services	N/A			
Custom code	Content Management System (CMS)	**TCP**	**HTTP**	**80**
			HTTPS	**443**
			Alternate HTTP	**8080**
Data & Data Stores	N/A			

Figure 3. An example of a Communication Map (columns on the right). Communication information regarding the ports, protocols, and applications are added to the Functional Security Matrix. Here the core component being analyzed is a fictional company's Microsoft web server on their extranet. New additions to the FSM are bolded.

4.2 Communications Map

After developing the functional baseline, analysts map the specific communication infrastructure associated with the core system. This allows for the creation of a communication map. A communication map is comprised of the following:

- Any hardware communications channels that are installed and operational;
- Known ports and services configuration; and
- Associated protocols.

The communications map, as shown in Figure 3, is an invaluable tool when performing attack surface analysis--but only when fully developed.

4.3 Security Posture Analysis

ReACT is designed to organize cyber security information and show how the existing security posture on core systems affects the company's risk. As with previous steps, existing security controls for core systems are organized in the FSM to show where the security controls are clustered. By documenting the technical security by FSL, the gaps in security become more apparent (see Figure 4).

4.4 Attack Surface Analysis (ASA)

Attack Surface Analysis (ASA) assists users with identifying areas of their system which should be tested for vulnerabilities and which require additional protection. While this information can be presented in the FSM, that is not a requirement. When performing ASA, analysts should keep in mind the preferred security baseline for each item in the FSL is at least three defensive security measures and at least two detection controls. Any deviation below the baseline is considered a gap and results in greater attack surface exposure.

There are substantial benefits to conducting attack surface analysis preemptively, as during a ReACT assessment. This allows organizations to identify any issues with their security posture prior to a costly breach or incident. Additionally, this process can help users identify when the attack surface has changed and when new assessments become necessary (see Figure 6).

Functional Security Layer	Functional Baseline	Communications Map			Existing Security Posture	
		Protocol	Services	Ports	**Existing Defensive Measures**	**Existing Detective Measures**
UR&R	Local accounts (user, service, machine)	N/A			**Guest account disabled**	**Enhanced audit policy & logging**
	Domain accounts (user, service, machine)	N/A			**No domain accounts used**	**UAC events monitored daily**
Network	TCP/IP	All	All	All	**DMZ firewall**	**Enhanced audit policy & logging**
					Network IDS	**System & security events monitored daily**
					DMZ subnet segregation	
Firmware	N/A					
Operating System	Windows Server 2003 R2	TCP	RPC	135	**Anti-virus**	**Enhanced audit policy & logging**
			RPC	137	**SDLC for operating system**	**System & security events monitored daily**
			RPC	139		
Virtualization	N/A					
Applications	.Net framework	TCP	HTTP	80	**Patches applied quarterly**	**Application & security events monitored daily**
			HTTPS	443		
			Alternate HTTP	8080		
	IIS web server	TCP	HTTP	80	**Removed sample scripts and debugging tools; Patches applied monthly**	**Enhanced audit policy & logging; Application and security events monitored daily.**
			HTTPS	443		
			Alternate HTTP	8080		
	Microsoft SQL server	TCP	HTTP	80	**Patches applied monthly**	**Application & security events monitored daily**
			HTTPS	443		
			Alternate HTTP	8080		
Cloud, hosted, or vendor services	N/A					
Custom code	Content Management System (CMS)	TCP	HTTP	80	**N/A**	**N/A**
			HTTPS	443		
			Alternate HTTP	8080		
Data & Data Stores	N/A					

Figure 4. An example of a Security Posture Analysis (located in the column on the right). The core component being analyzed is a fictional company's Microsoft web server on their extranet. New additions to the FSM are bolded.

4.5 Root Cause Failure Analysis (RCFA)

After the completion of attack surface analysis, organizations have the foundations for performing Root Cause Failure Analysis (RCFA). RCFA is a key product of the ReACT which provides groups with a starting point to improve their existing security posture. Ultimately, RCFA marks the first steps towards remediation. Included below is a short example of RCFA with regards to an input validation security issue in custom code.

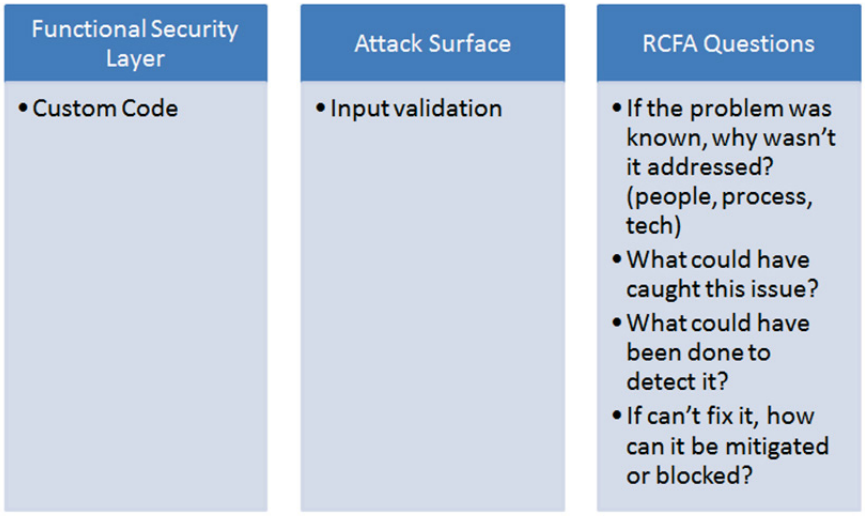


Figure 5. An example of RCFA. Here the attack surface being mitigated is an input validation issue in custom code.

4.6 ReACT Response Plan

The final product of the ReACT process is the ReACT Response Plan. This piece is intended to address specific issues identified throughout the course of the assessment, as well as any issues identified during RCFA. The ReACT Response Plan assists organizations with the development of policies that will prevent security breaches going forward. In order to be successful, a ReACT Response Plan should bear in mind an attacker's workflow. Attackers require a vulnerability, exploit code, and attack path. Limiting access to even one of these components will lessen an organizations attack surface.

5. Results and Discussion - ReACT Case Study

As part of the ReACT proof of concept project, the INL team conducted an onsite assessment with an industry partner. This case study was intended to prove value added for industry going forward. In particular, asset owners expressed their appreciation for the organized, methodical approach of ReACT, which limited subjectivity in the development of effective security postures. Additionally, this assessment assisted with the development of a more complete ReACT methodology. Finally, the feedback from the industry partner will help to shape the next steps for the ReACT project.

5.1 Summary of Case Study at Industry Partner Site

INL researchers conducted an onsite assessment with a large energy utility company. The purpose of this visit was to further develop the ReACT process as well as gather invaluable feedback from industry partners. Onsite work was conducted over three and a half business days. However, the timeframe for the ReACT process is highly variable and dependent on a number of different factors including an organization's threat assessment capabilities, an organization's existing security posture, the complexity of the core system being analyzed, and an analyst's current knowledge of the core system. Wherever possible this summary includes time estimations for future assessments.

During this onsite, INL researchers conducted several meetings with parties familiar with both the business goals and the functional requirements of the core system selected (the Energy Management System (EMS)).[2] Industry partner participants included representatives from the following groups: IT management, EMS management, network operations, and the security operations center.

INL researchers conducted initial meetings in order to introduce the ReACT and ATAC process to the industry partner. These meetings were also used to determine the time commitments of key individuals during the week. Additionally, INL researchers used this time to direct a group discussion to define critical impact based on the organization's business and mission goals. During the case study, these meetings were relatively brief (1-2 hrs.). However, these meetings become less critical when conducting in-house assessments.

Several meetings conducted in the first two days focused on developing a detailed understanding of the functionality and operations of the EMS. In essence, this work focused on gathering the necessary information to develop the functional baseline. These meetings were orchestrated by the industry partner for the benefit of INL researchers (2-3 hrs.). However, when conducting an in-house assessment, these meetings may become unnecessary. In many cases, an analyst may have sufficient knowledge of the system or be able to access internal documentation to develop the functional baseline independently. While these meetings can be limited, it is advisable that an analyst still budget 2-3 hours for the development of the functional baseline. This is because the ReACT assessment is most successful as part of a collaborative effort to identify technology needs and functionality.

During the onsite assessment, one full day was devoted to developing the communications maps and gathering existing security posture information (~8 hrs.). The collection of communication and security posture information provides asset owners with the data necessary to perform ASA. INL researchers also used time during the meetings to develop a list of critical components, services, and data for use during the ATAC evaluation. The length of these meetings was primarily dictated by the complexity of the EMS. An in-house analyst more familiar with this system may have been able to limit this component to a half-day (~4 hrs.), but some additional meeting requirements are likely. This is due not only to the complexity of the system, but also the dependent relationships between the EMS and other management

[2] In this case the core system was selected prior to onsite meeting. Through teleconferences and discussions, the industry partner-led group selected the Energy Management System (EMS).

Functional Security Layer	Functional Baseline	Communications Map			Existing Security Posture		Gap Analysis
		Protocol	Services	Ports	Existing Defensive Measures	Existing Detective Measures	
UR&R	Local accounts (user, service, machine)	N/A			Guest account disabled	Enhanced audit policy & logging	**Missing one defensive measure.**
	Domain accounts (user, service, machine)	N/A			No domain accounts used	UAC events monitored daily	
Network	TCP/IP	All	All	All	DMZ firewall	Enhanced audit policy & logging	**No gaps**
					Network IDS	System & security events monitored daily	
					DMZ subnet segregation		
Firmware	N/A						
Operating System	Windows Server 2003 R2	TCP	RPC	135	Anti-virus	Enhanced audit policy & logging	**Missing 1 defensive measure.**
			RPC	137	SDLC for operating system	System & security events monitored daily	
			RPC	139			
Virtualization	N/A						
Applications	.Net framework	TCP	HTTP	80	Patches applied quarterly	Application & security events monitored daily	**Missing 2 defensive measures; Missing 1 detection measure.**
			HTTPS	443			
			Alternate HTTP	8080			
	IIS web server	TCP	HTTP	80	Removed sample scripts and debugging tools; Patches applied monthly	Enhanced audit policy & logging; Application and security events monitored daily.	**Missing 1 defensive measure.**
			HTTPS	443			
			Alternate HTTP	8080			
	Microsoft SQL server	TCP	HTTP	80	Patches applied monthly	Application & security events monitored daily	**Missing 2 defensive measures; Missing 1 detection measure.**
			HTTPS	443			
			Alternate HTTP	8080			
Cloud, hosted, or vendor services	N/A						
Custom code	Content Management System (CMS)	TCP	HTTP	80	N/A	N/A	**Missing 3 defensive measures; missing 2 detection measures.**
			HTTPS	443			
			Alternate HTTP	8080			
Data & Data Stores	N/A						

Figure 6. The Functional Security Matrix with Gap Analysis (bolded in the far right).

systems. It is unlikely that an analyst would independently have access to all the communication and security information necessary to complete this section of the assessment.

Following the completion of the onsite, INL researchers conducted ASA, RCFA, and cluster analysis on the EMS. This part of the process took approximately four hours, but it is likely the most difficult for industry to complete. In particular, ASA is the most intensive, and is based on experience (for the advanced user) or research (for the less experienced user). Likely time requirements for this process are six to twelve hours, but more in depth analysis may take up to forty hours. ASA, RCFA, and cluster analysis provide asset owners with key system information which feeds a ReACT Response Plan.

5.2 Feedback Summary

The industry partners provided the following feedback:

- Development of detailed and extensive instructions would assist with the training of onsite teams by industry.
- Future ReACT training materials should include a basic and an advanced user option. This would allow the process to have wider adoption by industry regardless of the level of sophistication of their security team.
- Creation of an automated process would allow for easier adoption by industry. This kind of arrangement is more feasible than most given the low degree of subjectivity in this process.

5.3 Lessons Learned

During the course of the onsite, INL researchers identified the following lessons learned:

- The industry partner used for the onsite assessment maintains a highly sophisticated security posture, and is exceptionally capable in their information gathering methods. Given this reality, additional case studies will have to be conducted in order to further develop the ReACT process. For example, INL suggests conducting a case study with organizations which have fewer resources (i.e. smaller utility). This will add value for the broader community.
- The current method for organizing communication data should be further developed in order to make it more consumable by analysts.

5.4 Resources Required

In order to effectively employ the ReACT methodology, an analyst will need to have access to substantial information regarding the core system.[3] Since the first steps of the ReACT process rely on the gathering of this information, the only preparation necessary is the identification of where this information can be found. Unfortunately, the needs of the analyst will vary from organization to organization. For example, some groups may keep a central database with detailed information regarding the core system. In this case, the analyst will be able to amass substantial data independently. However, if the core system is exceptionally complex (or if such a database does not exist) then an analyst will have to conduct interviews with various teams. There is no easy response to answer the question of who needs to be involved, as this answer will also vary from organization to organization. However, likely

[3] Examples of the information necessary include applications and services on the core system, key data stores for work, any connections to the system (neighboring databases, subsystems, etc.), and ingress and egress traffic (inter- and intranet).

participants include members of the core system management, IT management, network operations, and the security operations center.

5.5 Potential Applications

Regardless of the sophistication of the user group, the ReACT methodology offers a tool for the organization of core system information including subcomponents and existing security controls. Even for the inexperienced user, this dissection of security information by FSL makes root cause failures readily apparent. This will allow the users to begin the process of amending root cause failures through the development of a ReACT Response plan. More sophisticated groups can then use the information gathered from the ReACT assessment for the ATAC process.

6. Going Forward

Based on their experiences during the ReACT proof of concept project, INL researchers developed this section to describe and explore the current barriers for wide-scale adoption of the ReACT methodology.

6.1 Next Steps

The primary goal of the proof of concept was to use ReACT in a real-time application format at an industry onsite. Through this collaboration with industry, INL identified several areas which should be further developed as the ReACT process progresses:

- **Conduct additional case studies:** As mentioned in the lessons learned section of this document, additional case studies are necessary in order to better define the ReACT methodology. This remains INL's primary recommendation moving forward. In particular, additional case studies should be carried out among industry partners with differing levels of cyber security capabilities. Examples of recommended case studies would also involve a small, medium, and large utility.
- **Development of detailed training materials**: Moving forward, research should be directed at compiling the materials necessary for training individuals and teams about how to apply the ReACT framework most effectively. The industry partner expressed the importance of developing materials for beginner, intermediate, and advanced users. This will ensure that a broad spectrum of organizations is able to use this methodology.
- **Development of a security controls catalogue**: Through the course of this proof of concept project, INL researchers have become aware of the need for a defensive controls catalogue. This document, developed overtime, would include mitigation strategies organized by attack type. This document would assist less experienced teams with the mitigation of critical failures identified during a ReACT assessment.
- **Creation of an automated process**: Given that ReACT is an objective process, aspects of the process could be automated with relative ease. This would lower the amount of training necessary to conduct a ReACT assessment.

7. Conclusions

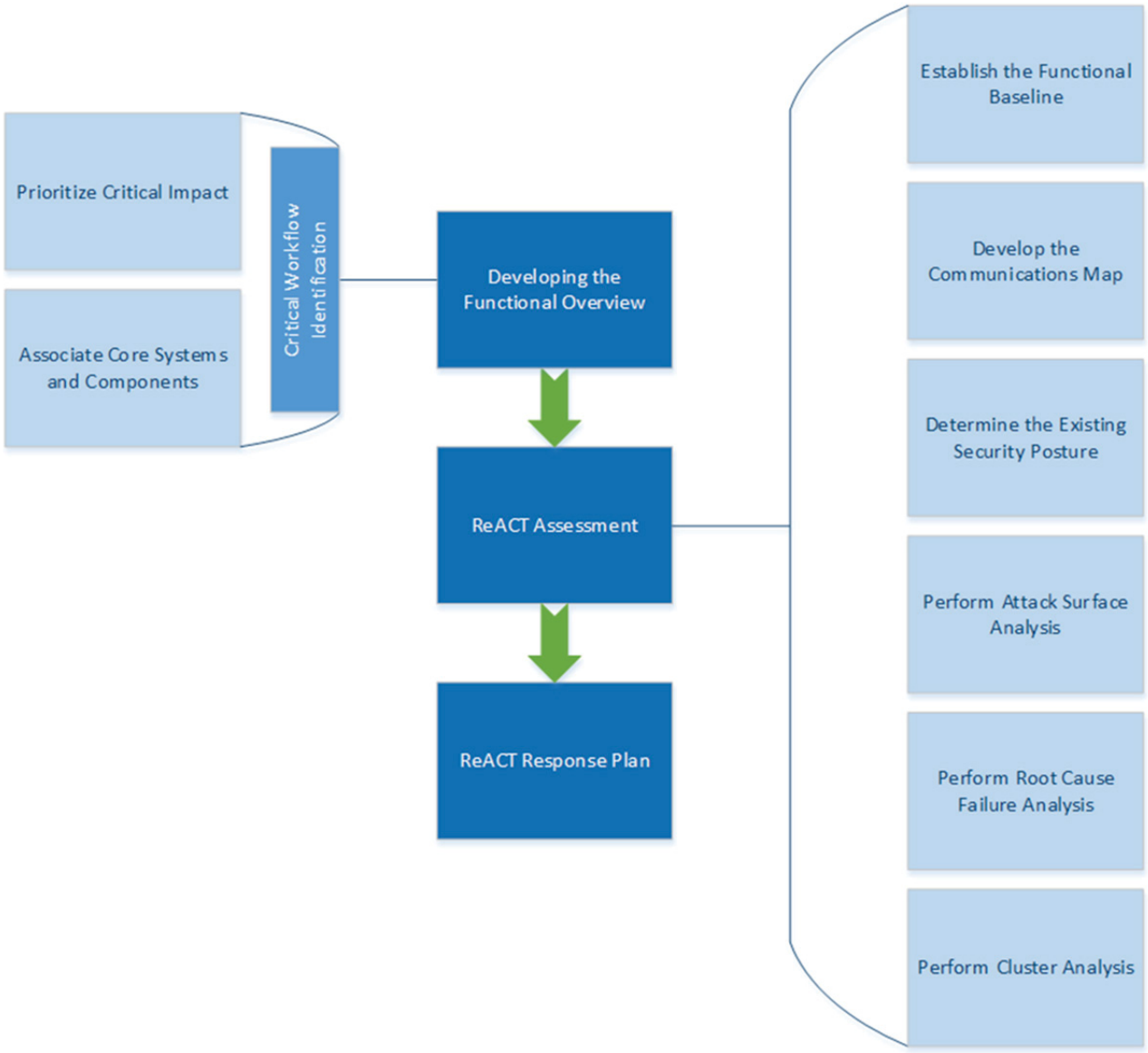
INL has succeeded in developing a methodology which benefits industry users by providing an organized, methodical approach for cyber security based on the FSL. This, in turn, aids these groups in the efficient and effective consumption of threat intelligence.

The ReACT proof of concept project had several challenges to overcome. First and foremost among these was the development of a method which met the needs of (and would continue to meet the needs of industry members. To this end, ReACT was vetted with an industry partner during an onsite assessment. Following the onsite assessment, ReACT received substantial positive feedback regarding its potential usefulness for asset owners.

The proof of concept sought to develop a basic methodology for the use of this tool by industry. This was accomplished through collaboration with industry partners and INL researchers. While the proof of concept project proved ReACT's potential usefulness to industry, it also identified many items that will need to be further developed and tested prior to wide industry adoption. INL has developed suggestions for the next steps for ReACT deployment.

Appendix I – ReACT Methodology

This section describes the current ReACT methodology developed as a result of the proof of concept project. As depicted below, there are three basic steps for the ReACT methodology, the development of the functional overview, the ReACT assessment, and the ReACT Response Plan. These processes are described below.



An overview of the ReACT process. The ReACT process can be broken down into three basic steps, included above in dark blue.

Developing the Functional Overview

Step 1. Identify Critical Impact and Prioritize Core Systems, Components, and Cyber Resources

The development of the functional overview is a precursor to the ReACT assessment. While a number of different risk assessment models can be used, the industry partner chose the Impact Driven Risk Analysis

(IDRA) model to identify critical impact and prioritize systems during the onsite case study. The IDRA model identifies core systems based on the ability an adversary would have if the systems were breached.

In order to respond to operational risk, which is measured in terms of Risk = f (Probability, Impact), both probability and impact need to be measured. In this section, critical impact is identified by the business unit and cyber resources that could—if the business were denied total access to them—result in catastrophic or critical failure.

The steps for identifying critical impact and prioritizing affiliated cyber resources are as follows:

1. Define critical impact for energy management system.
    a. Identify operations or process impact the organization can't sustain.
    b. Prioritize impacts in order of importance.
2. Identify top 3-5 systems that would allow critical impact to occur if they were to become entirely unavailable for use regardless of the source of disruption.
    a. Prioritize systems in order of importance vis-à-vis critical impact.
    b. Ascertain the order of importance of the security goals for each cyber resource, availability, integrity, and confidentiality. [4]
3. Have organizational stakeholders review and approve the impact and cyber resource prioritizations in order to ensure impact assessments and affiliated cyber resources align with the organization's risk perceptions. Key data points include:
    a. Impact value to organization;
    b. Critical cyber resources associated with impact;
    c. Prioritization of cyber resources; and,
    d. Prioritization of security impacts for each cyber resource.

Performing a ReACT Assessment

The initial steps of a ReACT assessment bring all of the technical cyber security data together. This information is then used to evaluate the probability of critical impact should an important cyber resource be breached. Each cyber resource in a ReACT assessment is evaluated using the Attack Surface Analysis (ASA), the Functional Security Layers (FSL), and the Functional Security Matrix (FSM). Root cause failure or cluster analysis can be performed after ASA is completed to pinpoint where and why security gaps exist.

Step 1a. Determining the User Value of Cyber Resources

The functional baseline expresses the relationship between how a company is organized and how technology is used to solve business problems. For each core system or critical cyber resource, the functional baseline takes into account two distinct aspects:

1. The value of a functionality, and how it allows people to work more effectively toward business goals (i.e. how technology enhances people's ability to work); and,
2. The role of a critical cyber resource's technical configuration plays in work flow (i.e. what technology is deployed and why it was deployed that way).

[4] "Understanding The Security Triad (Confidentiality, Integrity, and Availability)," *PEARSON,* accessed March 11, 2014, http://www.pearsonitcertification.com/articles/article.aspx?p=1708668

The first is an optional component, which helps technical security and risk management teams demonstrate how cyber security risk directly affects business. The second is one of the three tasks required to perform ASA.

The first component of the functional baseline is not technical in nature. However, this component provides useful context for understanding the root cause failure and cluster analysis which are performed later. This context allows for the development of more effective risk management and technical security decisions. The steps for identifying which applications, services, systems, or data sets are most important to cyber resource stakeholders are outlined below:

1. Establish functional value for each critical cyber resource in order to determine which individual components of each cyber resource are most important, and which will be used during later response planning to determine what security defenses and detection methods will be most effective.
    a. Ask end users to:
        i. Name what tasks or work they perform on each of the critical cyber resources; and,
        ii. Describe why the applications, services, or data they administer is important to the cyber resource's functionality.
2. Rank the order of importance for each application, service, or data set based on end user needs by performing the following steps.
    a. Ask operational technology (OT) team to:
        i. Name what applications, services, or data they administer on each critical cyber resource;
        ii. Describe why the applications, services, or data they administer is important to the functionality identified by the end users; and,
        iii. Prioritize order of importance for each application, service, or data set based on OT team's input
    b. Ask Information Technology (IT) and network management team to:
        i. Name what applications, services, or data they administer on each critical cyber resource;
        ii. Describe why the applications, services, or data they administer is important to the functionality identified by the end users and administrative needs expressed by the OT team; and,
        iii. Prioritize order of importance for each application, service, or data set based on IT and network management team's input.
3. Ask security operations team to:
    a. Name what applications, services, or data they administer on each critical cyber resource;
    b. Describe why the applications, services, or data they administer is important to the functionality identified by the end users and administrative needs expressed by the OT, IT, and network management teams; and,
    c. Prioritize order of importance for each application, service, or data set based on security operation's team input.

4. Roll up functional use case data for each of the stakeholder teams into an aggregated ranking of each cyber resource to serve as the master ranking for each component of the cyber resource. To do so, the following tasks must be performed.
    a. Prioritize application, service, and data value for critical cyber resource.
    b. Perform a stakeholder review of the aggregated findings and approve the functional use case prioritization.
    c. Share the aggregated functional use case with all stakeholders to verify it represents their perspective.

Step 1b. Developing the Functional Baseline of Cyber Resources

The second component of the functional baseline is required to perform ASA. As discussed previously, an adversary must be able to deliver exploit code specific to a vulnerability on the target system over a communications path the vulnerable software uses. Developing a functional baseline of the cyber resources gives defenders a clear understanding of where vulnerabilities can and do exist on the target system.

In this step, the technical configuration of critical cyber resources is broken out into an FSL chart. Doing so allows the disparate types and sources of information regarding the resource to be gathered together in an easily understandable fashion. The steps for gathering the technical configuration data of critical cyber resources are delineated below:

1. Inventory the software on each critical cyber resource. Some of the most common means of doing so include but are not limited to:
    a. Reviewing the operating system inventory of installed programs;
    b. Using a 3rd party software inventory tool if possible; or,
    c. Performing passive scans of the resource to fingerprint the basic system configuration.
2. Inventory the user accounts on each critical cyber resource.
    a. Review the local accounts on each critical cyber resource. Note the
        i. Status of each account (active, disabled);
        ii. Type of account (local, domain);
        iii. Whether it is a computer, service, application, or user account; and,
        iv. What permissions each account has (administrator, user, special, or guest).
    b. Compare the list of accounts to the functional use case data to determine whether or not any of the accounts are extraneous or operating with unnecessarily enhanced permissions.
3. Break the software inventory list out an FSL table. At minimum, the inventory should contain the version and update status of the:
    a. Firmware;
    b. Operating system (OS);
    c. Virtualization software (if installed);
    d. Applications (3rd party, COTS, or GPL/GNU); and,
    e. Proprietary software and its dependencies.
4. Verify the software installation, version, and update status with any 2 of the following (if possible):
    a. 3rd party software asset management application;
    b. OS inventory script or native OS tools that inventory software on the system;

c. Network scans for open ports and services (NMap)[5]; or,
d. Vulnerability scans of cyber resource using administrator credentials.

Step 2. Developing Communications Map

Following the development of the functional baseline, users must develop the communication map. The communication map describes the ports, services, and protocols used for network communications on the target system. In order to be successful, adversary requires not only vulnerability-specific exploit code but also having a means of delivery. Developing a communications map of the cyber resources allows defenders to see what attack paths are open to an adversary.
In this step, the communications paths are added to the FSL chart created for the functional baseline. Doing so allows the disparate types and sources of information regarding the resource to be gathered together in an easily understandable fashion.

The steps for mapping the communications paths of critical cyber resources are described below:

1. Perform an inventory of all physical communications components on each critical cyber resource, noting the status of each (enabled, disabled).
2. Gather host-based data regarding the normal ports and services running on each cyber resource.
    a. Reviewing network statistics (netstat) data from operating system;
    b. Recording the ports and services open on the system throughout the week;
    c. Performing a network scan (if possible) to confirm the open ports and services; and,
    d. Comparing all of the host-based ports and services configuration data to identify any anomalies with what was expected and what is actually available on the host.
3. Gather network-based data regarding the normal ports and protocols used by each cyber resource.
    a. Capture ingress and egress traffic with a packet capture tool (WireShark) for 1-2 hours at varied periods of time a minimum of 4 times.
    b. Note ingress and egress network traffic patterns and track expected communications by:
        i. Source IP or MAC address;
        ii. Destination IP or MAC address;
        iii. Protocol used to communicate;
        iv. Port and service used for communications; and,
        v. Any errors resulting from the communications.
4. Record the ports, services, and protocols from the network traffic baseline in the FSL chart.

Step 3. Determine Existing Security Posture

The final step necessary prior to performing ASA is to characterize existing defenses for each critical cyber resource. Collecting all of the defensive and detection measures in place for a cyber resource reveals where attack surface is exposed to an attacker. As discussed previously, a defender can minimize the probability of a successful attack by affecting the attacker's ability to access the attack path or utilize an exploit and vulnerability.

[5] Additional information regarding *Nmap* can be found at: http://nmap.org/

In this step, analysts should expand upon the FSM. The defensive and detection controls are separated and added in individual columns under the "Existing Security Posture" master column.[6] The steps for mapping the existing security posture measures for critical cyber resources are described below:

1. Identify any outdated software and what FSL it is located in.
2. Note outdated software findings on both the ReACT Defensive and Detection FSM.
3. Identify any known vulnerabilities for each piece of software on the cyber resource by:
    a. Performing a vulnerability scan with administrative privilege (if possible); and,
    b. Researching known vulnerabilities available for each piece of software loaded.
4. Note known vulnerability findings on both the ReACT Defensive and Detection FSM.
5. Assign a vulnerability score using the organization's existing vulnerability ranking system or the CVSS[7] based on the:
    a. Number of outdated software packages, and
    b. Severity of known vulnerabilities.
6. Gather a list the defensive measures in place for each layer of the FSL and record it in the ReACT Defensive FSM.
7. Gather a list the detection measures in place for each layer of the FSL and record the detection measures in the ReACT Detection FSM.

Step 4. Ascertain Risk Probability by Performing Attack Surface Analysis

In 2003, Michael Howard of Microsoft introduced the concept of attack surface (AS), or the combined exposure of code, interfaces, services, protocols, and practices which are available to all users and to unauthenticated users.[8] Both the ReACT and ATAC consider the attack surface of cyber architecture, including systems, applications, complex software environments, and data stores. After conducting ASA, teams can begin developing ReACT Response Plans which reduce attack surface.

Prior to conducting ASA, groups need to amass the following information (collected during the preceding steps of this procedure):

1. Construct a functional baseline of the target systems, network, or cyber resources in order to determine what type of vulnerabilities exist and where they are located.
2. Develop a communications map to identify any possible attack paths that could be used by the attacker to deliver exploits to the target system.
3. Determine what the existing security posture is for the target system.

At this point, the analyst should have enough information to conduct an ASA (also known as gap analysis) on the core system. In ReACT, the preferred security baseline for each item in the FSL is at least three defensive security measures and at least two detection controls.[9] Any deviation below the baseline is considered a gap and results in greater attack surface exposure. Existing defenses and

---

[6] It is generally easiest to make two FSMs for cyber resources, one that maps detection measures and one that maps defensive controls. For less complex systems, one will be sufficient.

[7] Additional information regarding CVSS vulnerability scoring can be found at: http://nvd.nist.gov/cvss.cfm

[8] Michael Howard, "Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users," *MSDN Magazine*, accessed March 13, 2014, http://msdn.microsoft.com/en-us/magazine/cc163882.aspx. In 2003, Michael Howard also introduced the concept of attack surface reduction (ASR). ASR is based on the concept that there is a zero percent likelihood that code will exist without one or more vulnerabilities. Based on that perspective, ASR represents the compromise between complete safety (an environment with no code) and unmitigated risk, the goal of which is to limit the code exposed to untrusted users.

[9] It should be noted that the security baseline requirements (the number of detective and defensive security measures) may vary from organization to organization, based on the each group's risk tolerance.

detections can be recorded in the corresponding ASA column of the FSM. Gaps should also be noted in some fashion, for example highlighting the areas where gaps exist (see diagram below). Users then assign an ASA value to the gap using organizational risk analysis valuation techniques.

Step 5. Performing Root Cause Failure and Cluster Analysis

Once the attack surface has been identified for each cyber resource, root cause failure (RCFA) or cluster analysis can be performed for each layer of the FSL. Both RCFA and cluster analysis focus on where and why security gaps exist. Each gap or issue identified in the ASA is evaluated in terms of the Functional Security Matrix (FSM).

Step 5a. Performing Root Cause Failure Analysis

RCFA is performed after the ReACT assessment has been completed. RCFA is used to determine what the most effective security measures would be for reducing the attack surface of a critical cyber resource given its functional use case and technical configuration.

RCFA should be performed any place the existing security posture does not meet the minimum security requirements for attack surface reduction. RCFA is performed by completing all of the following steps. In ReACT, a minimum of 3 defensive measures and 2 detection measures are recommended for each FSL. Any variant from this baseline either increases or reduces the exposed attack surface, thereby increasing or decreasing the probability of a successful cyber attack occurring.

1. Review the ReACT FSM for each cyber resource.
2. Identify any layer of the FSL that does not have 3 defensive security measures in place.
    a. Develop a list of recommended or potential defensive measures that could be implemented.
    b. Note which stage of the SDLC, design, implementation, maintenance, or end-of-life, these would be incorporated in.
3. Identify any layer of the FSL that does not have 2 detection measures in place.
    a. Develop a list of recommended or potential detection measures that could be implemented.
    b. Note which stage of the SDLC, design, implementation, maintenance, or end-of-life, these would be incorporated in.
4. Compare and contrast the list of recommended or potential security measures (defensive and detection) with the existing security posture of each critical cyber resource.
5. Prioritize which gaps in potential versus existing security posture result in the most attack surface exposure.
6. Create a list of security measures (defensive, detection) could be incorporated to reduce the attack surface for each FSL.
7. Perform RCFA with stakeholders to determine why existing security posture is not sufficiently reducing exposed attack surface.
    a. Review gap analysis results and potential defensive measures.
    b. Determine what—if any--factors have limited or prevented the recommended or potential security measures from being put in place.
    c. Establish the RCF for each factor that limits or prevents the security measures from being implemented
8. Characterize the origin of the root cause failure.

a. Note the FSL in which the RCF originates.
b. Note whether the RCF originates from an issue with an organization (people), a process (work flow), or the technology deployment itself.
c. Isolate the SDLC stage (DIME) in which the RCF originates.

9. Decide which security measures need to be implemented based on the results of the:
    a. Functional use case;
    b. Technical configuration of the critical cyber resource; and,
    c. RCFA.

Step 5b. Performing Cluster Analysis

An optional step, performed in conjunction with Root Cause Failure Analysis, cluster analysis is a breakdown of the root cause failures in order to determine if an organization has a systemic failure or cluster of failures in one aspect of DIME or the Organizational Hierarchy. For example, consistent RCFA indicators in the design stage of an application roll-out may indicate a systemic failure in the way business requirements are used to select or design technology. Cluster analysis is also used to determine if the people, process, or technology sub-components of the FSL contribute to repetitive failures.

Cluster Analysis assists organizations with the identification of key issues, which typically indicate technical security measures will not resolve the RCFs. Rather, clusters of RCFs across a single FSL, origin, or SDLC stage generally mean multiple business units contribute to the origin of the RCF cluster and will require each of the business units to participate in a risk management plan.

Cluster analysis results from several cyber resources are compared in order to determine whether or not RCFs are occurring across the enterprise or are restricted to only a few critical cyber resources.

1. Review the RCF origins from the RCFA reports for critical cyber resources.
2. Compare the RCF origins across the cyber resources.
3. Perform cluster analysis to identify areas in which RCFs cluster across a:
    a. Single Functional Security Layer,
    b. Type of security measure (defensive or detection),
    c. RCF origin (people, process, or technology), or
    d. Single stage of the Software/System Development Life Cycle.
4. Determine whether clusters of RCFs affect the organization's cyber security risk and require a business process improvement plan to resolve.

Developing the ReACT Response Plan

The final step of the ReACT methodology is the development of a ReACT Response Plan. This step is intended to make the necessary changes to the security plans in order to reduce attack surface, correct any root cause failures, and address any gaps. Included below is a general strategy for the development of a ReACT Response Plan:

1. Review ReACT Defensive FSM for each cyber resource for FSL layers that do not have at least three defensive controls in each of the four SDLC life cycle stages. Add additional controls as necessary.
2. Review ReACT Detection FSM for each cyber resource for FSL layers that do not have at least detection controls in each of the four SDLC life cycle stages. Add additional controls as necessary.

When developing a ReACT Response Plan it is helpful to keep in mind the goals of an adversary. The primary goal of any adversary is the execution of remote arbitrary code and the elevation of privileges from unauthorized or limited access to administrative. In order to be successful, an adversaries attack requires three basic requirements:

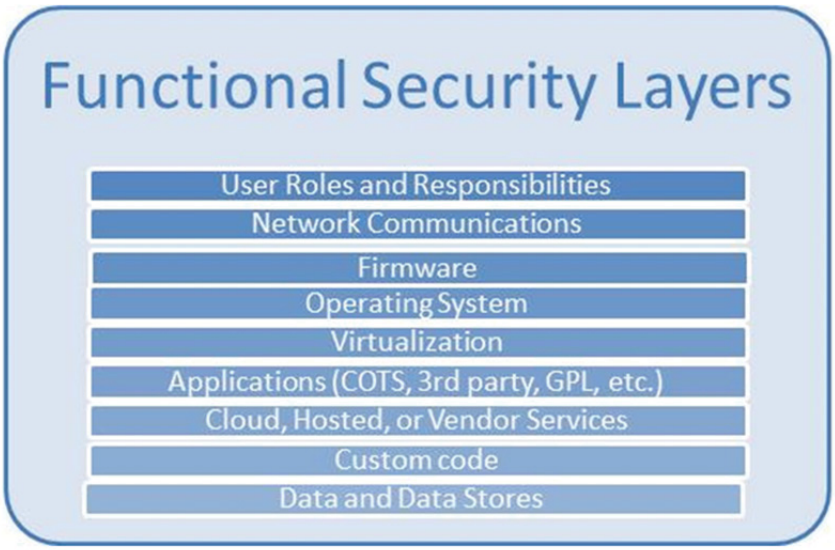
- A vulnerability (CVE) or weakness (CWE) on the target system;
- An exploit code specific to the vulnerability; and,
- An attack path.

A defender only needs to limit an adversary's ability to use one of these three components. This technique of limiting the attacker's access to required resources is referred to as attack surface reduction. By reducing the attack surface, the defender accomplishes the following:

1. Attack surface is reduced, minimizing the number of ways an attacker could compromise the target system.
2. The probability of a successful attack occurring on a target system or resource is reduced because the adversary's options for running an attack have been decreased.
3. Enterprise risk is lowered because the probability of a successful breach via cyber means has declined.

Appendix II – Explanation of the Functional Security Layers

The functional security layers (FSL) are a fundamental component of ReACT. The FSL tool is simply a data schema that allows large amounts of technical data to be gathered methodically and represented in an easily-understood format.



The advantage of evaluating core systems (and their technology) according to FSL is that individual components and attack vectors are less likely to be overlooked. If information regarding core systems' components or existing security posture is not gathered, security issues may not be recognized during the ReACT process. Failure to identify those issues may provide an opening for an attacker, thereby increasing an organization's risk exposure.

Appendix III – Explanation of Heat Maps

An optional product of the ReACT process, a heat map is a visual representation of the cyber risk an organization faces.[10] For the ReACT process, components are graphed along two axes, Impact (the vertical axis) and Probability (typically the horizontal axis) In many cases, these heat maps are color coded, with a typical display moving from green to yellow to red (as shown in the example heat map below). These visualizations clearly display areas of concern, which cluster near the upper right corner.

Included below is a theoretical example of a heat map for an energy utility company. The critical impact being graphed is a power outage of greater than 48 hours for a significant geographic region. Impact is defined in terms of the severity of an event, with critical impact (as defined above) representing the upper right quadrant. Probability is defined as the likelihood that an event causing critical impact will occur.

[10] Heat maps are also known as risk maps.

Appendix IV – ReACT Functional Security Matrix

Functional Security Layer	Functional Baseline of Target	Communications Map			Attack Surface Analysis		
					Existing Security Posture		Gap Analysis
		Protocol	Services	Ports	Existing Defensive Measures	Existing Detective Measures	
UR&R							
Network							
Firmware							
Operating System							
Virtualization							
Applications							
Cloud, hosted, or vendor services							
Custom code							
Data & Data Stores							

ReACT Response Plan Matrix (Defensive or Detection)

Functional Security Layer	ReACT Response Plan *(Defensive or Detection)*			
	Design	Implementation	Maintenance	End of Life (EoL)
UR&R				
Network				
Firmware				
Operating System				
Virtualization				
Applications				
Cloud, hosted, or vendor services				
Custom code				
Data & Data Stores				

Bibliography

Howard, Michael. “Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users.” *MSDN Magazine*. http://msdn.microsoft.com/en-us/magazine/cc163882.aspx.

[1] PEARSON. “Understanding The Security Triad (Confidentiality, Integrity, and Availability).” Accessed March 11, 2014. http://www.pearsonitcertification.com/articles/article.aspx?p=1708668.

ATAC and ReACT Data Definitions

Advanced Persistent Threat (APT):

A group with the intent, means, and capability to sustain a long-term attack against an adversary.

Attack Technology, Analysis and Characterization (ATAC) tool:

A process by which individuals or organization can methodically characterize threats and develop technical response plans to manage cyber risk presented by threats.

Applications:

One of the Functional Security Layers (FSL), applications refers to any commercial off-the-shelf (COTS) applications that are default applications which come with a system or those loaded onto a system by users. Unlike custom or proprietary software, the source code of the application is NOT owned or managed by the core system owner. Examples of applications include remote server management, internet browser, database, media player, or web server software.

ATAC Lifecycle:

A lifecycle model that characterizes the stages of an attack into four stages: Target Development, Exploitation and Pivoting, Attack Operations, and Attack End-of-Life. In order to execute a successful attack, an adversary must perform all these stages, although the steps necessary to meet goals at each stage may vary from attack to attack. The ATAC Life Cycle mirrors the Software/System Development Life Cycle, but it represents how an attacker or attack team must manage the work flow and planning associated with an attack.

Attack End-of-Life (EoL):

The final stage of the ATAC Lifecycle during which the operational goals of an adversary are met. In the Attack EoL, technical work is peripheral to achieving strategic goals like data exfiltration, etc.

Attack Operations:

The third stage of the ATAC Lifecycle which occurs after an adversary has gained entry to a network. In this stage, the adversary establishes a foothold on the network that allows him to manage compromised systems remotely, establish command and control communications (C&C), or perform evasive maneuvers to escape detection. He or she will also begin identifying target systems, information, and credentials necessary to meet their operational goals.

attack methodology:

The combination of attack technology and techniques employed by an attacker in order to gain unsanctioned access to or to compromise a system. Attack methodology tends to be unique to an individual or team because the selection of specific tools, techniques, and methodologies combined to perform an attack will vary based on the adversary's or team's skills, preferences, and work flow management.

Attack Path:

The combination of network protocols, host-based ports and services, and physical communications components used by an adversary to deliver an exploit for initial access, upload payloads to compromised systems, or to manage C&C networks.

Attack Path Modeling:

The third piece of Simple Threat Analysis, attack path modeling is the process by which analysts identify the attack paths of high value targets and associate them with likely attack techniques.

Attack Surface:

The attack surface of a system is the combination of exposed attack paths which can be used to compromise a system.

Attack Surface Analysis (ASA):

An analytical process which involves evaluating the exposure of an application, system, or network to attack vis-à-vis a comparison of its base technology build, available attack paths, existing security posture, and known attack methodology. Simply put, attack surface analysis is determining the gap between what is well protected and what is not. Versions of attack surface analysis are conducted during both the ATAC and ReACT processes.

Attack Technique:

The type of attack used to perform key tasks like Elevation of Privilege (EoP)during the attack but not specific to a specific attack technology. Example attack techniques include SQL injection, heap spraying, reverse proxy communications, C&C beaconing, etc. and do not refer to specific pieces of malware or exploit code used in attacks.

Attack Technology:

The actual technology used to perform an attack or attack operations. Attack technology refers to the specific toolkits, payloads, and exploits code employed by an attacker to gain unsanctioned access to or to compromise a system.

Attack Timeline:

A chronological listing of the various events of a previous attack which includes information about how an adversary moves within a compromised system or network, the delivery date of the payload, and any changes to the system or network. May be represented on a standard timeline or through functional use at certain stages of ATAC Lifecycle.

Attack Timeline (or Order of Operations) Development:

The first step of Complex Threat Analysis concerned with determining the order of adversary actions and movements within a system or network. When chronicling a past attack, this step involves the creation of an attack timeline; however, when evaluating potential attacks, this step focuses on the attack workflow with an order of operations.

Cluster Analysis:

An optional step, performed in conjunction with Root Cause Failure Analysis, cluster analysis is a breakdown of the root cause failures in order to determine if an organization has a systemic failure, or cluster of failures in one aspect of DIME or the Organizational Hierarchy. For example, consistent RCFA indicators in the design stage of an application roll-out may indicate a systemic failure in the way business requirements are used to select or design technology. Cluster analysis is also used to determine if the people, process, or technology sub-components of the FSL contribute to repetitive failures.

Communications Map:

A listing of all the pathways (ports, protocols, physical components) used by a cyber component to communicate within a system or network.

Communications Map Development:

The second step of Simple Threat Analysis (STA) Communications Map Development focuses on the path used by an adversary to deliver exploit code or malware to a vulnerable system. Communications Map Development can also be used to determine the communications paths leveraged by an attacker to perform attack operations, which will typically include both ingress and egress traffic from a compromised cyber resource. This delivery information is organized in the ATAC Functional Security Matrix (FSM) by Functional Security Layer (FSL). For example, a web browser based attack employing malicious Java applets may use ports 80, 8080, and 443, information which would be recorded by the ATAC tool user in the Applications section of the Communications Map Information column of the ATAC FSM.

Complex Threat Analysis (CTA):

Following Simple Threat Analysis (STA), CTA encompasses Predictive Attack Path Analysis (PAPA) and Forecasting Attack Technology. This portion of the ATAC process is intended to provide organizations with additional information for use during preemptive security efforts.

Core System:

Also known as critical work components, a core system is comprised of any software, communications technologies, data, or services necessary for an organization to achieve their mission goals. A core system may be used to perform multiple tasks associated with the mission goals but has only a single technical purpose. An example of a core system might be the Front End Processor (FEP) used to manage multiple, remote endpoints in the process environment.

Core System Identification:

A component of the Impact Driven Risk Analysis (IDRA) methodology, Core System Identification is the process by which groups identify systems necessary for critical workflow. Core systems must be identified by both the function and technical make-up of a process or ICS function. For example, the core systems used to manage the transmission of an oil pipeline might include the remote flow sensors, the RTUs or PLCs managing those sensors, the central ICS management system that aggregates data and process control from multiple PLCs or RTUs, and the historian database used to push the flow data to a billing server.

Critical Impact Identification:

Also known as impact identification. A component of the Impact Driven Risk Analysis (IDRA) methodology, Critical Impact Identification is the process by which groups characterize and rank the effects associated with a loss of function. In terms of cyber security and IDRA, critical impact allows organizations to prioritize their risk and to allocate resources necessary for mitigation efforts.

Critical Workflow:

Any work function which is necessary for an organization to achieve their business goals.

Critical Workflow Identification:

Also known as development of the functional overview. A component of the Impact Driven Risk Analysis (IDRA) methodology, Critical Workflow Identification is a step conducted by organizations prior to beginning a ReACT assessment, the goal of which is to identify core systems and critical impacts associated with the workflow. Put another way, a critical workflow is comprised of the processes necessary to ensure an organization's mission goals. In the context of the ReACT assessment, the Critical Workflow Identification limits the focus of

the assessment to an organization's most important business processes, the critical impacts associated with those processes, and the core systems that could be used by an adversary to realize critical impact.

Custom or Proprietary Software:

One of the Functional Security Layers (FSL), custom or proprietary software (aka "custom code") refers to any software for which the system owner is responsible for maintaining the source code, application, or scripts throughout the Software Development Life Cycle. Examples include remote management scripts used to manage ICS server, ladder logic used by ICS that must be maintained for the process to run, and applications or software written by an integrator or 3rd party.

Cyber Resources:

The various components which make up a core system. Cyber resources may include any combination of user activities, applications, data, services, or systems.

Cyber Risk:

An individual's or group's intentional or accidental exposure to danger, loss, or harm through data, services, computers, networks, or technology.

Data and Data Storage:

One of the Functional Security Layers (FSL), data and data storage refers to the information and information holding components used by a core system. Data storage may include any permanent or temporary storage mechanism used by the read, write, or execute functions for storing, transmitting, or manipulating data. An example includes the temporary cache of sensor data in the ICS application when the sensor data is synchronized between ICS devices.

Emerging Threat Identification:

The preliminary step of the ATAC process, which is characterized by the identification of a new threat (attack technology, adversarial group, etc.).

Exploitation:

The fourth step of the Lockheed Martin Intrusion Kill Chain which is characterized by the execution of malicious code on the target system in order to gain an initial Point of Entry on a target network or to pivot from one foothold to another in an already compromised network.

Exploitation and Pivoting:

The second stage of the ATAC Life Cycle which corresponds to the Implementation phase of the System/Software Development Life Cycle.. This stage encompasses the Lockheed Martin Intrusion Kill Chain steps of Delivery and Exploitation. In this stage, an adversary gains an initial Point of Entry (PoE) to one or multiple systems or pivots to another system or systems using the foothold gained during the initial PoE. It is during this stage that additional target systems may be identified for attack and to further the adversary’s operational goals.

Forecasting Threat Technology:

Part of Complex Threat Analysis (CTA), Forecasting Threat Technology is the process by which organizations identify either the most likely delivery mechanisms for future attacks against specific targets or, alternatively, identify the most probable evolutions of known attack technologies and techniques necessary for bypass and evasion.

Firmware:

One of the Functional Security Layers (FSLs), firmware (or embedded device software) is a combination of special purpose hardware, persistent memory, program code and the data stored on it. Examples of firmware include: BIOS, chipset, video card, programmable logic controller (PLC), or smart meters.

Functional Baseline:

An output of the ReACT assessment, the Functional Baseline is a picture of a core system's technical architecture. Functional baseline information is expressed as a list of the core system's software inventory broken-down by Functional Security Layer (FSL). In order to perform RCFA or Cluster Analysis, the Functional Baseline must be also understood in terms of its use case functionality, i.e. who uses it and why, and how the architecture of the core system meets those business needs.

Functional Overview:

See Critical Workflow Identification.

Functional Security Layers (FSL):

A means of organizing functional baseline information (during the ReACT process) and attack technology attack workflow information (during the ATAC process). The Functional Security Layers provide cyber security professionals with a means of organizing and synthesizing data, and ensure that relevant information is not overlooked during the ReACT and ATAC processes.

Functional Security Layers (FSL) subcomponents:

The subcomponents of the FSL are people, process and technology and are incorporated into the FSL rows in the Functional Security Matrix (FSM). The subcomponents are used primarily for performing RCFA and Cluster analysis during a ReACT assessment.

Functional Security Matrix:

A template used during both ATAC and ReACT assessments to organize information from the FSL, the FSL subcomponents, and the ATAC or ReACT Life Cycles. This information is then used to analyze information regarding either an attacker's use of threat technology throughout the attack work flow or the defender's management of core systems throughout the SDLC.

Functional Security Translation:

The first step of Simple Threat Analysis (of the ATAC Process). A process for organizing known attack technology information within the Functional Security Layers (FSL). The information organized in this step should be highly detailed and address how the attack technology was used by the adversary across the various functions of the ATAC Life Cycle.

Heat Map:

An optional product of the ReACT process, a heat map is a visual representation of the cyber risk an organization faces. For the ReACT process, components are graphed along two axes, Impact (the vertical axis) and Probability (typically the horizontal axis).

Hosted and Cloud Services:

One of the Functional Security Layers (FSL), hosted and cloud services refers to any combination of hosted, managed, 3rd party, or cloud services used by an organization to perform a core function in the critical work flow. Hosted or cloud services includes any of the

*as-a-Service offerings (software, platform, or infrastructure) provided by a 3rd party provider over the internet or wide area networks.

Impact Driven Risk Analysis Methodology (IDRAM):

A risk identification and analysis methodology which characterizes risk in terms of what's important to a business and what core systems could be used to impact an organization's ability to perform.

In-House analyst:

For the purposes of this document, an in-house analyst is an analyst, cyber security professional, etc. who is a full time employee of a company.

Intrusion Kill Chain:

A model developed by Lockheed Martin to describe the actions conducted by an adversary from the conception of an attack through its completion. The model is described as a kill chain to emphasize the interdependency of the steps; disruption anywhere along the Intrusion Kill Chain will result in a failed attack.

Incident Response:

Also known as incident management, it is the process of responding to or managing a functional or security-impacting incident that caused (or may cause) an interruption or a reduction in the quality of an IT or ITC service. ATAC, ReACT, and IDRAM all utilize the ITIL concepts of incident and problem management.

Network Communications:

One of the Functional Security Layers (FSL), network communications must be understood by security professionals as they can provide adversaries with a remotely-accessible attack path to a targeted system. Examples of network communications include: Distributed Network Protocol 3 (DNP3) communications between a control center and an RTU; CompuTrace beaconing from the BIOS of a CompuTrace-protected system over any DSL, Ethernet, wireless, or satellite communications channel; cellular communications from a remote substation to a control center; and Secure Shell (SSH) connection over TCP/UDP port 22 used to manage a server remotely.

Operating System (OS):

One of the Functional Security Layers (FSL), in its simplest form an OS is the software collection that manages resources and provides services for computer programs. An OS can be physical, virtual, embedded or mobile in nature. Examples include: the platform operating system that the Energy Management System (EMS) runs on; an embedded Linux kernel in an RTU, FEP, or PLC; or an Android OS on the mobile phone hosting the web-enabled Human Machine Interface (HMI) application used to manage a SCADA network.

Order of Operations:

Also known as the Order of Attack Operations, this is the general order of operations for a potential attack. This concept is used to understand the workflow of an attack, which are expressed as the Target Development, Exploitation and Pivoting, Attack Operations, and Attack End of Life (EoL) in ATAC. The Order of Operations chronology differs from the attack timeline, which is a chronological order of operations for a past attack.

Payload:

The malicious software, aka malware, which is loaded on compromised systems by the adversary to perform attack operations. Payload may also be known as exploit kits, Trojan horses, or Remote Access Trojans (RATs) and is used to manage attack operations work such as C&C communications, data exfiltration, etc.

Pivoting:

The process by which an adversary identifies new potential targets and moves from one compromised system to another by employing additional attack technology. Pivoting occurs after the adversary has gained an initial foothold on the network through a Point of Entry (PoE) attack and is transitioning to another network segment or target type. When pivoting through a network, attackers generally use a second type of Elevation of Privilege attack technique to move around, not the initial PoE attack used on the PoE systems.

Predictive Attack Path Analysis (PAPA):

Based on a security posture or attack technology, predictive attack path analysis is the process of identifying how future attacks are likely to manifest themselves. Put another way, Predictive Attack Path Analysis is the process of identifying an adversary's likely attack path by observing the connections between core and other systems.

Preemptive Mitigation:

Corrections made to a security posture following Simple Threat Analysis (ATAC Process), intended to provide immediate protections from an emerging threat.

Response Analysis and Characterization (ReACT) tool:

An information schema and analysis methodology which provides organizations with an organized and comprehensive approach for assessing and improving their current security posture.

ReACT assessment:

An output of a Response Analysis and Characterization (ReACT) review, the ReACT assessment determines an organizations existing security posture to be used during attack surface analysis, root cause failure analysis and cluster analysis. ReACT assessments provide the basis for building a work plan to address the root cause failures that allow security weakness or vulnerabilities to exist.

Root Cause Failure Analysis (RCFA):

Following the completion of a ReACT assessment, Root Cause Failure Analysis is the process of identifying the reason behind weaknesses in security posture. During the ReACT process, these failures are categorized by Functional Security Layer (FSL), the organizational hierarchy (people, process or technology) and the System/Software Development Life Cycle (SDLC).

Security Posture:

The tools, policies, and protections currently deployed by a group, individual, or organization in order to address threats and maintain security. For example, an organization may frequently review access control lists to ensure that access is limited to only necessary individuals. In terms of the ReACT assessment, the security posture is used to perform attack surface analysis.

Simple Threat Analysis (STA):

Following the identification of a threat, the Simple Threat Analysis (STA) is comprised of three steps: Attack Surface Analysis (ASA), the development of an attack timeline (or order of operations), and attack path modeling.

STRIDE Threat Model:

A system developed by Microsoft for classifying computer security threats. It is comprised of six categories including: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

Subject Matter Expert (SME):

A SME is an individual with substantial expert knowledge in a particular field or topic. For the purposes of this document, the term SME distinguishes a contractor or external cyber security professional or threat analyst from an in-house analyst.

System (or Software) Development Life Cycle (SDLC):

A series of steps for the development of systems or software, including: design, implementation, maintenance and end-of-life. In the ATAC process, the ATAC Life Cycle is based on the SDLC.

Target Development:

The first stage of the ATAC Life Cycle, which includes the process of gaining an initial foothold and corresponds to the Design phase of the System Development Lifecycle. This stage incorporates the Lockheed Martin Intrusion Kill Chain steps: Reconnaissance and Weaponization. During this stage an adversary selects and researches a target in order to identify the most likely means of access.

Threat Technology:

Threat intelligence or technical threat intelligence is the initial input of the ATAC process. Examples of threat intelligence include, but are not limited to, alerts, RSS feed, and informal sharing.

User Roles & Responsibilities:

One of the Functional Security Layers (FSL), user roles and responsibilities (UR&R) defines the relationship between users, computer systems, network, and data. Examples include requiring VPN tokens and credentials to access a company's network or a WPA/PSK key for a specific wireless network.

Virtualization:

One of the Functional Security Layers (FSL), virtualization is any software loaded on a system that virtualizes a substantial feature of the system. While users can virtualize computer hardware platforms, operating systems, storage devices, or other computer network resources, in the case of the FSL virtualization generally refers to operating systems. Examples of virtualization include the platform and centralized management features for VMWare, Microsoft Hypervisor, or Xen.