ANGARA SOC

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ:
КАК МИНИМИЗИРОВАТЬ КИБЕРРИСКИ И ОБЕСПЕЧИТЬ НЕПРЕРЫВНОСТЬ БИЗНЕСА

ANGARA SOC

100+
человек в штате

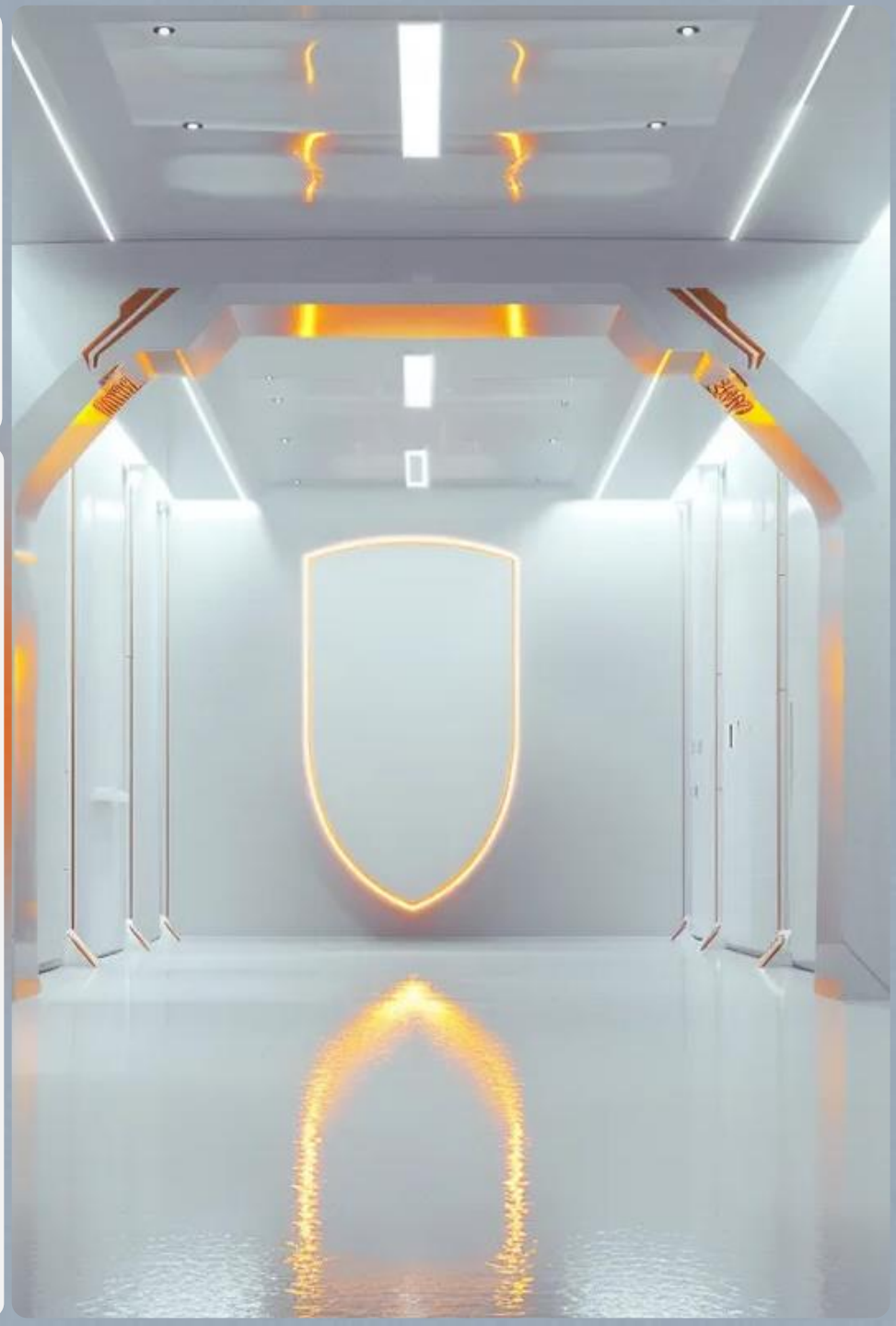
50+
клиентов

5+
лет на рынке

- Мониторинг и управление инцидентами | SOC
- Реагирование на инциденты и цифровая криминалистика | DFIRMA
- Поиск следов компрометации | Compromise assessment
- Корпоративный центр ГосСОПКА класса «А»
- Защита бренда | OSINT
- Атрибуция угроз

О ЧЕМ СЕГОДНЯ ПОЙДЕТ РЕЧЬ

1. Практика security operations и наработанный опыт
2. Задачи при управлении киберрисками
3. Актуальность ландшафта угроз и при чем здесь кибербразведка
4. Почему невозможно обеспечить 100% безопасность



ДОМЕН SECURITY OPERATIONS

Цель – не допустить риск ущерба
в результате злонамеренных действий

Задача – обеспечить эффективное
выявление актуальных киберугроз
и реагирование на них

КИБЕРРАЗВЕДКА (CTI)

CTI – применимые на практике знания о злоумышленниках и их деятельности, позволяющие снижать ущерб за счет принятия обоснованных решений в области информационной безопасности

The NIST Cybersecurity Framework (CSF) 2.0

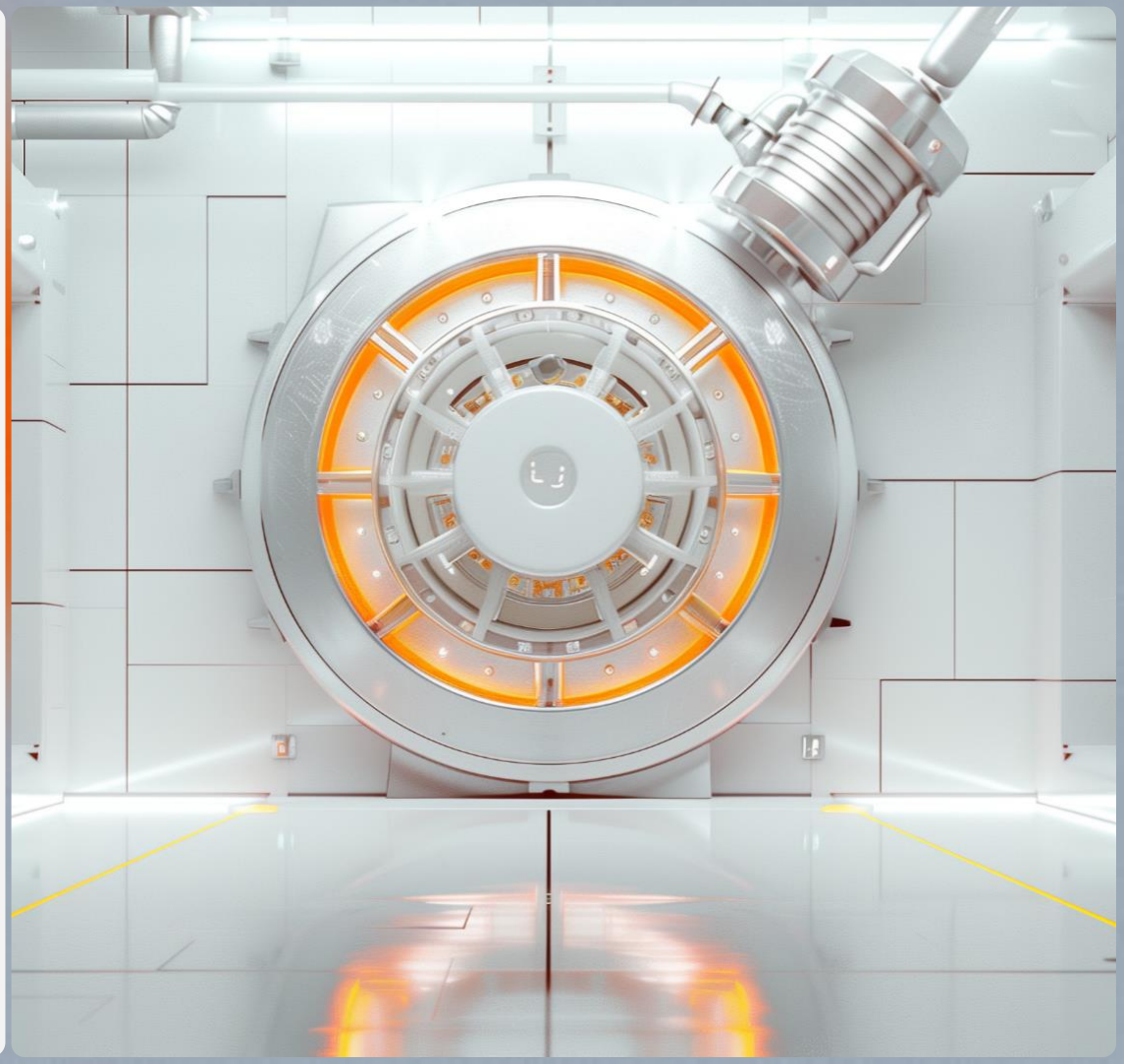
Выпущен 26.02.2024

GOVERN

И повторяем...

GOVERN

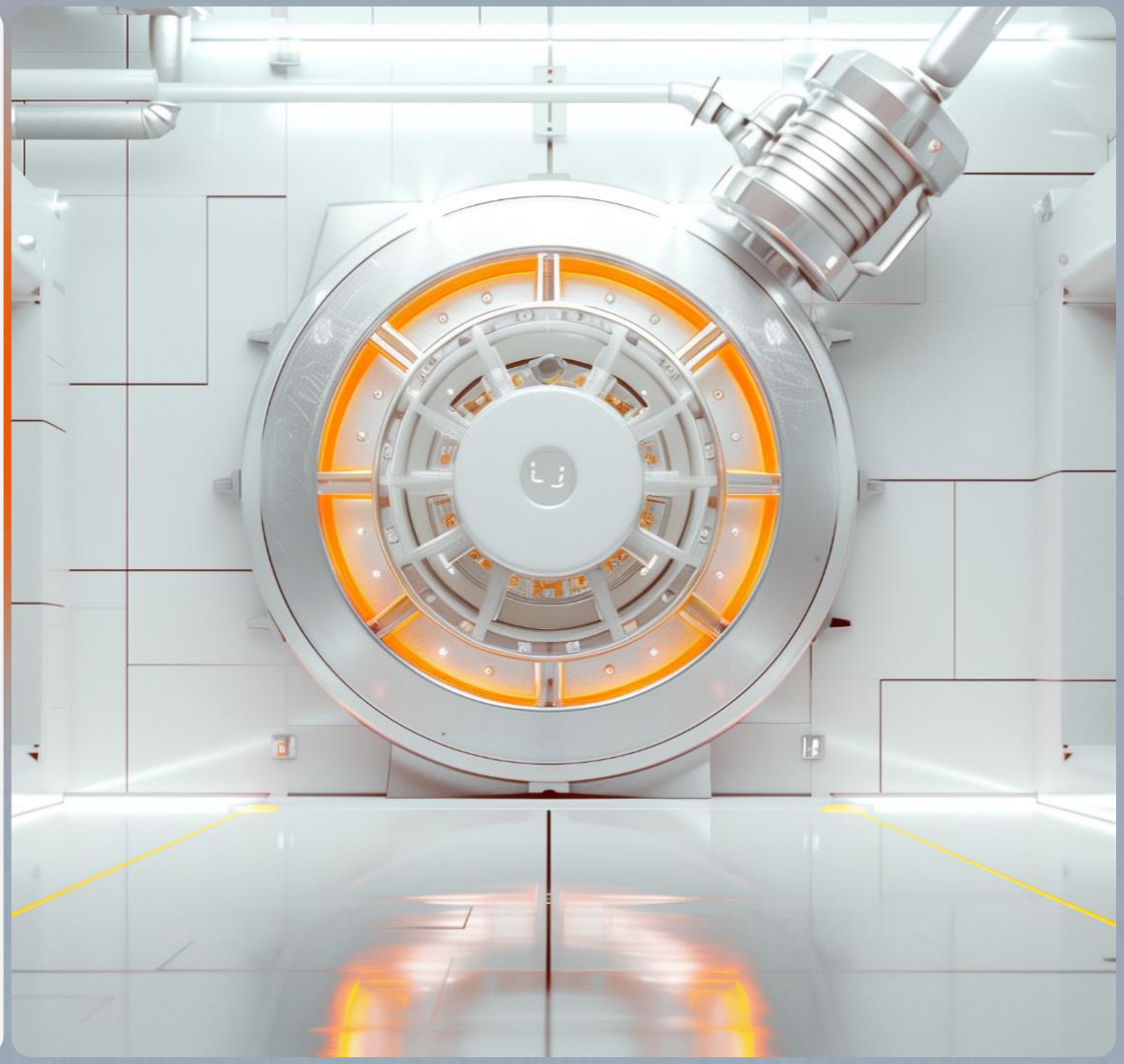
- Определяем стратегии, политики и ответственных
- Проводим количественную оценку рисков
- Определяем зависимости
- Прорабатываем планы восстановления



IDENTIFY

Определяем актуальные риски с учетом:

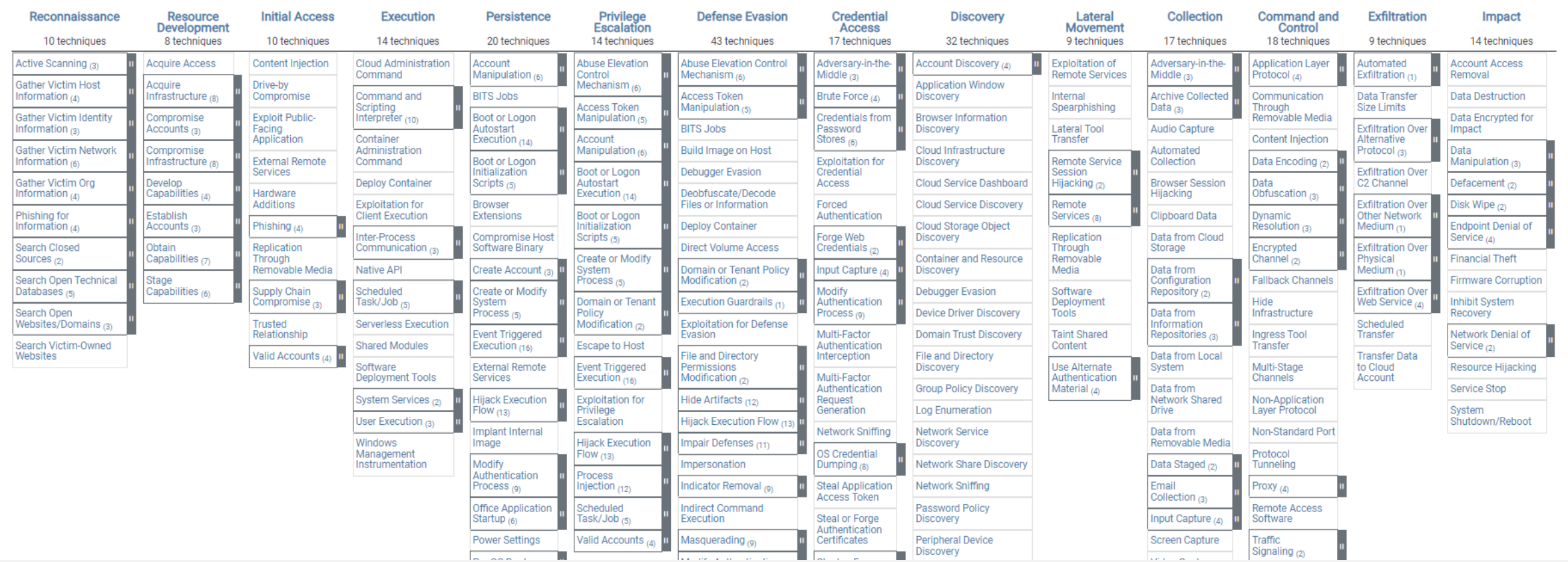
- Активов (оборудование, ПО, потоки данных, etc.),
- Сферы и вида деятельности организации,
- Региональной принадлежности



IDENTIFY

14 тактик
235 техник

> 400 подтехник
И очень много процедур

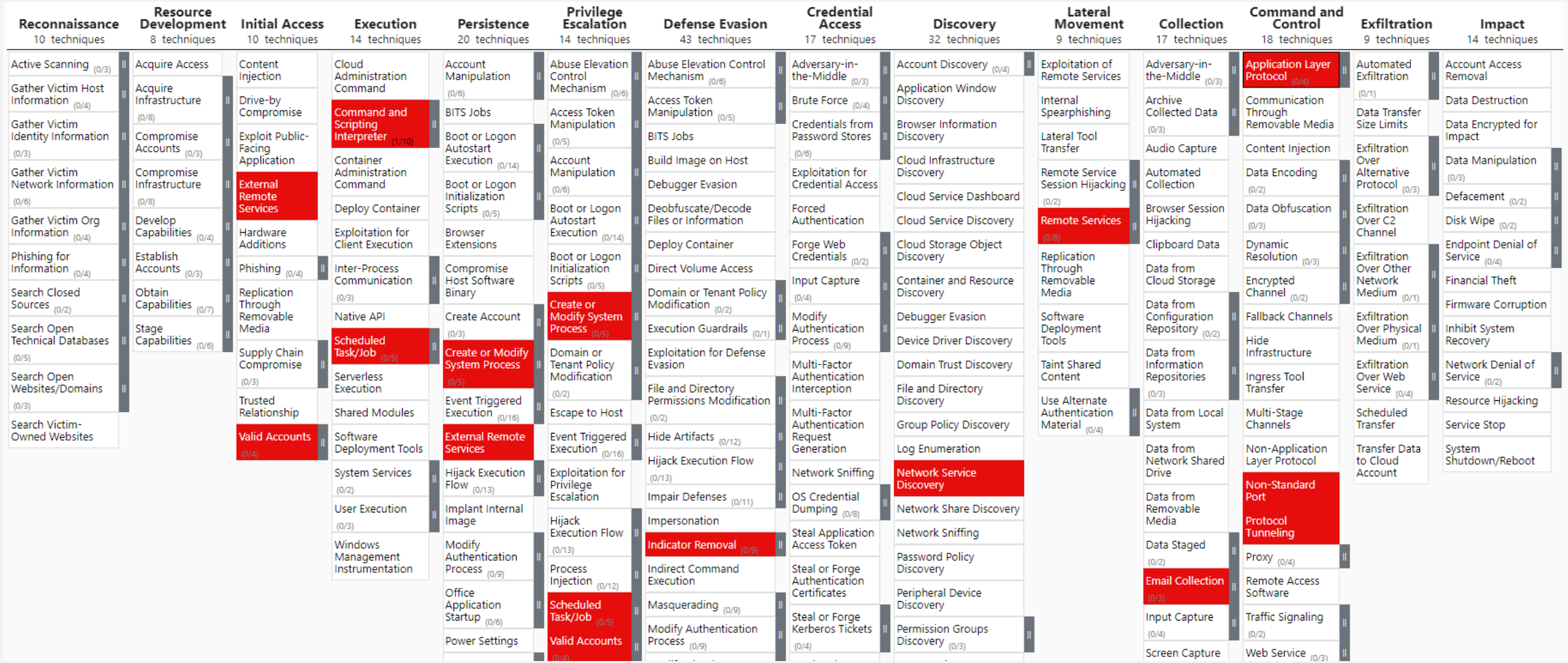


IDENTIFY
MITRE ATT&CK®: Design and Philosophy

you determine coverage. Anyone mapping to ATT&CK should be able to explain the procedures they cover. Similarly to how it's unrealistic to expect coverage of 100% of ATT&CK techniques, it's unrealistic to expect coverage of all procedures of a given technique, especially since we often cannot know all of them in advance.

Operationalizing ATT&CK for an organization also encompasses determining what it means for

IDENTIFY


Reconnaissance
10 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/4)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/8)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (0/7)
Stage Capabilities (0/6)
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/4)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (1/10)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/3)
Native API
Scheduled Task/Job (0/5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (0/3)
Windows Management Instrumentation
Persistence
20 techniques
Account Manipulation (0/6)
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Host Software Binary
Create Account (0/3)
Create or Modify System Process (0/5)
Event Triggered Execution (0/16)
External Remote Services
Hijack Execution Flow (0/13)
Implant Internal Image
Modify Authentication Process (0/9)
Office Application Startup (0/6)
Power Settings
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (0/6)
Access Token Manipulation (0/5)
Account Manipulation (0/6)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/5)
Domain or Tenant Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/16)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/13)
Process Injection (0/12)
Scheduled Task/Job (0/5)
Valid Accounts (0/4)
Defense Evasion
43 techniques
Abuse Elevation Control Mechanism (0/6)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/12)
Hijack Execution Flow (0/13)
Impair Defenses (0/11)
Impersonation
Indicator Removal (0/9)
Indirect Command Execution
Masquerading (0/9)
Modify Authentication Process (0/9)
Credential Access
17 techniques
Adversary-in-the-Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/9)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/4)
Discovery
32 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (0/3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (0/8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)
Collection
17 techniques
Adversary-in-the-Middle (0/3)
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (0/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Input Capture (0/4)
Screen Capture
Command and Control
18 techniques
Application Layer Protocol (0/4)
Communication Through Removable Media
Content Injection
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Software
Traffic Signaling (0/2)
Web Service (0/3)
Exfiltration
9 techniques
Automated Exfiltration (0/1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (0/4)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
14 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (0/3)
Defacement (0/2)
Disk Wipe (0/2)
Endpoint Denial of Service (0/4)
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (0/2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

LOCKHEED MARTIN

A Threat-Driven Approach to Cyber Security

Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization

Michael Muckin, Scott C. Fitch
Lockheed Martin Corporation

Abstract

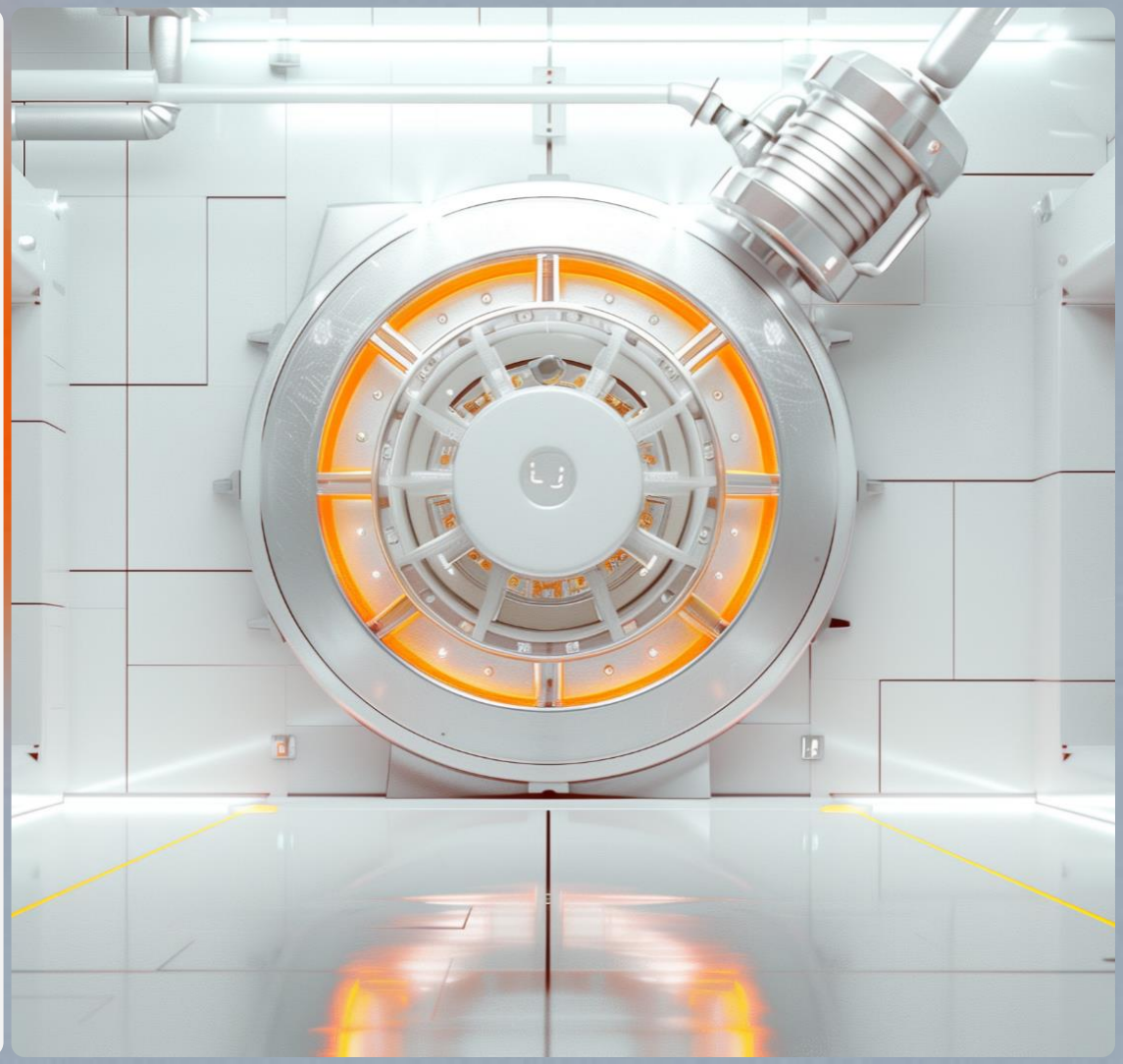
Contemporary cyber security risk management practices are largely driven by compliance requirements, which force organizations to focus on security controls and vulnerabilities. Risk management considers multiple facets – including assets, threats, vulnerabilities and controls – which are jointly evaluated with the variables of probability and impact. Threats cause damage to information systems. Threats utilize vulnerabilities to enact this damage, and security controls are implemented to attempt to prevent or mitigate attacks executed by threat actors. The unbalanced focus on controls and vulnerabilities prevents organizations from combating the most critical element in risk management: the threats. This unbalanced condition is manifested as incident response processes rather than threat intelligence management in the analyst realm, adherence to predefined standards and policies in security architecture and engineering practices, and compliance verification in the operational domain.

A functionally integrated cyber security organization is structured to place threats at the forefront of strategic, tactical and operational practices. Architects, engineers and analysts adhere to a common methodology that incorporates threat analysis and threat intelligence across systems development and operational processes. This ensures security controls are implemented, evaluated and adjusted over time per the most impactful threats and attack vectors. The resultant risk management practices are enhanced due to a higher fidelity of information regarding current state security postures. This drives improved resource allocation and spending, and produces an agile and resilient cyber security practice. When this threat-driven approach is implemented along with tailored compliance processes, organizations can produce information systems that are both compliant and more secure.

Keywords: threat modeling, attack trees, threat profiles, threat intelligence, threat and risk, security controls, cybersecurity, compliance

IDENTIFY

- Получаем актуальные данные об уязвимостях и закрываем их
- Определяем актуальные TTP
- Проводим оценку покрытия актуальных TTP
- Проводим Compromise assessment
- Проводим оценку готовности к реагированию на инциденты
- Проводим оценку подрядчиков



PROTECT

Выполняем:

- Харденинг
- Настройку ACL
- Сегментацию
- TIER AD
- configs review
- Контроль полноты аудита с учетом актуальных TTP
- etc.

DETECT

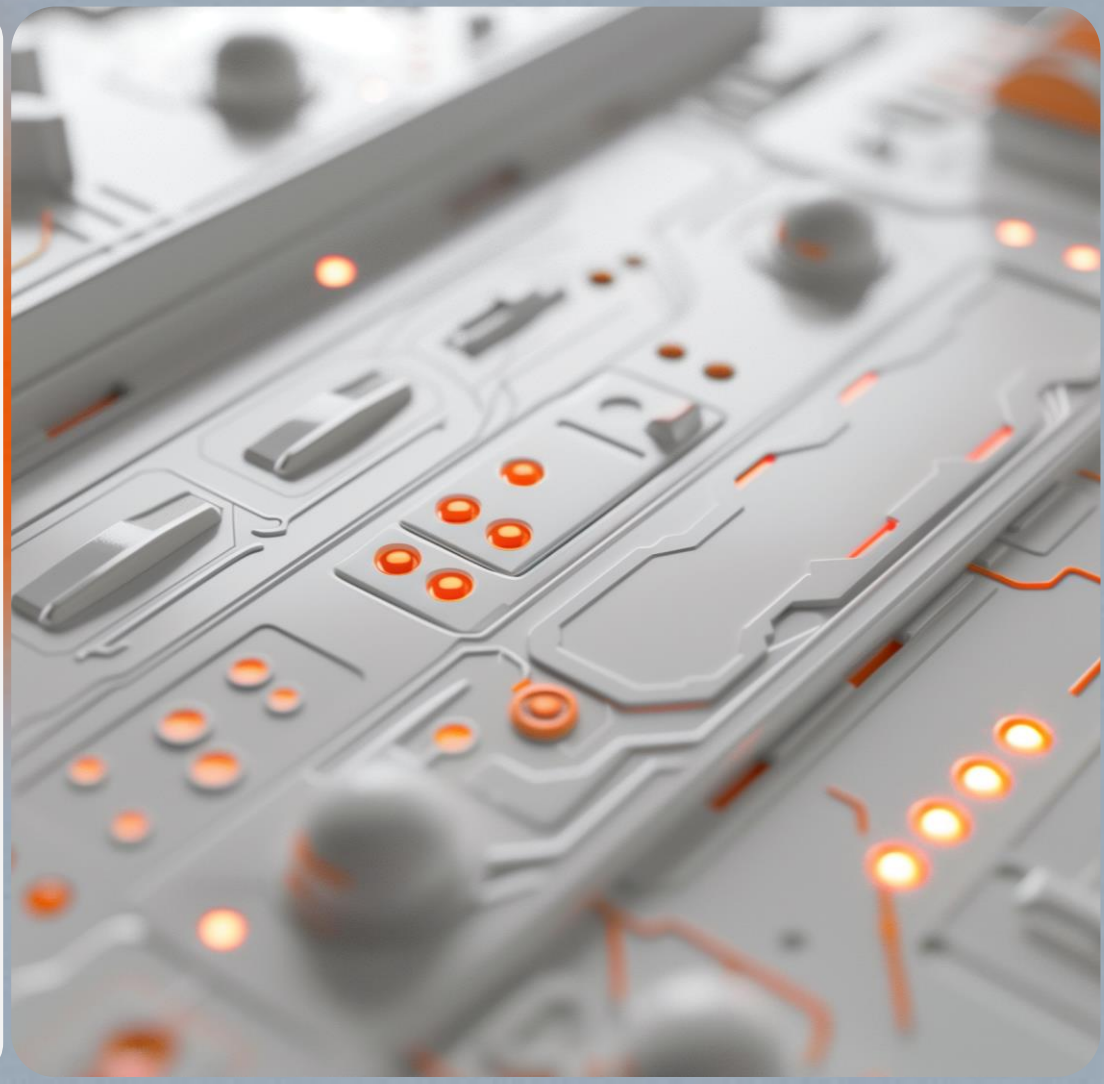
Упрощенная схема процесса выявления угроз

Определение источников событий -> Определение полноты покрытия -> Сбор событий -> Нормализация -> Таксономия -> Фильтрация -> Агрегация -> Исключения -> Обогащение -> Правила базовых контролей -> Правила нормального распределения -> Правила детектирования -> Правила корреляции (два уровня) -> Правила ML -> Отчеты -> Тренды -> Выгрузки -> Threat hunting -> Подключение архивов -> etc.

DETECT

Основные задачи:

- Обеспечить выявление актуальных угроз
- Найти баланс между полнотой сбора событий и количеством ложно-положительных срабатываний



RESPOND

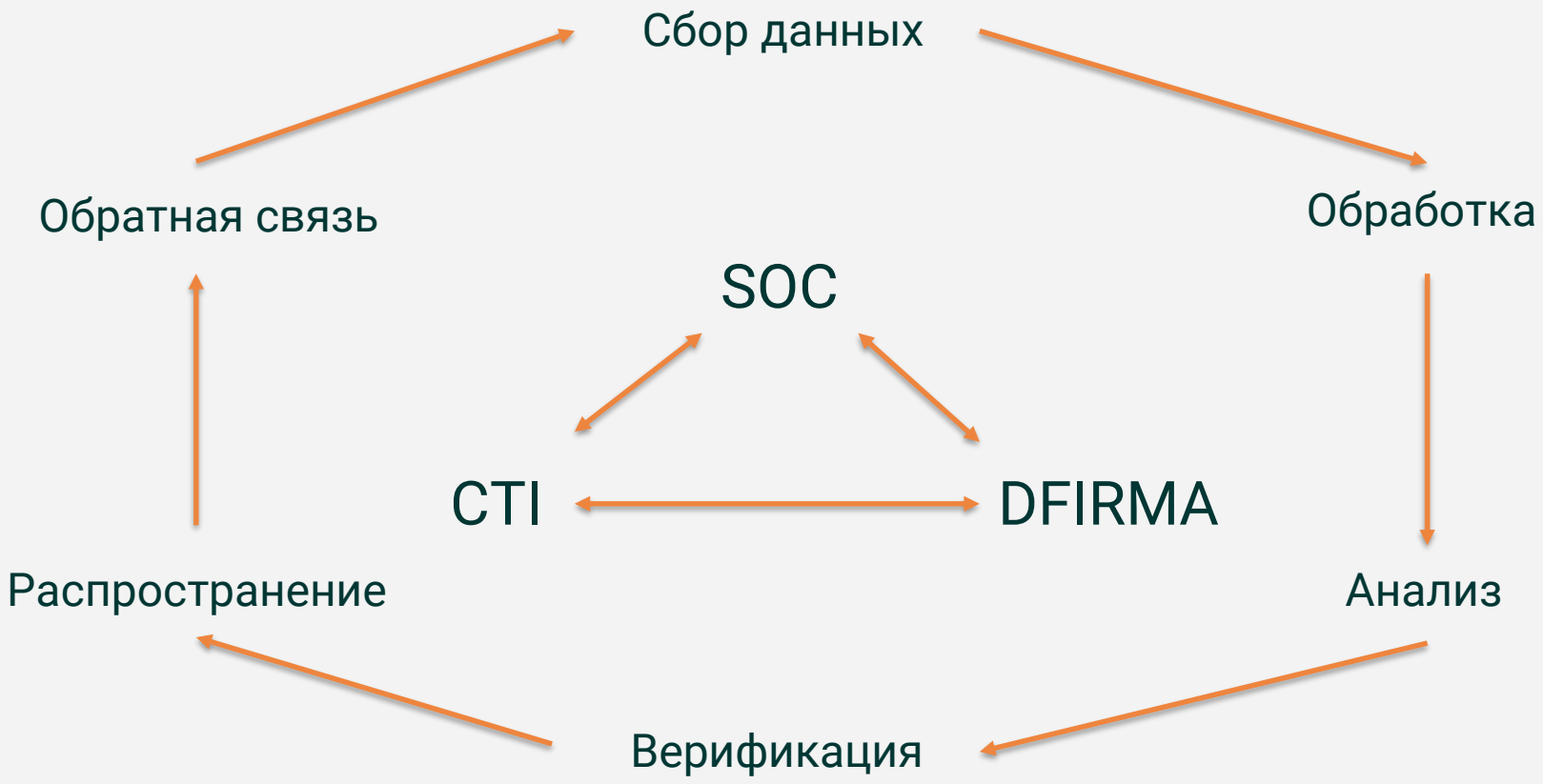
Определение стратегии и плана реагирования:

1. Наиболее вероятные тактики и техники злоумышленника, чтобы как можно быстрее определить «нулевого пациента» и точку входа
2. Определить первоначальные меры по сдерживанию злоумышленника и детектированию его активности (напр., включить дополнительно логирование, подключить доп. источники, etc.)
3. Определить критерии начала восстановления инфраструктуры с учетом критичности затронутых бизнес-процессов
4. Быстрое обогащение контекста инцидента
5. Определение дополнительных релевантных IoC/IoA для проверки
6. Восстановление kill-chain: от точки входа до нанесения ущерба

RECOVER

- Проверка бэкапов по выявленным IoC ДО восстановления
- Восстановление в соответствии с критериями на этапе Respond
- Срочная корректировка плана восстановления в случае выявления дополнительного контекста инцидента
- Обогащение данных CTI по результатам реагирования на инцидент
- Проверка и адаптация контрмер (lessons learned)

ЭКСПЕРТИЗА И ПРОЦЕССЫ



ЧТО ЕЩЕ ПОЛЕЗНО ИСКАТЬ

- Информацию об успешных атаках
- Предложения по продаже доступов/конфиденциальных данных
- Опубликованные секреты (логины/пароли, ключи, etc.)
- Фишинговые ресурсы, распространение ложной информации

ANGARA SECURITY

СПАСИБО ЗА ВНИМАНИЕ!

Артём Грибков

Angara SOC

https://www.angarasecurity.ru/soc/

+7 495 269-26-06

info@angarasecurity.ru