GIAN Short course

Cyber-Physical Security for the Smart Grid

Indian Institute of Technology, Bombay, India

Coordinator: Prof. R. K. Shyamasundar

Manimaran Govindarasu

Dept. of Electrical and Computer Engineering

Iowa State University

Email: gmani@iastate.edu

http://powercyber.ece.iastate.edu

March 5-16, 2018

Course Agenda

Day 01	• Module 1: Cyber Threats, Attacks, and Security concepts
Day 02	• Module 2: Risk Assessment and Mitigation & • Overview of Indian Power Grid
Day 03	• Module 3: Attack-resilient Wide-Monitoring, Protection, Control
Day 04	• Module 4: SCADA, Synchrophasor, and AMI Networks & Security
Day 05	• Module 5: Attack Surface Analysis and Reduction Techniques
Day 06	• Module 6: CPS Security Testbeds & Case Studies
Day 07	• Module 7: Cybersecurity Standards & Industry Best Practices
Day 08	• Module 8: Cybersecurity Tools & Vulnerability Disclosure
Day 09	• Module 9 : Review of materials, revisit case studies, assessments
Day 10	• Module 10: Research directions, education and training

Outline of **Module 8**

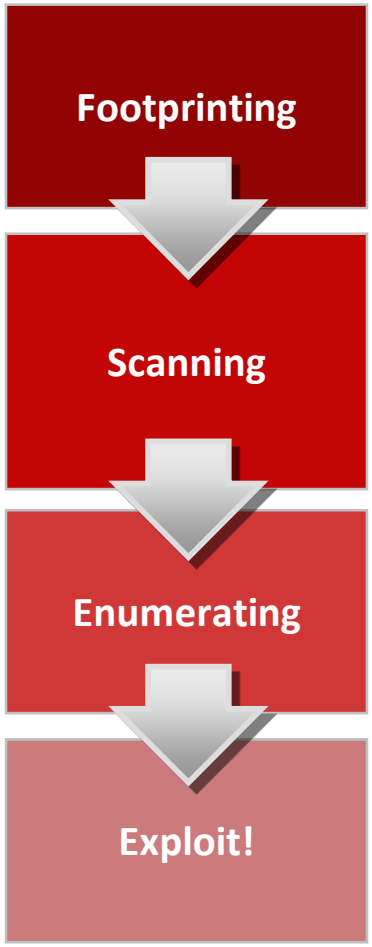
- Vulnerability Assessment Tools
- SIEM tools
- Intrusion Detection (IDS) Tools
- Vulnerability and Security Assessment
- Vulnerability Disclosure Policy

Vulnerability Assessment

Inspect weaknesses in industry standards, software platforms, network protocols and configurations

- Common activities include
  - Vulnerability Scanning
  - Cryptography Analysis
  - Software fuzz testing
- Common tools
  - Nmap – a security scanner to discover hosts and services on a network
  - Wireshark – a network packet sniffer & analyzer tool
  - Nessus – a comprehensive vulnerability scanning program

Intrusion Process



Vulnerability Assessment Tools: Nmap

Zenmap

Scan Tools Profile Help

Target: 192.168.5.210

Command: nmap -p 1-20000 -T4 -A -v 192.168.5.210

Hosts | Services

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

OS | Host

192.168.5.1
192.168.5.10
192.168.5.37
192.168.5.123
192.168.5.199
192.168.5.201
192.168.5.202
192.168.5.203
192.168.5.207
192.168.5.210
192.168.5.211
192.168.5.213
192.168.5.217
192.168.5.218
192.168.5.224
192.168.5.225
192.168.5.226
192.168.5.252
192.168.5.253
192.168.5.254

Filter Hosts

nmap -p 1-20000 -T4 -A -v 192.168.5.210

```
Scanning 14 services on 192.168.5.210
Completed Service scan at 21:00, 105.97s elapsed (14 services on 1 host)
Initiating OS detection (try #1) against 192.168.5.210
NSE: Script scanning 192.168.5.210.
Initiating NSE at 21:00
Completed NSE at 21:02, 106.99s elapsed
Nmap scan report for 192.168.5.210
Host is up (0.00023s latency).
Not shown: 19986 closed ports
PORT      STATE SERVICE        VERSION
13/tcp    open  daytime        Tardis 2000 daytime
37/tcp    open  time           (32 bits)
102/tcp   open  iso-tsap?
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds
1123/tcp  open  msrpc          Microsoft Windows RPC
2638/tcp  open  sybase?
2869/tcp  open  http           Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code
|_http-title: Site doesn't have a title (text/html).
3389/tcp  open  ms-wbt-server?
5434/tcp  open  postgresql     PostgreSQL DB
10008/tcp open  octopus?
10500/tcp open  unknown
20000/tcp open  dnp?
MAC Address: 00:0D:56:F1:B4:02 (Dell Pcba Test)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP Professional SP2 or SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat:
|   NetBIOS name: SCADAWS02, NetBIOS user: <unknown>, NetBIOS MAC: 00:0d:5
|   Names
|     SCADAWS02<00>        Flags: <unique><active>
|     SCADA<00>            Flags: <group><active>
|     SCADAWS02<20>        Flags: <unique><active>
|_    SCADA<1e>            Flags: <group><active>
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: SCADAws02
|   NetBIOS computer name: SCADAWS02
```

Zenmap

Scan Tools Profile Help

Target: 192.168.5.210

Command: nmap -p 1-20000 -T4 -A -v 192.168.5.210

Hosts | Services

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

OS | Host

192.168.5.1
192.168.5.10
192.168.5.37
192.168.5.123
192.168.5.199
192.168.5.201
192.168.5.202
192.168.5.203
192.168.5.207
192.168.5.210
192.168.5.211
192.168.5.213
192.168.5.217
192.168.5.218
192.168.5.224
192.168.5.225
192.168.5.226
192.168.5.252
192.168.5.253
192.168.5.254

192.168.5.210

Host Status

State:	up
Open ports:	14
Filtered ports:	0
Closed ports:	19986
Scanned ports:	20000
Up time:	Not available
Last boot:	Not available

Addresses

IPv4:	192.168.5.210
IPv6:	Not available
MAC:	00:0D:56:F1:B4:02

Operating System

Name: Microsoft Windows XP Professional SP2 or SP3

Accuracy: 100%

- Ports used
- OS Classes

- TCP Sequence
- IP ID Sequence
- TCP TS Sequence
- Comments

Vulnerability Assessment Tools: Nessus

Nessus vulnerability scanner

administrator | Help & Support | Sign Out

Results | Scans 0 | Templates | Policies | Users | Configuration

rtu 192.168.5.210

Filter Options 0 | Audit Trail | Delete All Results

Hosts 1

Vulnerabilities 39

Export Results

192.168.5.210

Knowledge Base | Filter Vulnerabilities

high	Microsoft Windows SMB Shares Unprivileged Access	Windows	1
high	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remo...	Windows	1
medium	Microsoft Windows SMB Guest Account Local User Access	Windows	1
medium	Microsoft Windows SMB NULL Session Authentication	Windows	1
medium	Terminal Services Encryption Level is Medium or Low	Misc.	1
medium	Microsoft Windows Remote Desktop Protocol Server Man-in-the-...	Windows	1
medium	NTP ntpd Mode 7 Error Response Packet Loop Remote DoS	Misc.	1
medium	Sybase ASA Client Connection Broadcast Remote Information Di...	Databases	1
medium	SMB Signing Disabled	Misc.	1
low	Terminal Services Encryption Level is not FIPS-140 Compliant...	Misc.	1
info	Nessus SYN scanner	Port scanners	10
info	Service Detection	Service detection	2
info	Microsoft Windows SMB Service Detection	Windows	2

Vulnerability Assessment using Fuzz Testing ?

Mu Test Suite

https://192.168.5.211/app/?wicket:interface=:28::

Signed in as scada | Sign Out | Support | Help

Tests | Results | Apps | Template | System

No running test

Fault Overview | Engine Log | Fault Trace

Protocol Mutation Fault

Vector	DNP3 Select and Operate Requests - select.datalink.payload.string.utf-8[0-15]	4/24/12 9:31:56 PM
Isolation/Detection	Variant / Instrumentation (! ! ! ! !)	
CVSS	**Base Metrics**	
	Access Vector Unknown (0.823)	
	Access Complexity Low (0.710)	
	Authentication Unknown (0.571)	
	Availability Impact Partial (0.275)	
	Calculate CVSS Score	
	(Unknown values could not be estimated)	
Test Run	DNP3	
Export	Sample Pcap Report Engine Log	

DNP3

Distributed Network Protocol (DNP3) is a layer-2 protocol that handles communications between devices and software used by electric and water companies. DNP3 protocols handle data transfers and ensure interoperability between Supervisory Control And Data Acquisition (SCADA) system components for the electrical powergrid, even when those components are produced by different vendors. DNP3 enables reliable (but not necessarily secure) communications in environments with EMI distortion, legacy systems, and poor transmission mediums.

SCADA systems are large-scale, distributed measurement and control systems used to monitor and manage chemical, physical, or transport processes. A SCADA system includes SCADA Master Stations (Control Centers), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). Communications between a master station and RTUs or IEDs use DNP3; communications between masters (inter-master communication) uses the Inter-Control Centre Protocol (ICCP).

DNP3 provides multiplexing, data fragmentation, error checking, link control, prioritization, and layer 2 addressing services for user data. To ensure integrity in noisy environments, DNP3 uses embedded checksums in all packet layers. DNP3 can use TCP/IP for transport. DNP3 transactions involve control requests sent by Master Stations and data responses sent by outstations (RTUs and IEDs). Each request has a single response, although masters can send multiple requests simultaneously. In some DNP3 implementations, outstations can send unsolicited responses for specific situations.

Each request and response contains DNP3 information in three networking layers: Application, Transport, and Data Link. These layers comprise the Enhanced Performance Architecture (EPA) communication model, which is based upon the 7-layer OSI model:

- **Application Layer.** The Application Layer layer carries the function code that specifies the purpose of the message and information (in the form of DNP3 objects) about the requested data.
- **Transport Layer.** The transport layer carries fragments of application layer data and sequencing information. The message sender must fragment application data when the size of message fragment exceeds the maximum segment size that can be handled by the data link layer. Each fragment, known as a Transport Segment, is prepended with a transport header that specifies the position of the fragment in the relation to other Transport Segments.
- **Data Link Layer.** The Data Link layer encapsulates Transport Segments received from the Transport layer within data link frames acceptable to the communication channel. Upon message receipt, this layer extracts Transport Segments from their frames and passes up to the Transport layer. The Data Link layer also detects integrity errors using Cyclic Redundancy Checks (CRC), contains the source and destination addresses, and manages frame synchronization.

DNP3 Select & Operate Requests

Masters send DNP3 Select and Operate messages to instruct an outstation to prepare specific output points for data transfer. A Select message instructs an outstation to select data points, as directed by the data objects in the message; a Operate message instructs an outstation to activate those points. Selected points are not activated until the outstation receives a corresponding Operate message from the master.

Within each message, the Application layer carries the function code that specifies the purpose of the message and information about the data points (in the form of DNP3 objects) the receiver should select:

- For **Select** messages, the function code is 03 and the payload contains Select Data Objects.
- For **Operate** messages, the function code is 04 and the payload contains Operate Data Objects.

select.datalink.payload.string.utf-8

More Systematic Vulnerability Assessment

ICE-CERT's Assessment Program[1]

- **A dedicated federal facilities assessment team**
- **A dedicated private sector assessment team**

ICS-CERT offers a combination of processes in support of an integrated assessment product suite. Assessment products and services include

- Cybersecurity Evaluation Tool (CSET)
- Design Architecture Review (DAR)
- Network Validation and Verification (NAVV)

ICS-CERT's cybersecurity assessment services include evaluation of ICS design architecture, verification and validation of network traffic, and systems log review and analysis. An evaluation of the design architecture includes a high level preliminary evaluation of the site security posture, leveraging CSET, followed by an in-depth review and evaluation of the ICS network design, configuration, and inter-connectivity to internal and external systems. This system analysis provides ICS asset owners with a comprehensive cybersecurity evaluation focusing on defensive strategies associated with their specific control systems network.

Network data traffic analysis provides asset owners with information to identify anomalous and potentially suspicious communications sourced from, or destined for, control systems assets. This service offering provides a sophisticated analysis of the asset owner's network traffic, which asset owners collect, from within their control system network environment. ICS-CERT subject matter experts (SME) analyze the captured network traffic using a combination of open source and commercially available tools to develop a detailed representation of the communications, flows, and relationships between devices.

[1] **ICS-CERT Annual Assessment Report, FY 2016**

Outline of **Module 8**

- Vulnerability Assessment Tools
- SIEM tools
- Intrusion Detection (IDS) Tools
- Vulnerability and Security Assessment
- Vulnerability Disclosure Policy

What's SIEM?

SIEM (Security Info & Event Management) is defined as a group of complex technologies that together provide a bird's-eye view into an infrastructure.

- It provides centralized security event management
- It provides correlation and normalization for context and alerting
- It provides reporting on all ingested data
- It can take in data from multiple vendor or in-house applications

SIEM Tools: **Windows Defender Exploit Guard**

- Enterprise security administrators (Windows 10 version 1709)
- Host intrusion prevention that reduce the attack surface of apps used by systems/employees

<u>Features of Windows Defender EG</u>

- Exploit Protection
- Attack Surface Reduction Rules
- Network Protection
- Controlled folder access

Exploit Protection

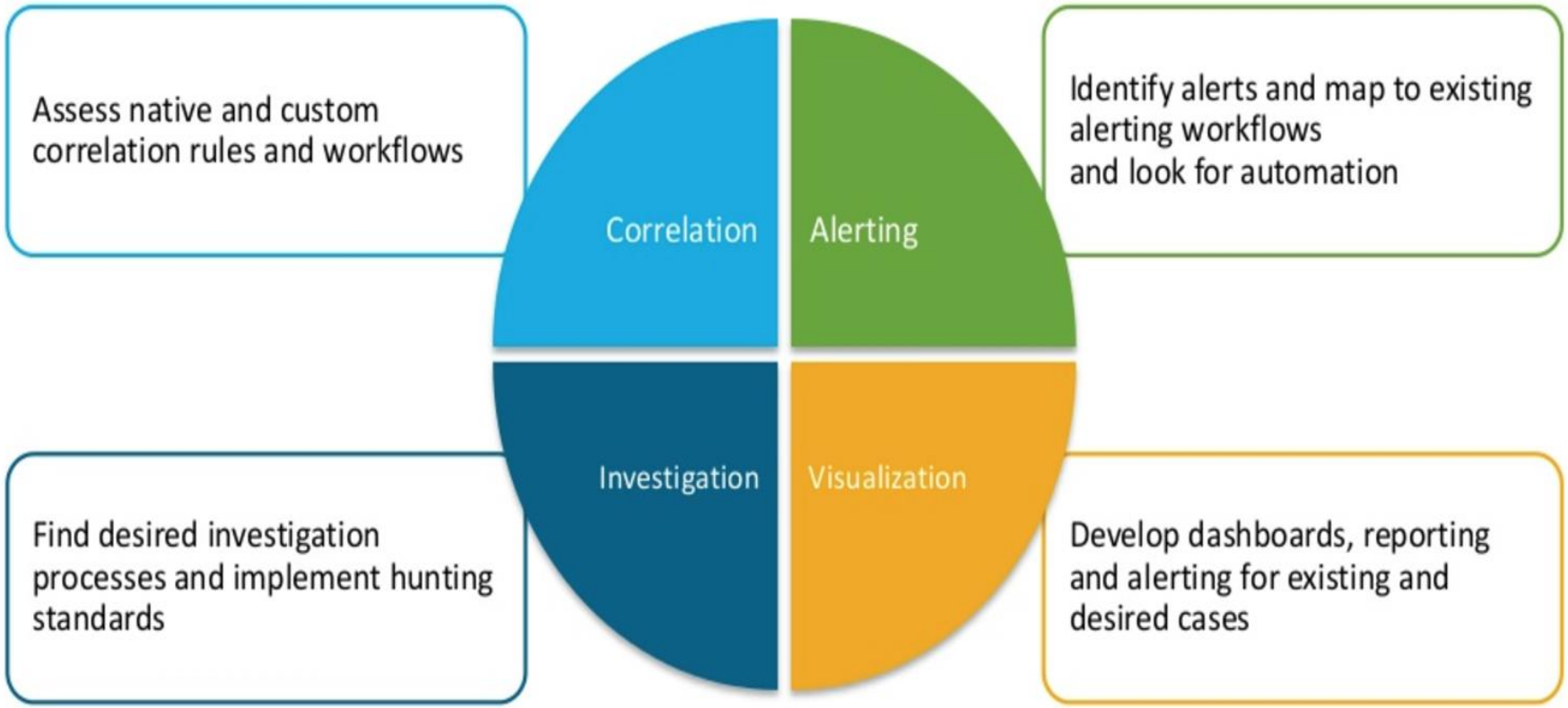
- It applies exploit mitigation techniques to apps
- Protects devices from malware that use exploits to spread and infect
- Mitigations that can be applied at either the OS level, or at the individual app level
- Detailed reporting of events and blocks as alert investigation scenarios.
- Can configure these settings using the Windows Defender Security Center app or PowerShell
- Export the configuration as an XML file that you can deploy to other machines (Group policy)

Exploit Protection Continued...

- Customize the notification when Mitigation is encountered
- Can enable the rules individually
- **Audit mode** to evaluate how Exploit protection would impact organization
- Can test how the feature will work in organization to ensure it doesn't affect business apps, and to get an idea of how many suspicious or malicious events generally occur over a certain period
- Windows Defender Security Center app
- Group Policy
- PowerShell

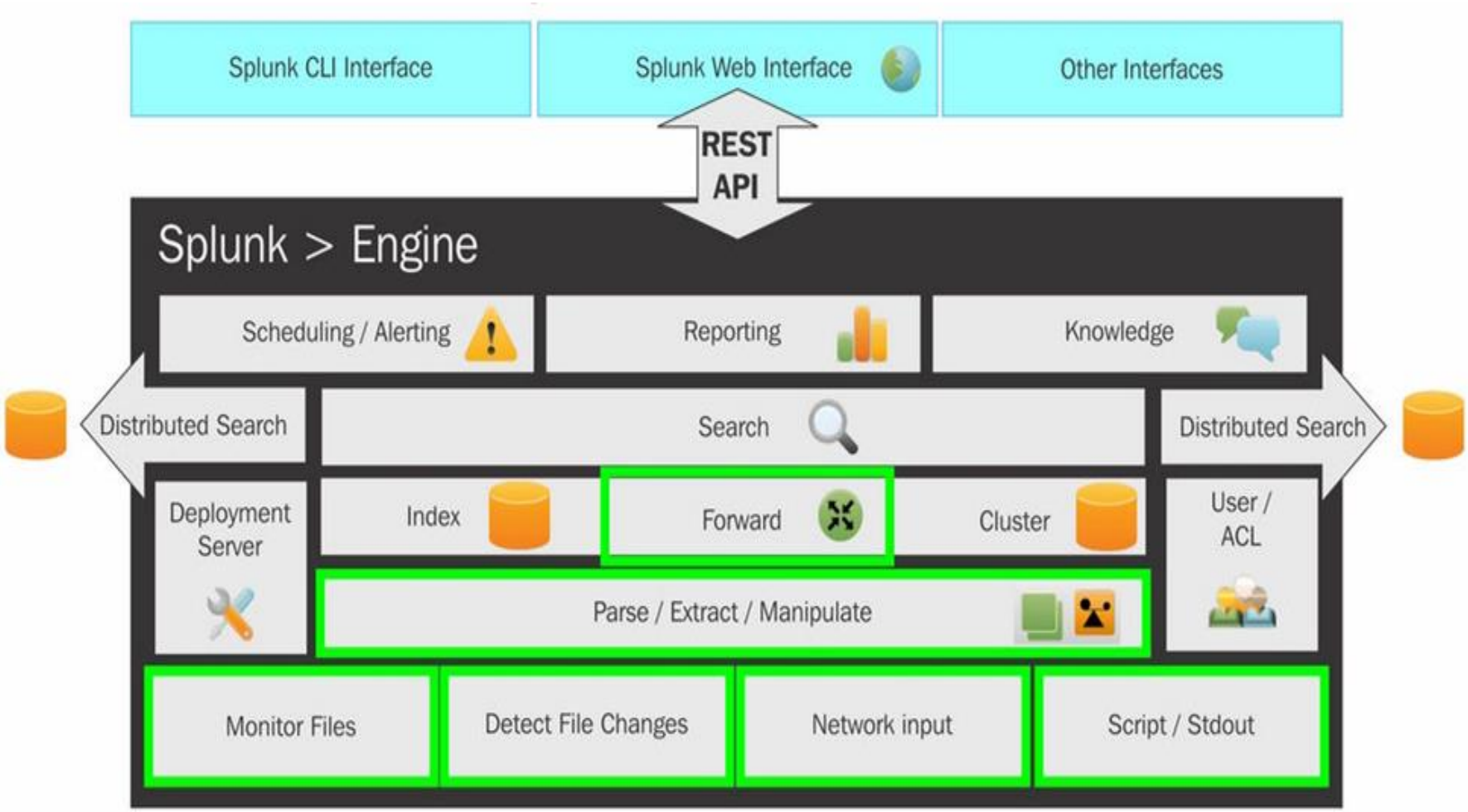
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/customize-exploit-protection

SIEM Tools: **Splunk**



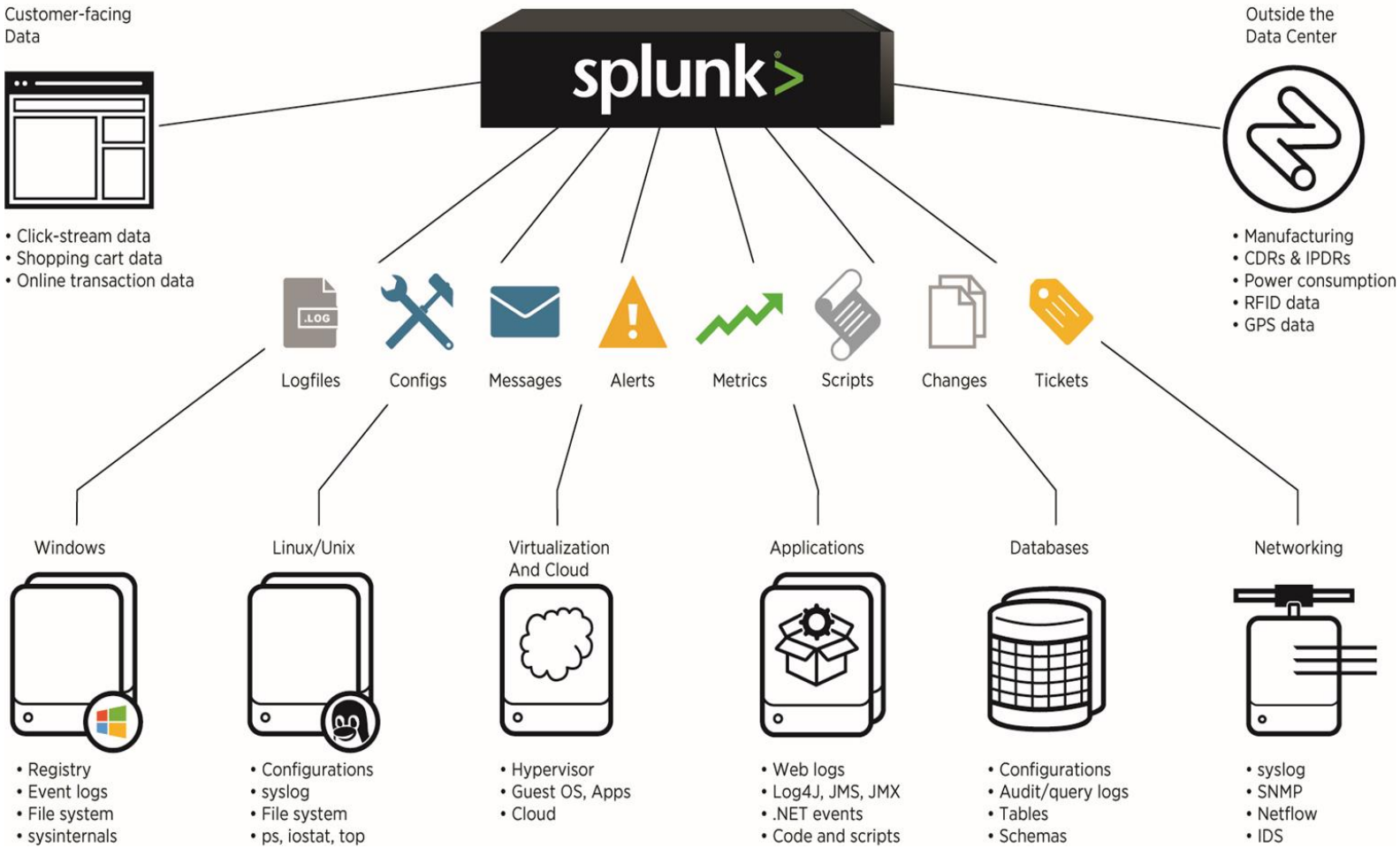
https://www.slideshare.net/RisiAvila/pptsplunklegacysiem101final

Architecture



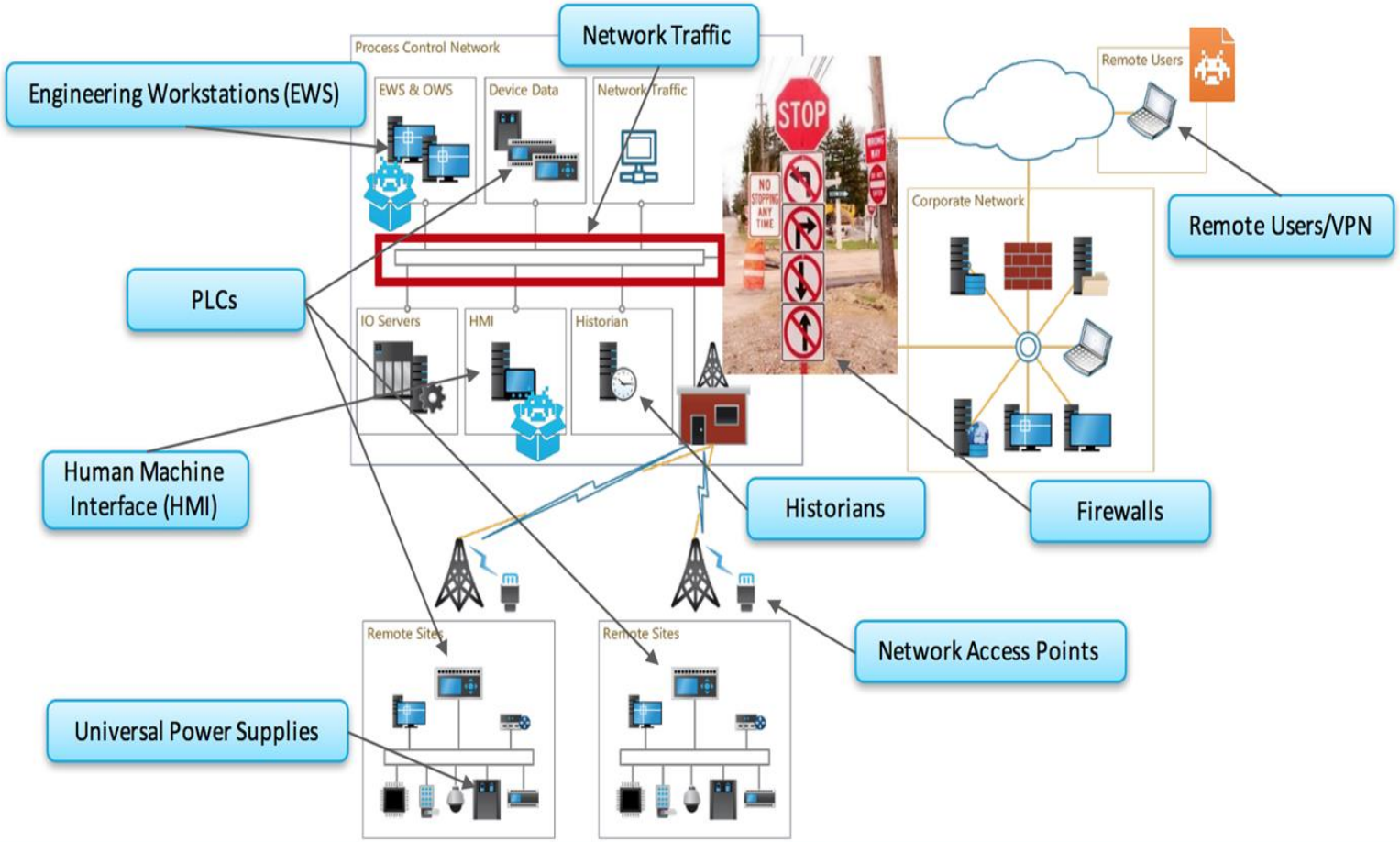
https://community.blackboard.com/thread/5120-splunk-architecture

Splunk Input/Output



http://dev.splunk.com/view/dev-guide/SP-CAAAE3A

Splunk Input/Output



https://www.splunk.com/pdfs/presentations/govsummit/saf-ics-dynamic-risk-monitoring-and-protection-of-ics-scada-and-other-critical-infrastructure.pdf

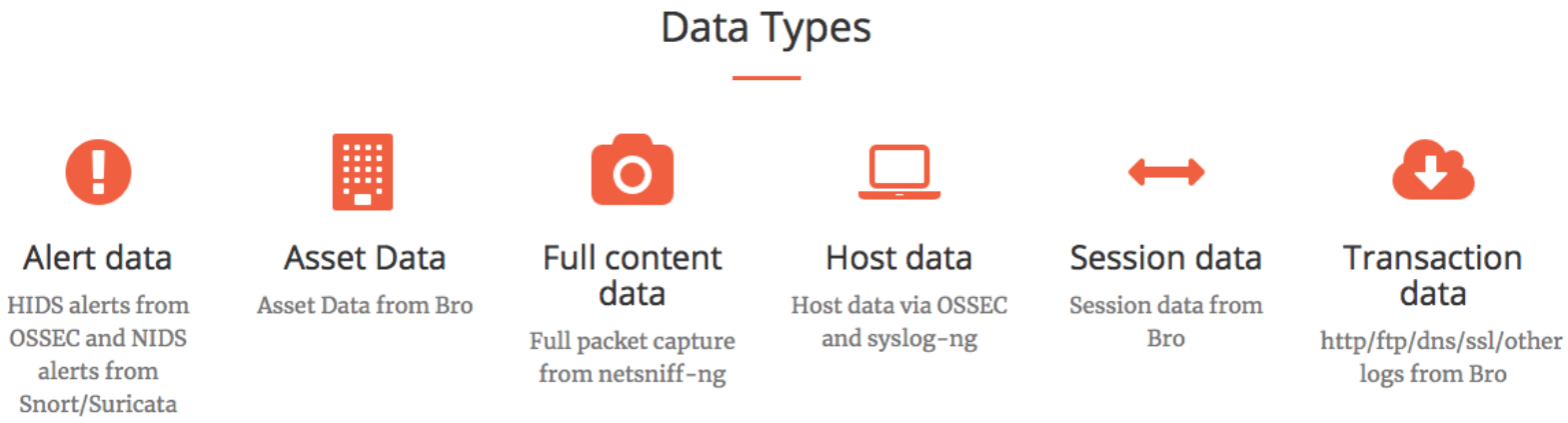
Splunk Applications in the Grid

- Live data feed from energy operators
- Telemetry logs
- SCADA system events
- Modbus data engine events
- Infrastructure management systems
- Anomalous VPN Traffic
- Firmware Changes
- Operational/Mechanical Failures
- Rogue Device Detection
- Spurious RF Emissions
- Network Reconnaissance Scans
- Reported Vulnerabilities

https://www.splunk.com/pdfs/customer-success-stories/splunk-at-enernoc.pdf

SIEM Tools: **Security Onion**

Security Onion is a Linux-based tool for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other security tools [1].



[1] https://securityonion.net

SIEM Tools: **Security Onion**

Open source

IDS:

- Rule driven : Snort,
- Analysis driven : Bro

Analysis tools:

- Sguil: Centralized syslog framework. IDS alerts
- Elsa: Log receiver, serchier, indexer

Build your own custom dashboards using ELSA

Top NIDS Alerts

sig_msg	Count
ET TROJAN Gh0st Remote Access Trojan Encrypted Session To CnC Server	321
ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102	298
ET TROJAN Backdoor family PCRat/Gh0st CnC traffic	297
ET CURRENT_EVENTS DRIVEBY Nuclear EK Payload	139
ET INFO EXE - Served Inline HTTP	72

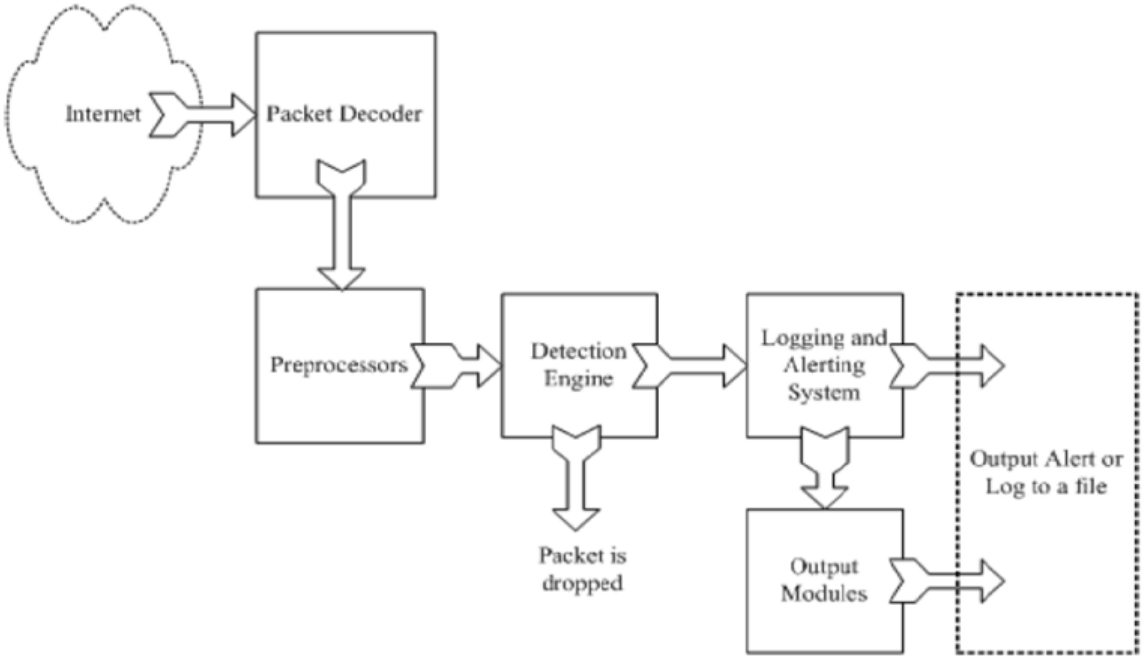
Can write custom scripts and signatures

https://securityonion.net

IDS Tools: Snort

What is Snort?

It is an open source intrusion prevention system capable of real-time traffic analysis and packet logging.



IDS Tools: Snort

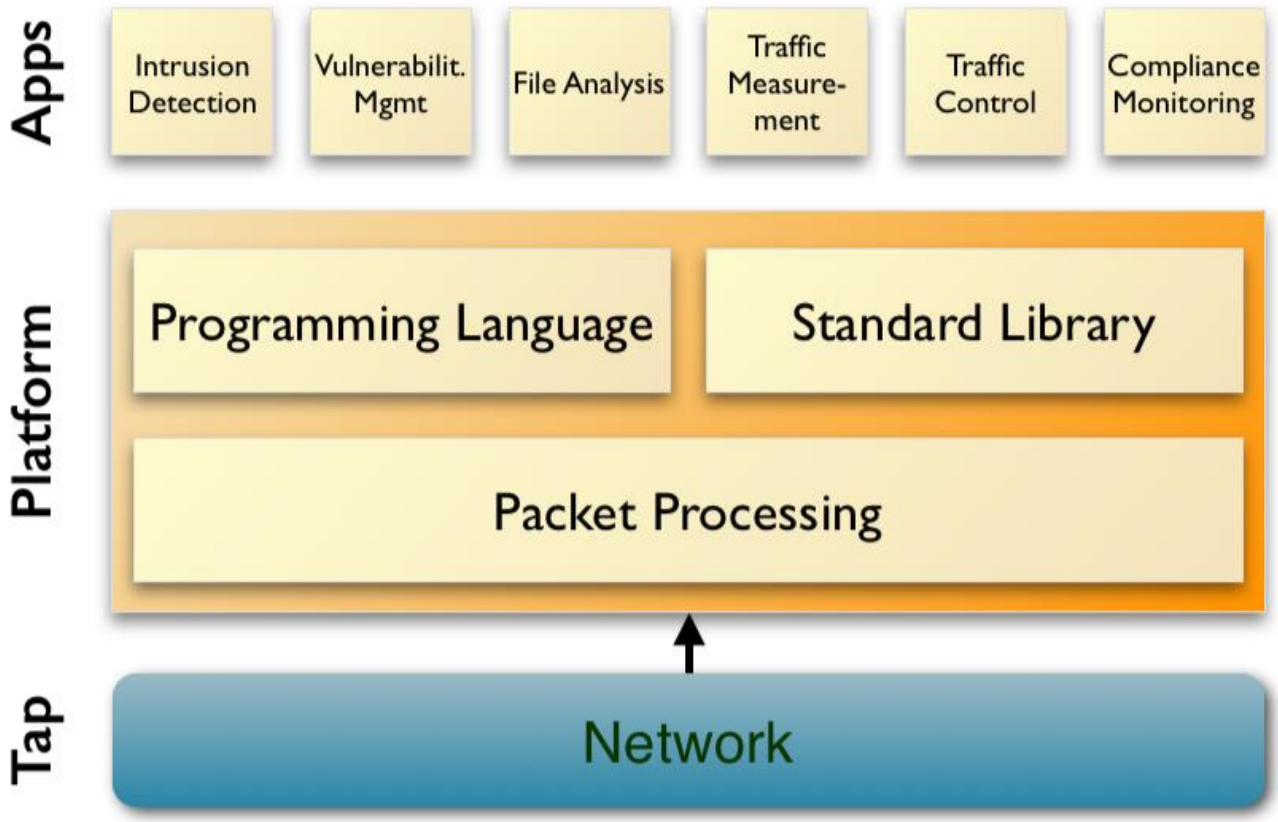
Packet Decoder: Takes packets from the different network interfaces and prepares packets to be preprocessed.

Preprocessor: Packets are arranged or modified before sending them to the detection Engine. Detect anomalies. Perform packet reassembly

Detection Engine: Detect if any intrusion activity exists in the packet. Snort rules. If a packet matches any rule an appropriate action is taken such as logging or dropping a packet

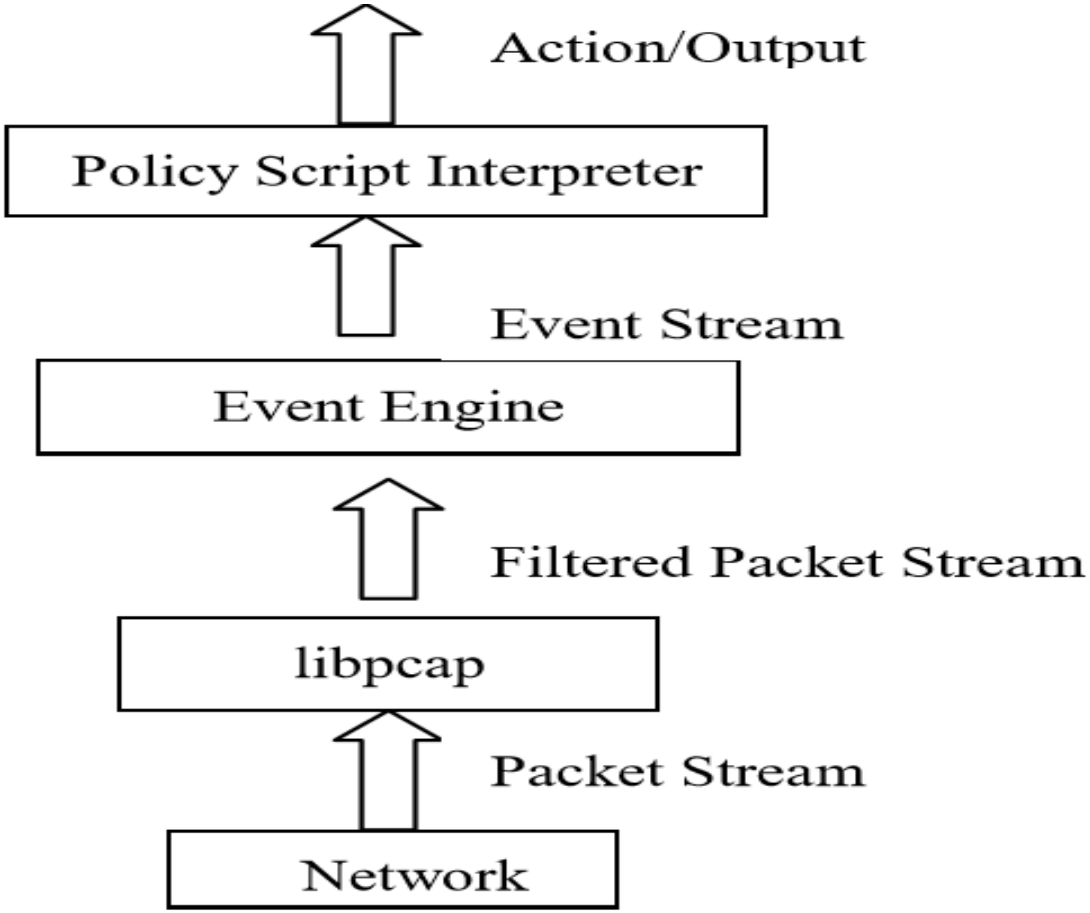
Logging and Alerting System: Generate alerts and log messages depending upon what the detection engine finds inside a packet

IDS Tools: Bro



https://www.bro.org/current/slides/broverview-2015.pdf

IDS Tools: Bro



IDS Tools: Bro

Libpcap: Pcap library to capture packets from the network interfaces. Takes care of all the traffic that comes from the network layer. Filters non important elements

Event Engine: Captures packets and put them together to become events explaining the performed actions

Policy Script Interpreter: Compares high level events and compares these with policy scripts in the system. Events are stored in a FIFO list. Takes action if it detects suspicious and dangerous activities

IDS Tools Comparison

	Snort	Bro
Operation System	Any	Unix
High speed network capability	Medium	High
Thread	Single	Single
Clusters	No	Yes
IPS	yes	No
Community	Big	Small

Outline of **Module 8**

- Vulnerability Assessment Tools
- SIEM tools
- Intrusion Detection (IDS) Tools
- Vulnerability and Security Assessment
- Vulnerability Disclosure Policy

Vulnerability Assessment Tools: Shodan

Shodan – A search engine using crawlers to get device/service data visible on the public network. It's used to earch for internet-facing SCADA/ICS devices/systems.

The basic algorithm for the crawlers is[1]:

1. Generate a random IPv4 address
2. Generate a random port to test from the list of ports that Shodan understands
3. Check the random IPv4 address on the random port and grab a banner
4. Go to 1

[1] John Matherly, "Complete Guide to Shodan"

Vulnerability Assessment Tools: Shodan

Shodan | Developers | Book | View All... | Show API Key | Help Center

SHODAN | country:US vuln:CVE-2014-0160 | Explore | Downloads | Reports | Developer Pricing | Enterprise Access | Contact Us | My Account | Upgrade

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

28,976

TOP COUNTRIES

United States	28,976

TOP CITIES

Ashburn	1,465
Los Angeles	1,275
Phoenix	808
Thousand Oaks	792
New York	446

TOP SERVICES

HTTPS	21,523
HTTPS (8443)	3,407
9443	1,640
Webmin	635
WHM + SSL	287

TOP ORGANIZATIONS

Verizon Wireless	2,914
Amazon.com	1,954
Comcast Cable	1,369
Comcast Business	1,033
Time Warner Cable	974

TOP OPERATING SYSTEMS

Linux 3.x	486
Linux 2.6.x	38
Linux 2.4-2.6	8
Windows 7 or 8	6
Windows XP	5

Frontier
50.43.81.38
static-50-43-81-38.bvtn.or.frontiernet.net
Frontier Communications
Added on 2018-03-13 20:46:29 GMT
United States, Hillsboro
Details
Affected by: Heartbleed

SSL Certificate
Issued By:
|- Common Name: Jungo CA
Issued To:
|- Common Name: 192.168.1.1
Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Content-Type: text/html
Set-Cookie: rg_cookie_session_id=2046701718; path=/; HttpOnly
Cache-Control: no-cache,no-store
Pragma: no-cache
Expires: Tue, 13 Mar 2018 20:44:03 GMT
Date: Tue, 13 Mar 2018 20:44:03 GMT
Accept-Ranges: bytes
Connection: close
```

"Banner" - a piece of textual info returned by the crawlers.

cPanel Login
50.31.2.239
ip239.50-31-2.static.steadfastdns.net
Steadfast
Added on 2018-03-13 20:45:18 GMT
United States, Chicago
Details
Affected by: Heartbleed

SSL Certificate
Issued By:
|- Common Name: cPanel, Inc.
Certification Authority
|- Organization: cPanel, Inc.
Issued To:
|- Common Name:
vm.featheredhorse.com
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 401 Access Denied
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Tue, 13 Mar 2018 20:45:16 GMT
Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: cpsession=%3aW71PUiFoIOnaK5lw%2c845498abf2c758f24313023f2...
```

Apache HTTP Server Test Page powered by CentOS
172.241.78.20
servey-mail.online
Leaseweb USA
Added on 2018-03-13 20:43:39 GMT
United States, Phoenix
Details
Affected by: Heartbleed

SSL Certificate
Issued By:
|- Common Name:
vpn00234.saleyesterday.com
|- Organization: SomeOrganization
Issued To:
|- Common Name:
vpn00234.saleyesterday.com
|- Organization: SomeOrganization
Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Parameters
Fingerprint: RFC3526/Oakley Group 14

```
HTTP/1.1 403 Forbidden
Date: Tue, 13 Mar 2018 20:31:08 GMT
Server: Apache/2.2.15 (CentOS)
Accept-Ranges: bytes
Content-Length: 4961
Connection: close
Content-Type: text/html; charset=UTF-8
```

ICS devices that are found affected by Heartbleed in US.

Vulnerability Assessment Tools: Shodan

Shodan | Developers | Book | View All... | Show API Key | Help Center

SHODAN | category:ics country:IN | Explore | Downloads | Reports | Developer Pricing | Enterprise Access | Contact Us | My Account | Upgrade

Exploits | Maps | Images | Share Search | Download Results | Create Report

TOTAL RESULTS

19,715

TOP COUNTRIES

India	19,715

TOP CITIES

Jalandhar	1,235
Delhi	623
Mumbai	558
Gurgaon	284
New Delhi	256

TOP SERVICES

Automated Tank Gauge	15,661
DNP3	2,103
Mitsubishi MELSEC-Q	319
OMRON FINS	184
EtherNetIP	128

TOP ORGANIZATIONS

ApnaTeleLink pvt.	4,945
U.p. Communication Services Pvt	897
BSNL	677
Zapbytes Technologies Pvt.	605
Ishan's Network	292

TOP OPERATING SYSTEMS

Linux 3.x	11
Linux 2.6.x	1

TOP PRODUCTS

AG5-HP	7,531
LB5	1,660
P5B-300	1,285
N5B-300	1,192
P5B-400	792

183.82.122.115
broadband.actcorp.in
Atria Convergence Technologies pvt
Added on 2018-03-13 21:36:33 GMT
India, Hyderabad
Details

ICS devices visible in India.

103.244.121.123
Ishan's Network
Added on 2018-03-13 21:27:57 GMT
India
Details

```
Ubiquiti Networks Device
IP: 103.244.121.123
MAC: 44:d9:e7:56:1a:4c
Hostname: PowerBeam M5 400
Product: P5B-400
Version: XW.ar934x.v5.6.15.30572.170328.1052
```

139.59.22.76
Digital Ocean
Added on 2018-03-13 21:26:04 GMT
India, Bangalore
Details
cloud

```
HTTP/1.0 200 Document follows\r\nServer: MiniServ/1.720\r\nDate: Tue, 13 Mar 2018 21:26:04 GMT\r\nContent-type: text/html; Charset=iso-8859-1\r\nConnection: close\r\n\r\n<h1>Error - Document follows</h1>\n<p>This web server is running in SSL mode. Try the URL <a href=\'https://139.59.22.76:20000/...
```

103.199.146.6
Blue Lotus Support Services Pvt
Added on 2018-03-13 21:22:28 GMT
India, Chennai
Details

```
Ubiquiti Networks Device
IP: 103.199.146.6
MAC: 80:2a:a8:62:a8:2e
Alternate IP: 169.254.168.46
Alternate MAC: 80:2a:a8:62:a8:2e
Hostname: RWH Ap Idea
Product: AG5-HP
Version: XW.ar934x.v5.6.2.27929.150716.1149
```

1.186.61.210
1.186.61.210.dvois.com
D-Vois Broadband Pvt
Added on 2018-03-13 21:17:58 GMT
India
Details

```
Ubiquiti Networks Device
IP: 1.186.61.210
MAC: 04:18:d6:ea:12:fc
Alternate IP: 192.168.25.21
Alternate MAC: 04:18:d6:eb:12:fc
Hostname: NanoStation Loco M5
Product: LM5
Version: XW.ar934x.v5.5.9.21734.140403.1801
```

Vulnerability Assessment Tools: Shodan

Now try it yourself…

1. Open Shodan login page and login with one of the possible ways suggested

2. Specify a typical port number used by a typical service (e.g. 22, 23, 80, 20000, …) in the searching filter

3. Specify the 2 letter code of a country in the filter

4. Filter should look like “port:XX country:XX”

5. Find anything interesting?

NOTE: Please use it only for learning and improving the security

Project SHINE

- Project started in April 2012 to identify internet facing Critical Infrastructure devices
  - Does this by using a SHODAN search engine and searching control systems related terms
  - Used freely available tools to identify critical infrastructure devices on the internet

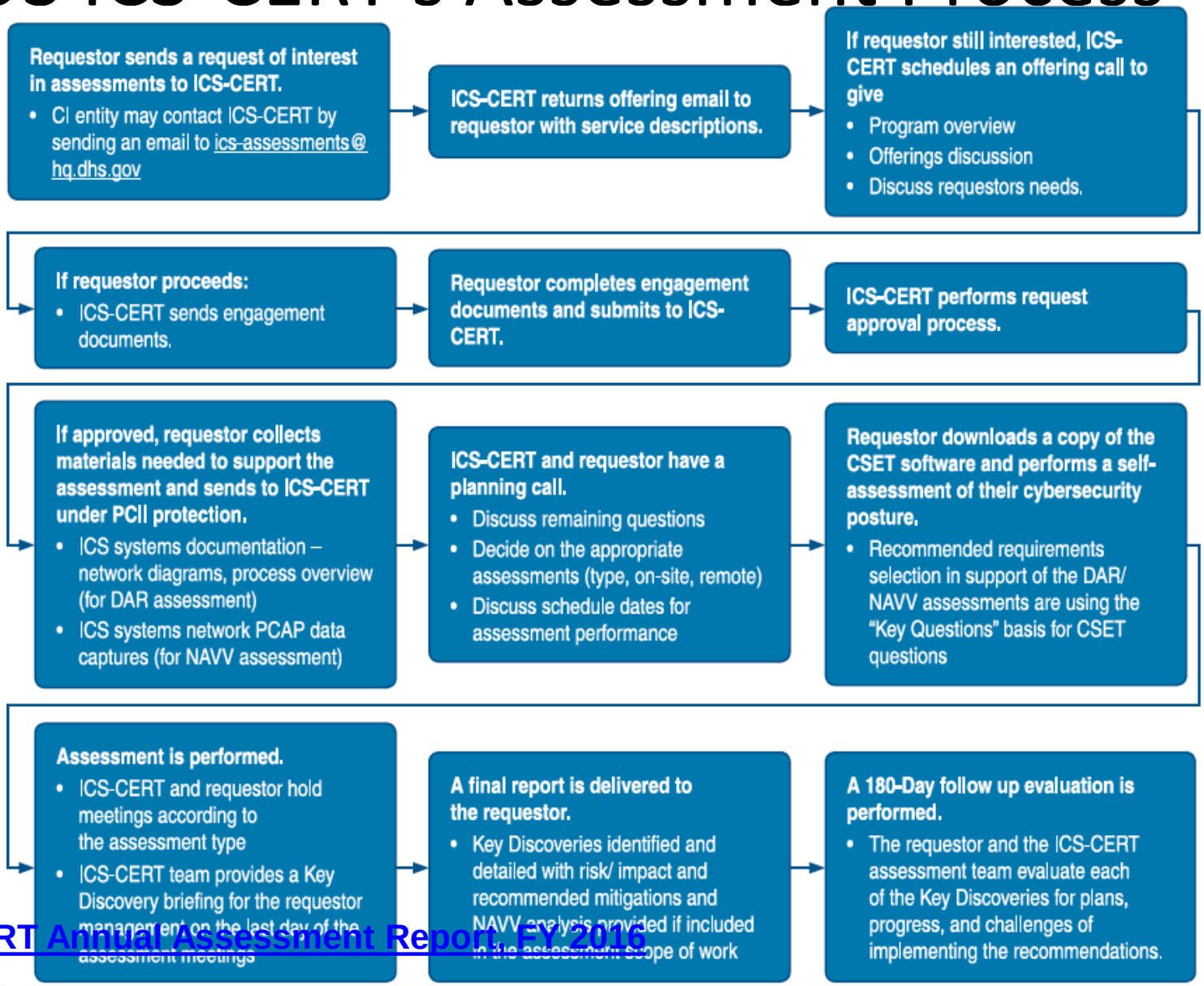
Source: http://www.ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

Project SHINE findings

- At the time of Oct. 2012 ~460,000 IP addresses are
  - *directly facing the internet*
  - related to critical infrastructure devices
- Several of the resources have weak, default or non-existent logon credential mechanisms
- These devices are an entry point into a control networks

Source: http://www.ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

US ICS-CERT's Assessment Process



[1] ICS-CERT Annual Assessment Report, FY 2016

Outline of **Module 8**

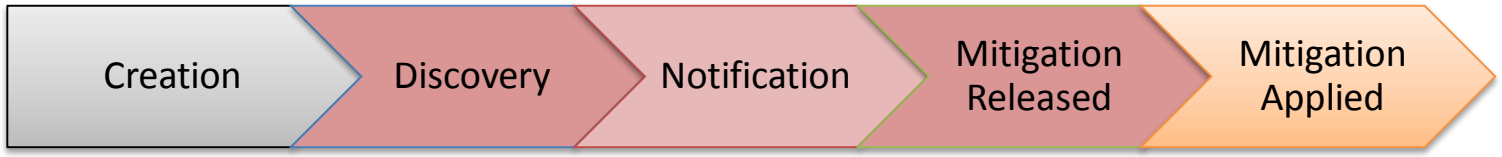
- Vulnerability Assessment Tools
- SIEM tools
- Intrusion Detection (IDS) Tools
- Vulnerability and Security Assessment
- **Vulnerability Disclosure Policy**

Vulnerability Lifecycle

Vendor mistake in design/development process

(Vendor/Coordinator/Researcher) disclose the vulnerability to utilities and/or general public

Utilities/System integrators work on testing, deploying patch



Vulnerability discovered by (Vendor/ Utility/Security Researcher/Attacker)

Vendor provides patch and/or configuration strategy to mitigate the issue

Vulnerability Disclosure: Parties Involved

Security Researchers	• Academia, national labs, independent security researchers • Substantially different objectives/ethics
Vendor	• Development of software (EMS, SCADA, substation automation) and hardware (PLCs, IEDs)
Customer	• Utilities/ISOs depending on vendor products
Coordinating Agency	• Trusted third party to help coordination/remediation • e.g. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Hahn, A.; Govindarasu, M., "Cyber vulnerability disclosure policies for the smart grid," Power and Energy Society General Meeting, 2012 IEEE , vol., no., pp.1,5, 22-26 July 2012

Responsible Vulnerability Disclosure Problem

Many vulnerabilities discovered by parties not affiliated with the vendor

- Security researchers are often academia, national labs, utility, independent security researchers

Vulnerability information needs to be disclosed to both the public and vendor

- Vendors need to create patches/mitigation
- Utilities need to develop work arounds, update IDS alerts

But…

- Researchers often distrust vendors
- Vendors notorious for delaying mitigation

Disclosure strategies

Full Disclosure	Limited Disclosure	Non Disclosure

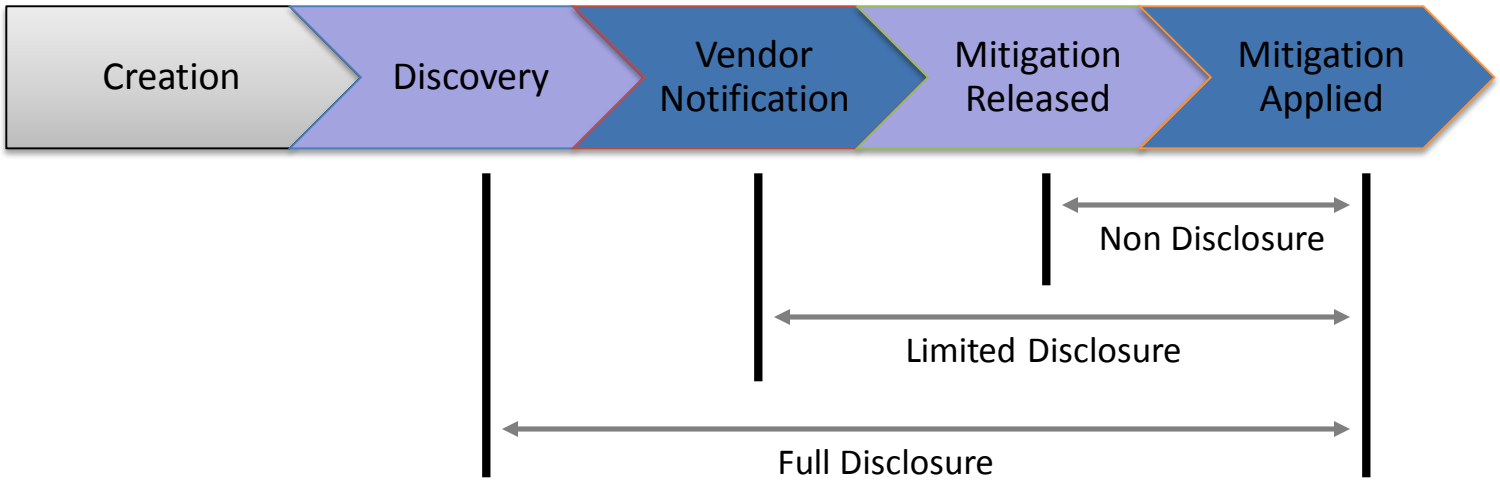
• Researcher immediately discloses all information to the public.
• *Advantages* –
  • vendors pressured to create timely mitigation
• *Disadvantages* –
  • Increased risk from exposed, but unmitigated vulnerabilities
	• Research informs vendor and potentially coordinating agency
	• *Advantages* –
	  • Information not released to public until mitigation available
	• *Disadvantage*
	  • Vendors historically delay mitigation deployment
		• Vulnerability data not released to public
		• *Advantages* –
		  • Potential attackers never alerted about vulnerability
		• *Disadvantages* –
		  • Little incentive for vendor to release mitigation
		  • Utilities unaware of importance of deploying patches/mitigations

Limiting disclosed/unmitigated vulnerabilities

Increase public awareness of issue

Risk from Unpatched Vulnerabilities

- Length of time between public disclosure and applied mitigation directly



Risk from disclosed/unmitigated vulnerabilities

Industry Goal

Influence "Limited Disclosure" practices within the security research community.

- "Vulnerability Disclosure Framework" National Infrastructure Advisory Council (NIAC), 2004 [NIAC 04]
  - Provides a guideline for stakeholders
  - Vendor specific advice includes:
    - 1) Public vulnerability management pages on their website.
    - 2) Mechanisms to support vulnerability reports (such as a email address or web form).
    - 3) A defined time frame for acknowledging the received report.
    - 4) A public security advisory notification method.

[NIAC 04]: National Infrastructure Advisory Council (NIAC). Vulnerability disclosure framework, Jan. 2004.

Vulnerability Disclosure

ICS-CERT Advisory

- An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks. (http://ics-cert.us-cert.gov)

NERC ES-ISAC

- "Facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and practices". (http://www.nerc.com)

ICS CERT Advisory

- A typical ICS-CERT Advisory contains:
  - **Affected products**
  - **Impact**
  - **Background**
  - **Vulnerability Characterization**
    - **Vulnerability Overview**
    - **Vulnerability Details**
      - **Exploitability**
      - **Existence of Exploit**
      - **Difficulty**
  - **Mitigation**

Example of an ICS CERT Advisory

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-102-05—SIEMENS SCALANCE S SECURITY MODULES MULTIPLE VULNERABILITIES

April 11, 2012

OVERVIEW

ICS-CERT has received a report from Siemens regarding two security vulnerabilities in the Scalance S Security Module firewall. This vulnerability was reported to Siemens by Adam Hahn and Manimaran Govindarasu for coordinated disclosure.

The first issue is a brute-force credential guessing vulnerability in the web configuration interface of the firewall. The second issue is a stack-based buffer overflow vulnerability in the Profinet DCP protocol stack.

Siemens has published a patch that resolves both of the identified vulnerabilities.

AFFECTED PRODUCTS

The following Scalance S Security Modules are affected:

- Scalance S602 V2
- Scalance S612 V2
- Scalance S613 V2

IMPACT

Successful exploitation of the brute-force vulnerability may allow an attacker to perform an arbitrary number of authentication attempts using different password and eventually gain access to the targeted account.

Successful exploitation of the stack-based buffer overflow against the Profinet DCP protocol may lead to a denial of service (DoS) condition or possible arbitrary code execution.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

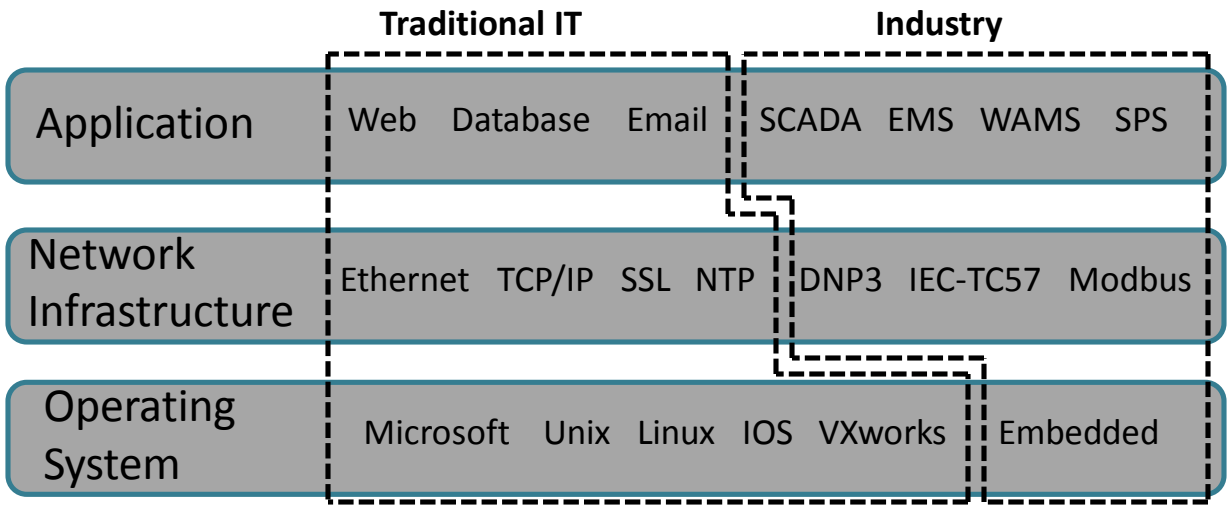
The Scalance S product is a security module that includes a Stateful Inspection Firewall for industrial automation network applications. This security module is intended to protect automation devices and

Current Vendor Disclosure Policies

	Coordinators		IT Vendors		Open Source		Industry vendors	
	CERT/CC	ICS-CERT	Microsoft	Google	Ubuntu	FreeBSD	SEL	Siemens
Policy Location	Webpage	Webpage	Webpage	Webpage	Webpage	Webpage	Document	Webpage
Disclosure Method	Limited	Limited	Limited	Limited	**Full**	Limited	Limited	Limited
Vuln. Mgmt. Page	Yes	Yes	Yes	Yes	Yes	Yes	**No**	Yes
Publish Time	**45 days**	Variable	Variable	**60 days**	Variable	Variable	Variable	Variable
Security Advisory	Technical notes, NVD	Technical notes, NVD	Security Bulletin, Advisories	Blog postings	Webpage, Email list	Security Advisories	Service Bulletins, Release Notes	Security Advisories
Discoverer Support	Public Acknowledgement	Public Acknowledgement	Public Acknowledgement	**Public Acknowledgement/Money**	Public Acknowledgement	Public Acknowledgement	**Not Specified**	Public Acknowledgement

Future Directions

– Heterogeneous environment with both industry-specific and traditional IT software



– Must be able to flexibly manage vulnerabilities discovered in both domains

Summary of the module

- Vulnerability Assessment Tools for used to find vulnerabilities in systems, protocols, devices. It's typically on testbed environments

- SIEM tools for used for event/log monitoring from multiple software/systems, and for dashboard

- IDS tools used for intrusion/anomaly detection and they can be integrated into SIEM

- Vulnerability and Security Assessment needs to systematic, and ICS-CERT has sound methodology

- Vulnerability disclosure policy is evolving