The Sweet Spot of Cyber Intelligence

16-November-2015

Tieu Luu, Sr. Director, Advanced Technology Group, SuprTEK

Jay Ruhnke, Sr. Architect, Advanced Technology Group, SuprTEK

SUPRTEK
ADVANCED TECHNOLOGY GROUP

About Our Company

SUPRTEK

Established in 1996, SuprTEK develops innovative software solutions to support our government clients in cyber security, healthcare, and defense missions.

Exceptional Solutions with Proven Results

www.suprtek.com

Agenda

- Cyber Intelligence
- Information Security Continuous Monitoring
- Threat Intelligence
- Information Overload
- The Sweet Spot
- Data Models and Standards
- How Do We Do This?
- Our R&D Efforts

SUPRTEK
ADVANCED TECHNOLOGY GROUP

Cyber Intelligence

Understanding of what’s
running on your networks

+

Awareness of what your
adversaries are up to

Intelligence Gathering, Information Sharing and Analytics

SUPRTEK
ADVANCED TECHNOLOGY GROUP

Lots of Money Being Thrown At It

$1.6B

Size of the SIEM market in 2014 (Gartner)

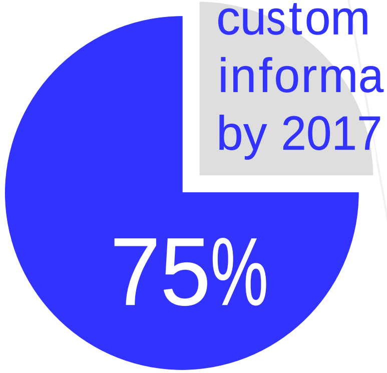
$3.2B

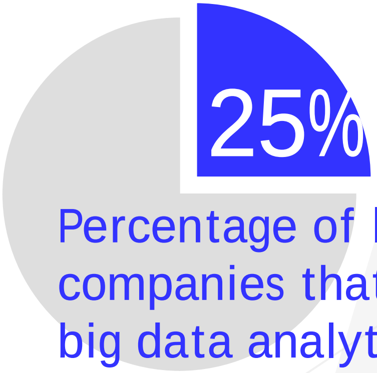
Size of the global security analytics market by 2018 (Markets & Markets)

$5.8B

Size of threat intelligence security market by 2020 (Research & Markets)

Percentage of large enterprises that will receive custom threat intelligence information tailored to them by 2017 (IDC)



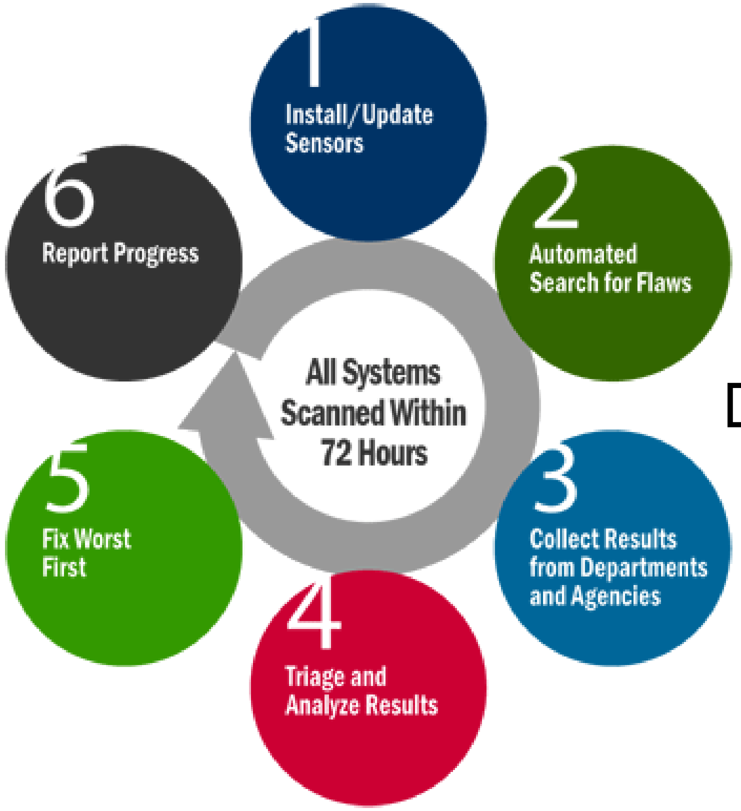


Percentage of large global companies that will have adopted big data analytics for at least one security use case by 2016 (Gartner)

SUPRTEK
ADVANCED TECHNOLOGY GROUP

Related Government Initiatives

NIST SP800-137



1 Install/Update Sensors
2 Automated Search for Flaws
3 Collect Results from Departments and Agencies
4 Triage and Analyze Results
5 Fix Worst First
6 Report Progress
All Systems Scanned Within 72 Hours

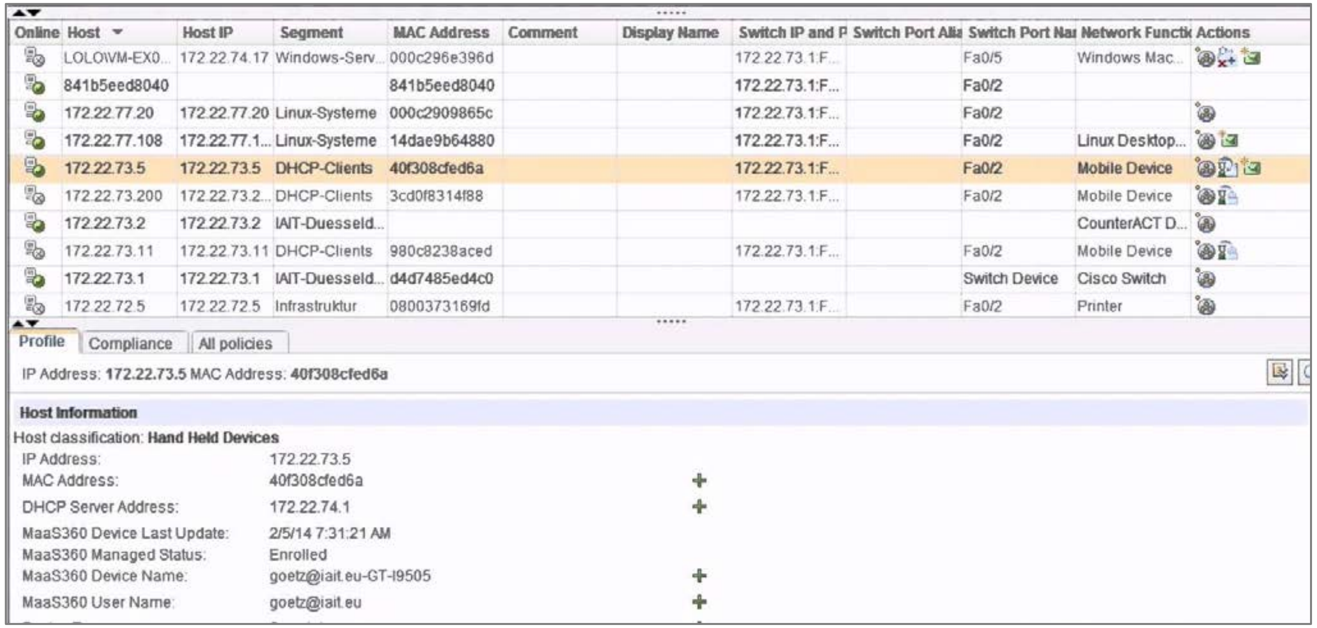
DHS Continuous Diagnostics & Mitigation (CDM)

Cybersecurity Information Sharing Act of 2015 (CISA)

Cyber Threat Intelligence Integration Center

OMB M-14-03

Understanding of What’s Running on Your Networks …



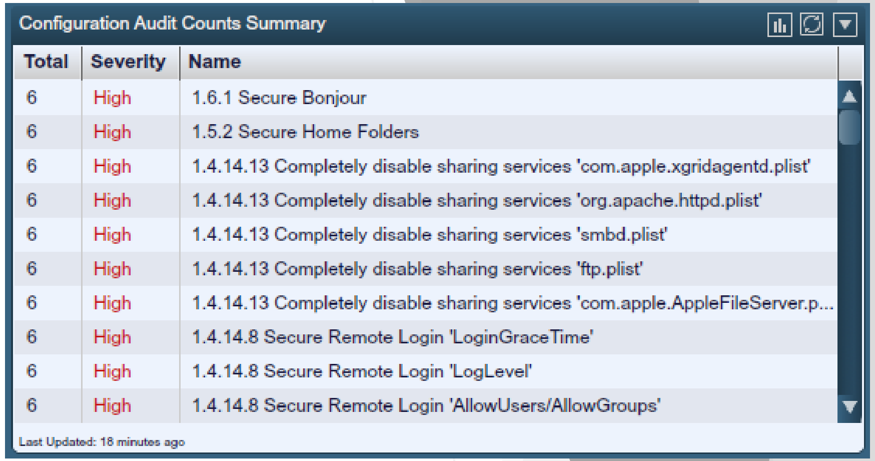
Online	Host	Host IP	Segment	MAC Address	Comment	Display Name	Switch IP and P	Switch Port Alia	Switch Port Nar	Network Functio	Actions
	LOLOWM-EX0...	172.22.74.17	Windows-Serv...	000c296e396d			172.22.73.1:F...		Fa0/5	Windows Mac...	
	841b5eed8040			841b5eed8040			172.22.73.1:F...		Fa0/2		
	172.22.77.20	172.22.77.20	Linux-Systeme	000c2909865c			172.22.73.1:F...		Fa0/2		
	172.22.77.108	172.22.77.1...	Linux-Systeme	14dae9b64880			172.22.73.1:F...		Fa0/2	Linux Desktop...	
	172.22.73.5	172.22.73.5	DHCP-Clients	40f308cfed6a			172.22.73.1:F...		Fa0/2	Mobile Device	
	172.22.73.200	172.22.73.2...	DHCP-Clients	3cd0f8314f88			172.22.73.1:F...		Fa0/2	Mobile Device	
	172.22.73.2	172.22.73.2	IAIT-Duesseld...							CounterACT D...	
	172.22.73.11	172.22.73.11	DHCP-Clients	980c8238aced			172.22.73.1:F...		Fa0/2	Mobile Device	
	172.22.73.1	172.22.73.1	IAIT-Duesseld...	d4d7485ed4c0					Switch Device	Cisco Switch	
	172.22.72.5	172.22.72.5	Infrastruktur	0800373169fd			172.22.73.1:F...		Fa0/2	Printer	

IP Address: **172.22.73.5** MAC Address: **40f308cfed6a**

Host Information

Host classification: **Hand Held Devices**

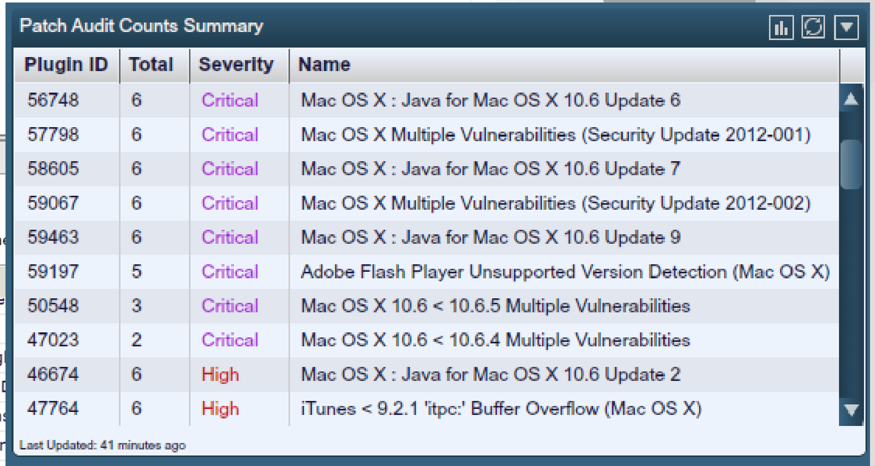
IP Address:	172.22.73.5
MAC Address:	40f308cfed6a
DHCP Server Address:	172.22.74.1
MaaS360 Device Last Update:	2/5/14 7:31:21 AM
MaaS360 Managed Status:	Enrolled
MaaS360 Device Name:	goetz@iait.eu-GT-I9505
MaaS360 User Name:	goetz@iait.eu



Configuration Audit Counts Summary

Total	Severity	Name
6	High	1.6.1 Secure Bonjour
6	High	1.5.2 Secure Home Folders
6	High	1.4.14.13 Completely disable sharing services 'com.apple.xgridagentd.plist'
6	High	1.4.14.13 Completely disable sharing services 'org.apache.httpd.plist'
6	High	1.4.14.13 Completely disable sharing services 'smbd.plist'
6	High	1.4.14.13 Completely disable sharing services 'ftp.plist'
6	High	1.4.14.13 Completely disable sharing services 'com.apple.AppleFileServer.p...
6	High	1.4.14.8 Secure Remote Login 'LoginGraceTime'
6	High	1.4.14.8 Secure Remote Login 'LogLevel'
6	High	1.4.14.8 Secure Remote Login 'AllowUsers/AllowGroups'

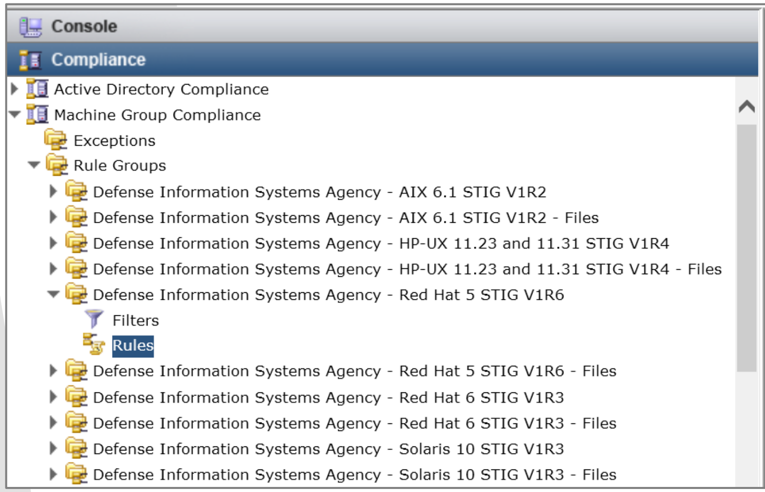
Last Updated: 18 minutes ago



Patch Audit Counts Summary

Plugin ID	Total	Severity	Name
56748	6	Critical	Mac OS X : Java for Mac OS X 10.6 Update 6
57798	6	Critical	Mac OS X Multiple Vulnerabilities (Security Update 2012-001)
58605	6	Critical	Mac OS X : Java for Mac OS X 10.6 Update 7
59067	6	Critical	Mac OS X Multiple Vulnerabilities (Security Update 2012-002)
59463	6	Critical	Mac OS X : Java for Mac OS X 10.6 Update 9
59197	5	Critical	Adobe Flash Player Unsupported Version Detection (Mac OS X)
50548	3	Critical	Mac OS X 10.6 < 10.6.5 Multiple Vulnerabilities
47023	2	Critical	Mac OS X 10.6 < 10.6.4 Multiple Vulnerabilities
46674	6	High	Mac OS X : Java for Mac OS X 10.6 Update 2
47764	6	High	iTunes < 9.2.1 'itpc:' Buffer Overflow (Mac OS X)

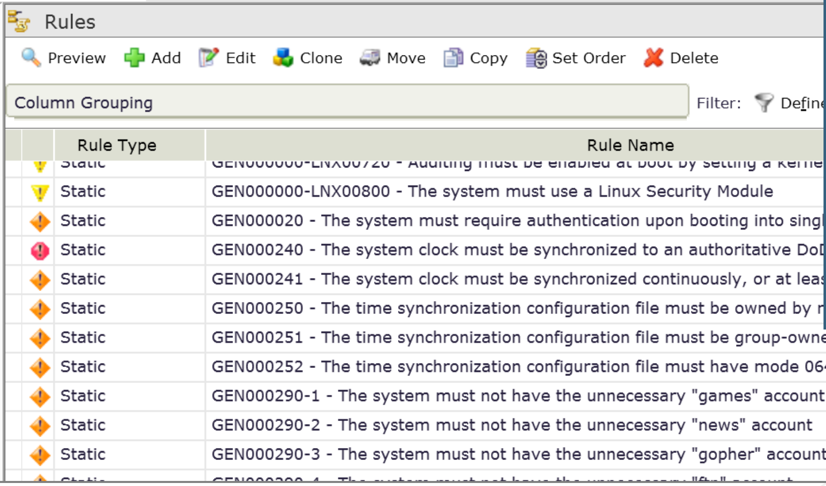
Last Updated: 41 minutes ago



Console

Compliance

- Active Directory Compliance
- Machine Group Compliance
  - Exceptions
  - Rule Groups
    - Defense Information Systems Agency - AIX 6.1 STIG V1R2
    - Defense Information Systems Agency - AIX 6.1 STIG V1R2 - Files
    - Defense Information Systems Agency - HP-UX 11.23 and 11.31 STIG V1R4
    - Defense Information Systems Agency - HP-UX 11.23 and 11.31 STIG V1R4 - Files
    - Defense Information Systems Agency - Red Hat 5 STIG V1R6
      - Filters
      - Rules
    - Defense Information Systems Agency - Red Hat 5 STIG V1R6 - Files
    - Defense Information Systems Agency - Red Hat 6 STIG V1R3
    - Defense Information Systems Agency - Red Hat 6 STIG V1R3 - Files
    - Defense Information Systems Agency - Solaris 10 STIG V1R3
    - Defense Information Systems Agency - Solaris 10 STIG V1R3 - Files



Rules

	Rule Type	Rule Name
!	Static	GEN000000-LNX00720 - Auditing must be enabled at boot by setting a kerne
!	Static	GEN000000-LNX00800 - The system must use a Linux Security Module
!	Static	GEN000020 - The system must require authentication upon booting into singl
!	Static	GEN000240 - The system clock must be synchronized to an authoritative DoD
!	Static	GEN000241 - The system clock must be synchronized continuously, or at leas
!	Static	GEN000250 - The time synchronization configuration file must be owned by r
!	Static	GEN000251 - The time synchronization configuration file must be group-owned
!	Static	GEN000252 - The time synchronization configuration file must have mode 0640...
!	Static	GEN000290-1 - The system must not have the unnecessary "games" account
!	Static	GEN000290-2 - The system must not have the unnecessary "news" account
!	Static	GEN000290-3 - The system must not have the unnecessary "gopher" account
!	Static	GEN000290-4 - The system must not have the unnecessary "ftp" account

SUPRTEK
ADVANCED TECHNOLOGY GROUP

Awareness of What Your Adversaries are Up To …

```
1856a6a28621f241698e4e4287cba7c9
1d016bb286980fd356cab21cdfcb49f4
3d2c2fdd4104978762b89804ba771e63
5ff5916c9f7c593d1d589c97c571b45a
3b3f46caffa4d5eccf9e063c620a7c23
4900d40f92408468f0c65942ac66749e
4a35fe1895aca6dc7df91b00e730b4df
7c2113d2d67926cc7b8c470b33ede5c4
825a5172dbd9abab7f14e0de8af3cc12
```

```
101.226.167.19
101.226.167.20
124.248.205.19
162.210.197.77
180.153.227.230
195.211.101.87
89.35.178.109
184.29.104.251
52.27.166.51
```

```
accessdest.strangled[.]net
bookstore.strangled[.]net
bug.ignorelist[.]com
cars-online.zapto[.]org
chinafood.chickenkiller[.]com
coldriver.strangled[.]net
developarea.mooo[.]com
downtown.crabdance[.]com
easport-news.publicvm[.]com
```

```
alert tcp any any -> any any (msg: "SYNful Knock
HTTP Header";\
    flow: from_server;\
    content: "HTTP/1.1 200 OK|0d 0a|Server:
Apache/2.2.17 (Ubuntu)|0d 0a|X-Powered-By:
PHP/5.3.5-1ubuntu7.7|0d 0a|Keep-Alive:
timeout=15, max=100|0d 0a|Connection: Keep-
Alive|0d 0a|Content-Type: text/html|0d 0a 0d
0a|<html><body><div>";
    offset:0; flags:PA; sid:999999;)
```

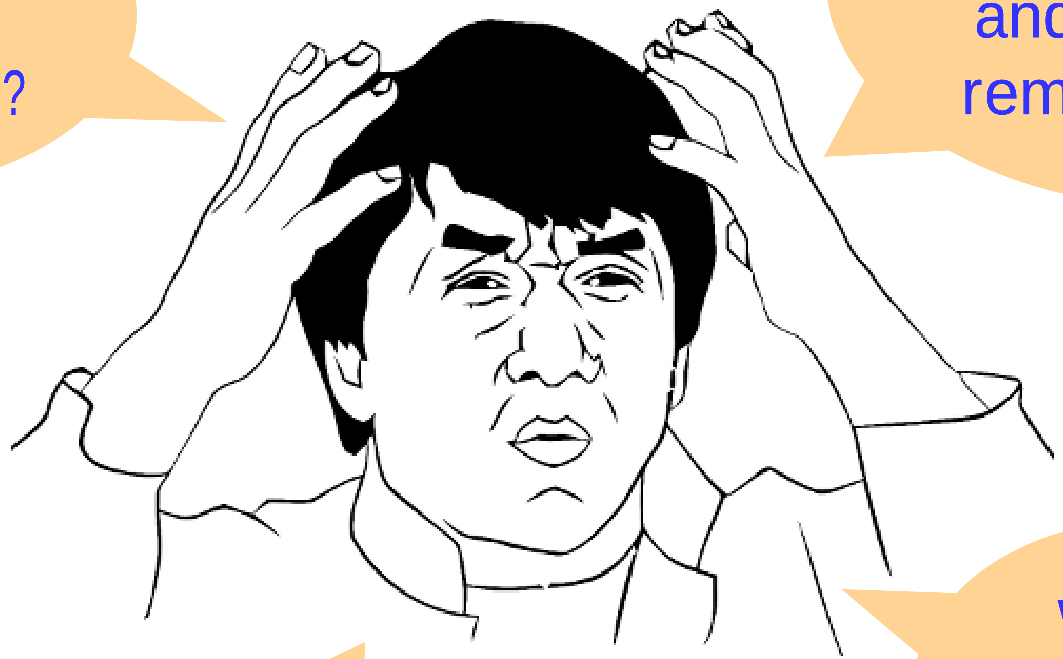
```
alert tcp any any -> any any
(msg: "SYNful Knock HTTP
Request"; flow:to_server;\
    content: "text"; offset:78;
depth:4;\
    content: "|00 00 00|";
offset:83; depth:3;\
    content: "|45 25 6d|";
offset:87; depth:3;\
    sid:9999998;)
```

SUPRTEK
ADVANCED TECHNOLOGY GROUP

Information Overload

What threats to investigate?

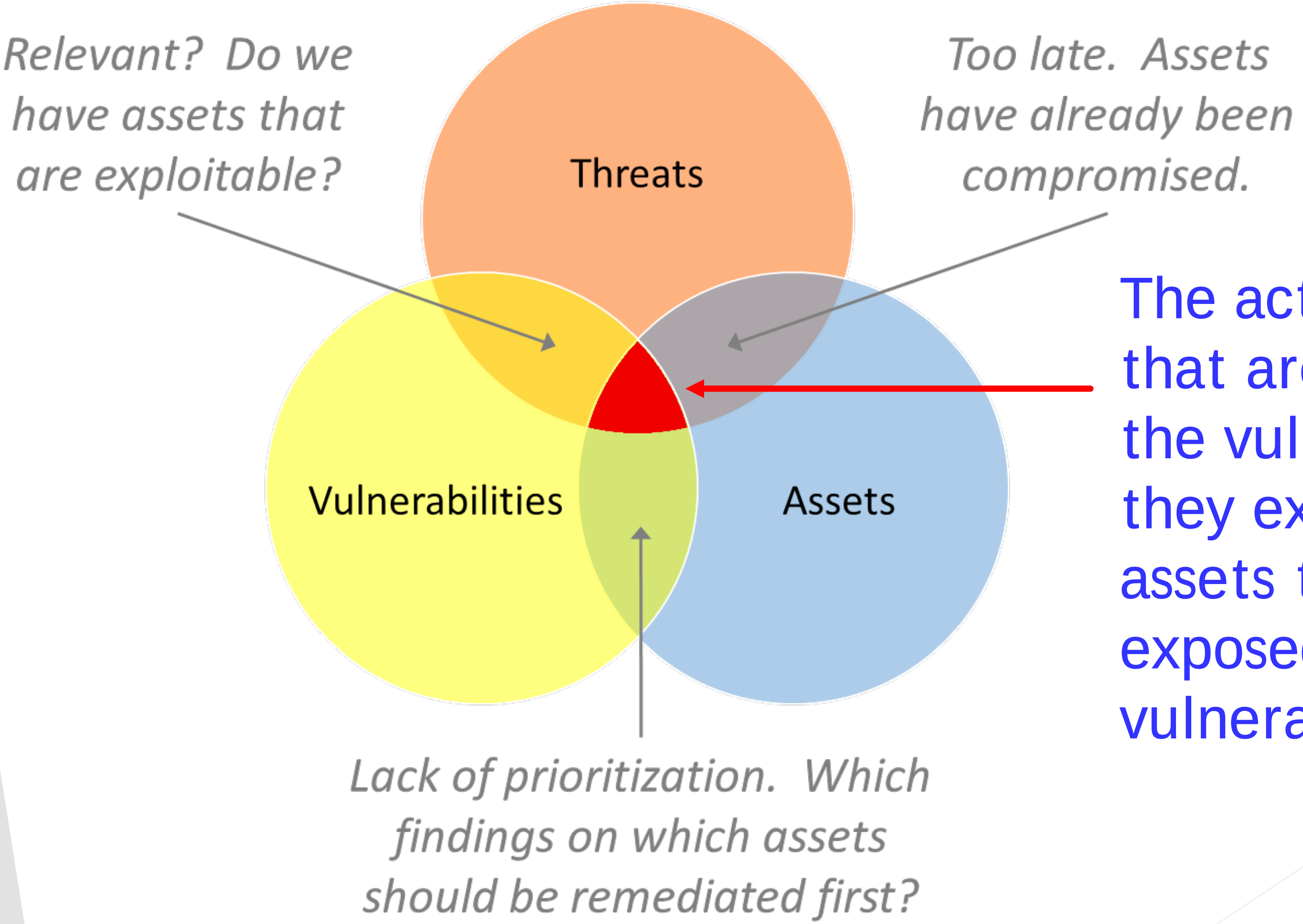
Which vulnerabilities and findings to remediate first?



Which devices to patch?

Which indicators are relevant and reliable?

The Sweet Spot



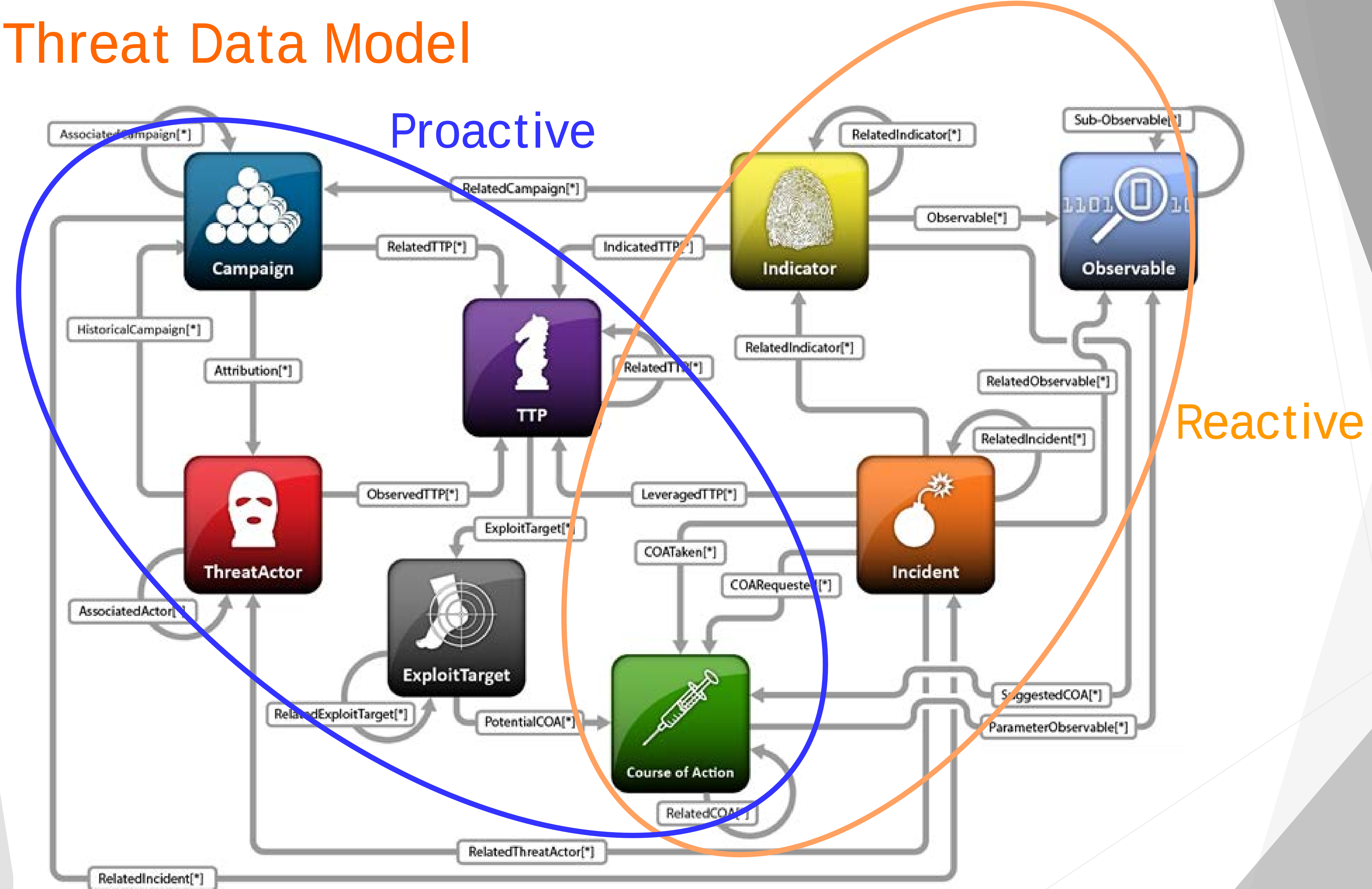
Relevant? Do we have assets that are exploitable?

Too late. Assets have already been compromised.

Lack of prioritization. Which findings on which assets should be remediated first?

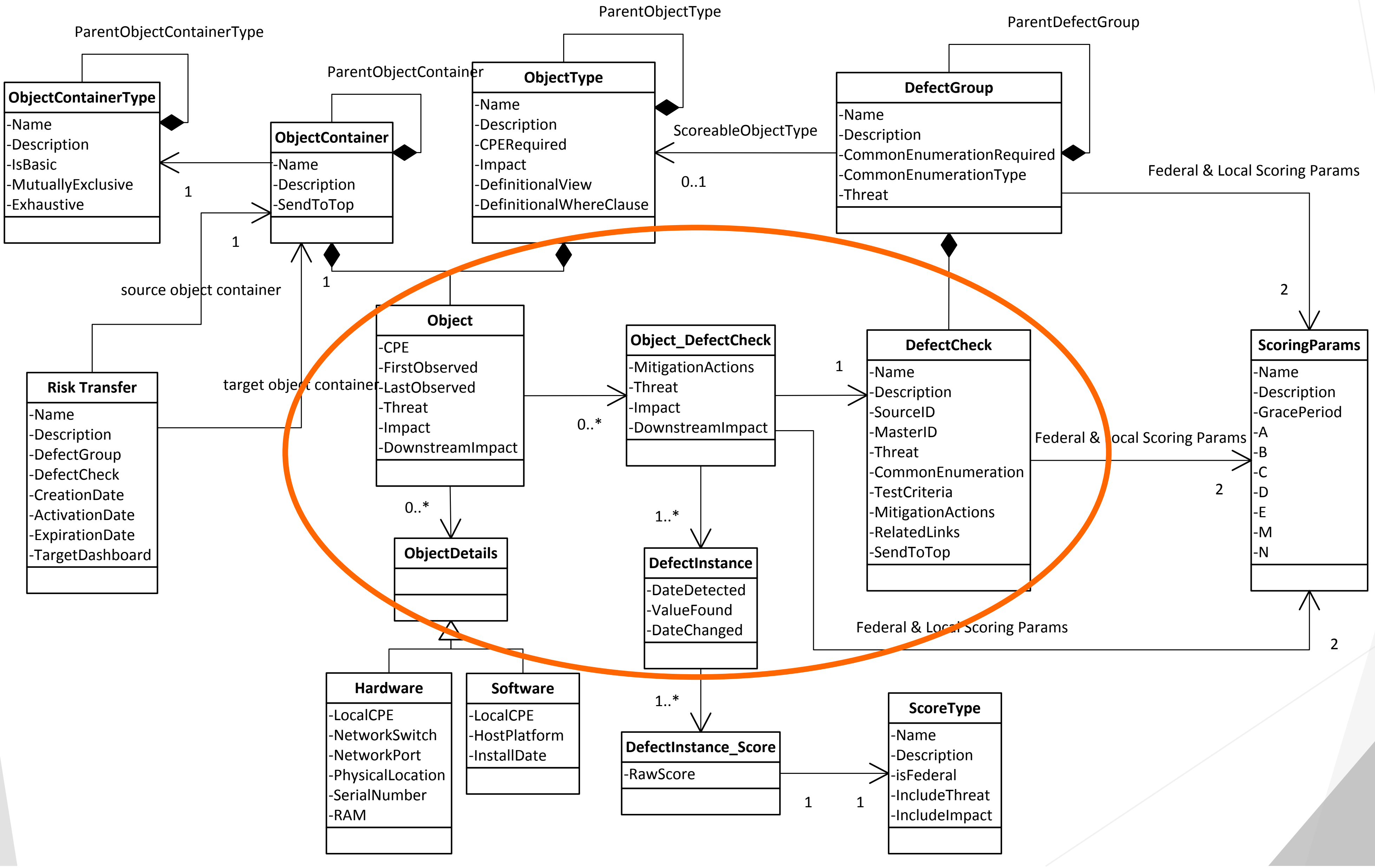
The active threats that are out there, the vulnerabilities they exploit, and the assets that are exposed to those vulnerabilities

Threat Data Model



SUPRTEK ADVANCED TECHNOLOGY GROUP

CDM Data Model



ObjectContainerType
-Name
-Description
-IsBasic
-MutuallyExclusive
-Exhaustive

ObjectContainer
-Name
-Description
-SendToTop

ObjectType
-Name
-Description
-CPERequired
-Impact
-DefinitionalView
-DefinitionalWhereClause

DefectGroup
-Name
-Description
-CommonEnumerationRequired
-CommonEnumerationType
-Threat

Risk Transfer
-Name
-Description
-DefectGroup
-DefectCheck
-CreationDate
-ActivationDate
-ExpirationDate
-TargetDashboard

Object
-CPE
-FirstObserved
-LastObserved
-Threat
-Impact
-DownstreamImpact

Object_DefectCheck
-MitigationActions
-Threat
-Impact
-DownstreamImpact

DefectCheck
-Name
-Description
-SourceID
-MasterID
-Threat
-CommonEnumeration
-TestCriteria
-MitigationActions
-RelatedLinks
-SendToTop

ScoringParams
-Name
-Description
-GracePeriod
-A
-B
-C
-D
-E
-M
-N

ObjectDetails

DefectInstance
-DateDetected
-ValueFound
-DateChanged

Hardware
-LocalCPE
-NetworkSwitch
-NetworkPort
-PhysicalLocation
-SerialNumber
-RAM

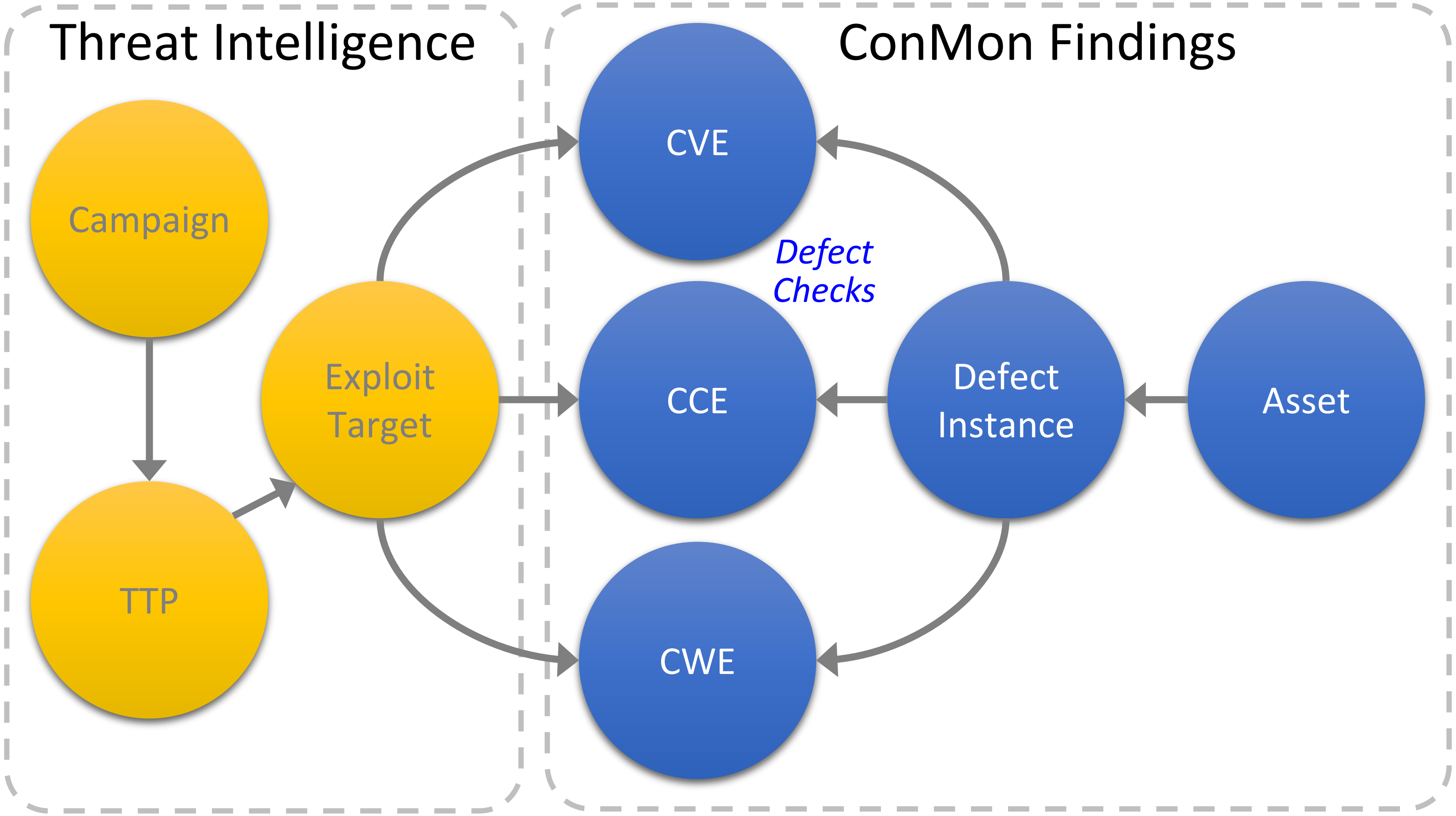
Software
-LocalCPE
-HostPlatform
-InstallDate

DefectInstance_Score
-RawScore

ScoreType
-Name
-Description
-isFederal
-IncludeThreat
-IncludeImpact

SUPRTEK
ADVANCED TECHNOLOGY GROUP

Correlating the Two Datasets



How Do We Do This?

Collection and Correlation

- Collect and correlate threat intelligence from multiple sources with information on your internal IT landscape collected from continuous monitoring

Proactive Threat Intel

- Focus on the proactive elements of threat intel such as the threat campaigns that are relevant to your organization, the threat actors perpetrating these campaigns, the TTPs that they use and the weaknesses and vulnerabilities that they exploit

Actionable Information

- Extract actionable information such as tactics, techniques, and procedures (TTPs) and exploit targets that are used by threat actors

Targeted Assets

- Identify targeted assets and develop specific preventive courses of action to thwart these TTPs

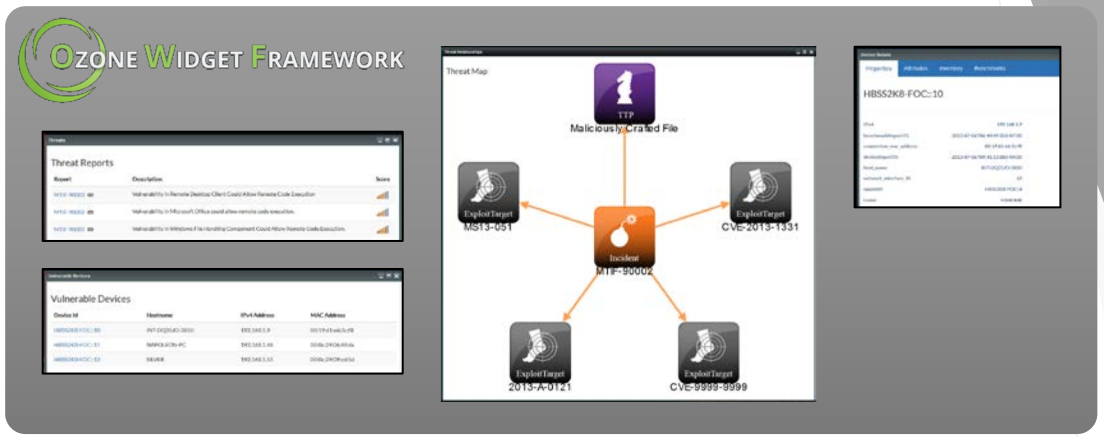
Prioritization

- Score and prioritize threat intelligence that are most relevant and critical to your organization

SUPRTEK
ADVANCED TECHNOLOGY GROUP

System Architecture

- High performance & scalability
- Based on open standards such as SCAP, ARF, ASR, STIX
- Open source big data and analytics components

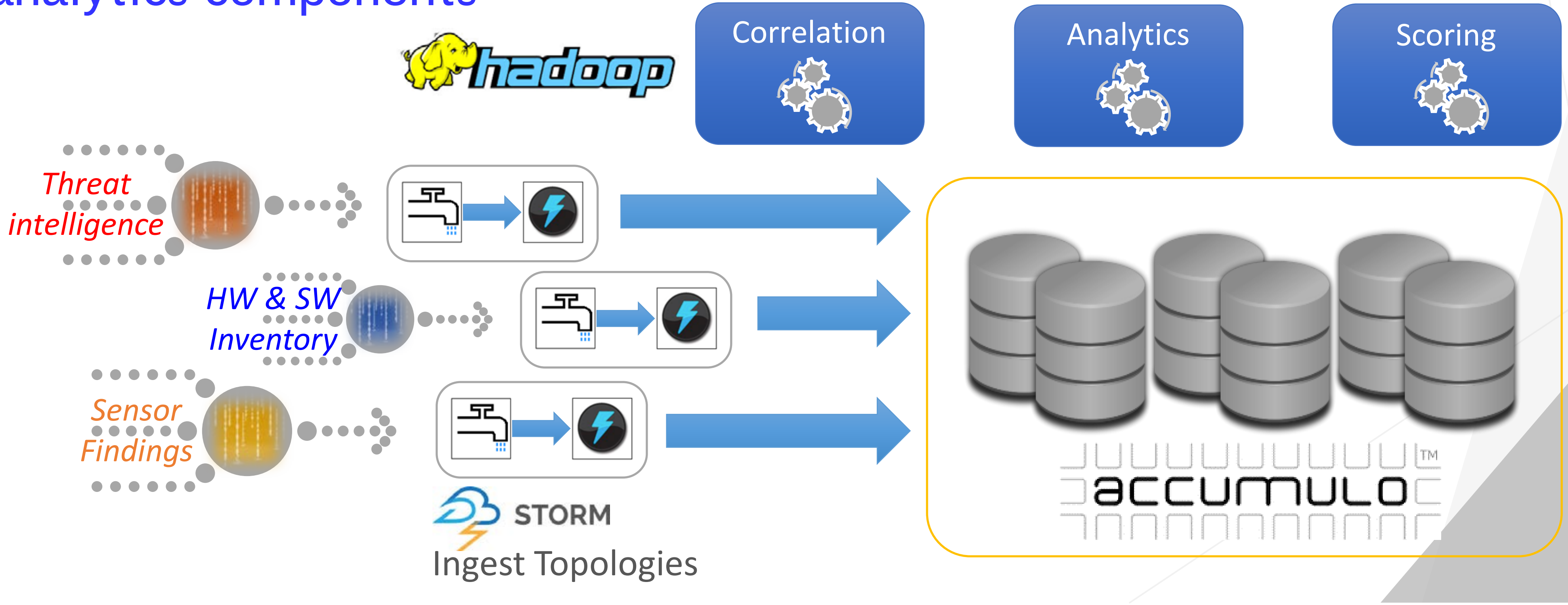


Threat Reports

Report	Description	Score
MTIF-90003	Vulnerability in Remote Desktop Client Could Allow Remote Code Execution	
MTIF-90002	Vulnerability in Microsoft Office could allow remote code execution.	
MTIF-90001	Vulnerability in Windows File Handling Component Could Allow Remote Code Execution.	

Vulnerable Devices

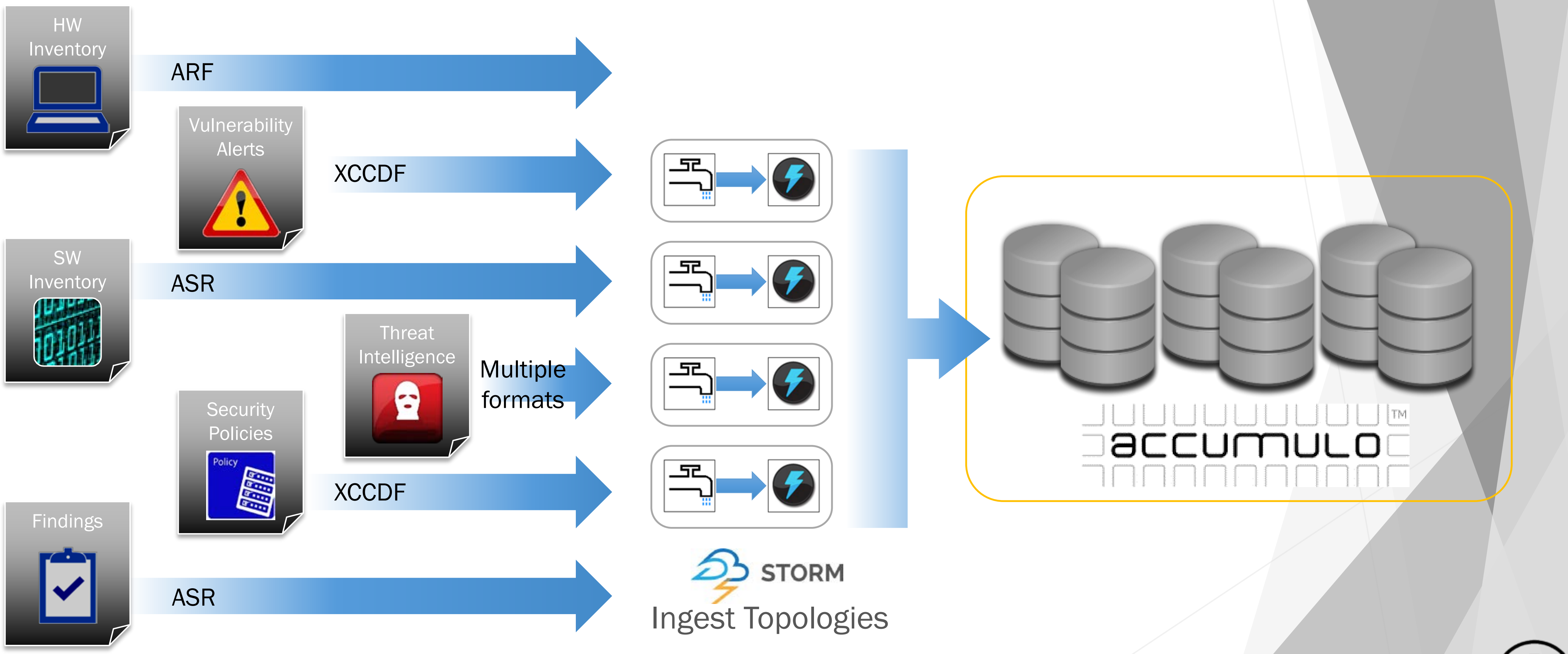
Device Id	Hostname	IPv4 Address	MAC Address
HBSS2K8-FOC::10	INT-DQ2UO-3850	192.168.1.9	[illegible]
HBSS2K8-FOC::11	NAPOLEON-PC	192.168.1.48	[illegible]
HBSS2K8-FOC::12	SILVER	192.168.1.33	[illegible]



Ingest Topologies

SUPRTEK ADVANCED TECHNOLOGY GROUP

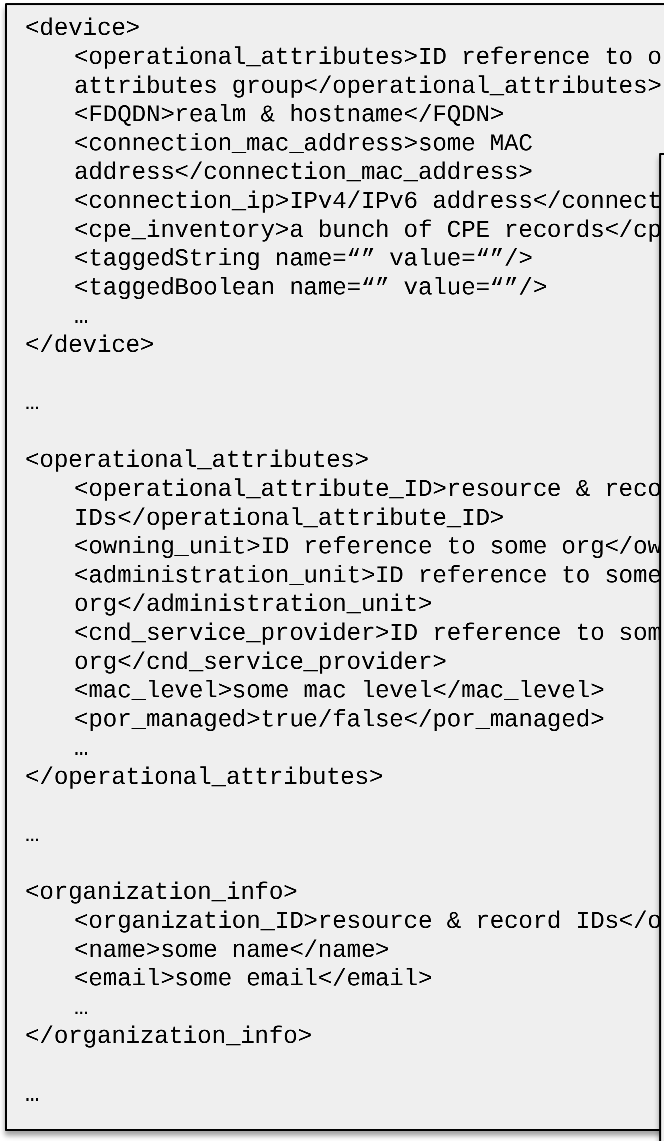
High Speed Data Ingest



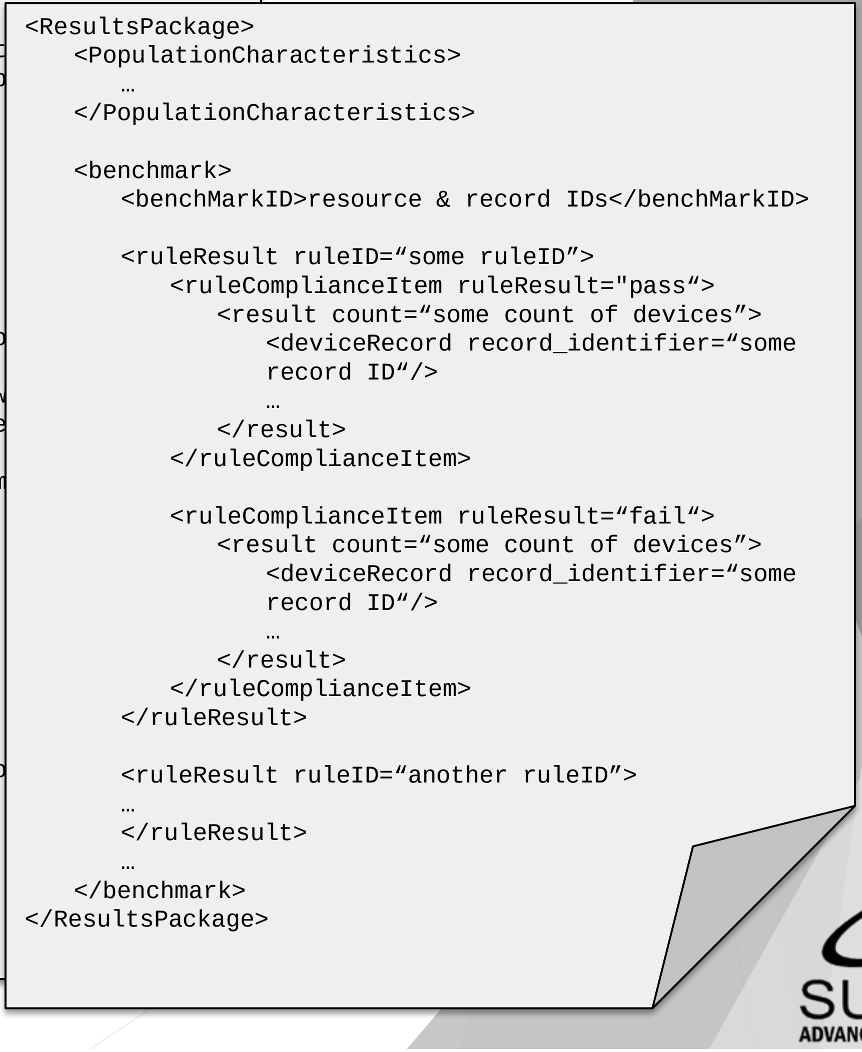
SUPRTEK ADVANCED TECHNOLOGY GROUP

SCAP Formats for Asset and Findings Data

- **ARF** – Asset Reporting Format
- **ASR** – Assessment Summary Results
- **XCCDF** – Policies, IAVMs, STIGs, Benchmarks
- **CPE** - Inventory

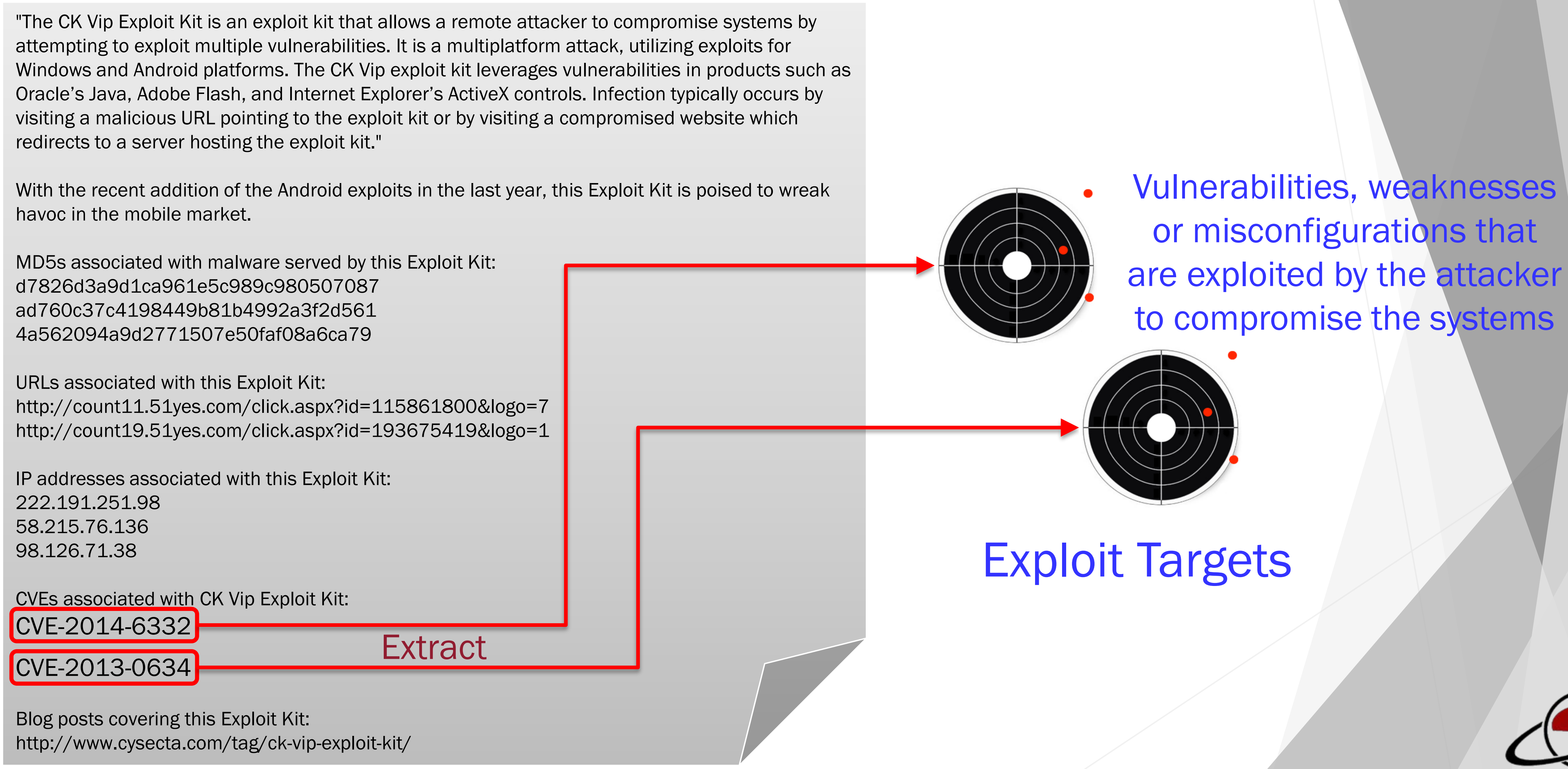


```
<device>
    <operational_attributes>ID reference to operational
    attributes group</operational_attributes>
    <FDQDN>realm & hostname</FQDN>
    <connection_mac_address>some MAC
    address</connection_mac_address>
    <connection_ip>IPv4/IPv6 address</connect
    <cpe_inventory>a bunch of CPE records</cp
    <taggedString name=“” value=“”/>
    <taggedBoolean name=“” value=“”/>
    …
</device>

…

<operational_attributes>
    <operational_attribute_ID>resource & reco
    IDs</operational_attribute_ID>
    <owning_unit>ID reference to some org</ow
    <administration_unit>ID reference to some
    org</administration_unit>
    <cnd_service_provider>ID reference to som
    org</cnd_service_provider>
    <mac_level>some mac level</mac_level>
    <por_managed>true/false</por_managed>
    …
</operational_attributes>

…

<organization_info>
    <organization_ID>resource & record IDs</o
    <name>some name</name>
    <email>some email</email>
    …
</organization_info>

…
```



```
<ResultsPackage>
    <PopulationCharacteristics>
        …
    </PopulationCharacteristics>

    <benchmark>
        <benchMarkID>resource & record IDs</benchMarkID>

        <ruleResult ruleID=“some ruleID”>
            <ruleComplianceItem ruleResult="pass“>
                <result count=“some count of devices”>
                    <deviceRecord record_identifier=“some
                    record ID“/>
                    …
                </result>
            </ruleComplianceItem>

            <ruleComplianceItem ruleResult=“fail“>
                <result count=“some count of devices”>
                    <deviceRecord record_identifier=“some
                    record ID“/>
                    …
                </result>
            </ruleComplianceItem>
        </ruleResult>

        <ruleResult ruleID=“another ruleID”>
        …
        </ruleResult>
        …
    </benchmark>
</ResultsPackage>
```

Extraction of Exploit Targets from Threat Intelligence



"The CK Vip Exploit Kit is an exploit kit that allows a remote attacker to compromise systems by attempting to exploit multiple vulnerabilities. It is a multiplatform attack, utilizing exploits for Windows and Android platforms. The CK Vip exploit kit leverages vulnerabilities in products such as Oracle's Java, Adobe Flash, and Internet Explorer's ActiveX controls. Infection typically occurs by visiting a malicious URL pointing to the exploit kit or by visiting a compromised website which redirects to a server hosting the exploit kit."

With the recent addition of the Android exploits in the last year, this Exploit Kit is poised to wreak havoc in the mobile market.

MD5s associated with malware served by this Exploit Kit:
d7826d3a9d1ca961e5c989c980507087
ad760c37c4198449b81b4992a3f2d561
4a562094a9d2771507e50faf08a6ca79

URLs associated with this Exploit Kit:
http://count11.51yes.com/click.aspx?id=115861800&logo=7
http://count19.51yes.com/click.aspx?id=193675419&logo=1

IP addresses associated with this Exploit Kit:
222.191.251.98
58.215.76.136
98.126.71.38

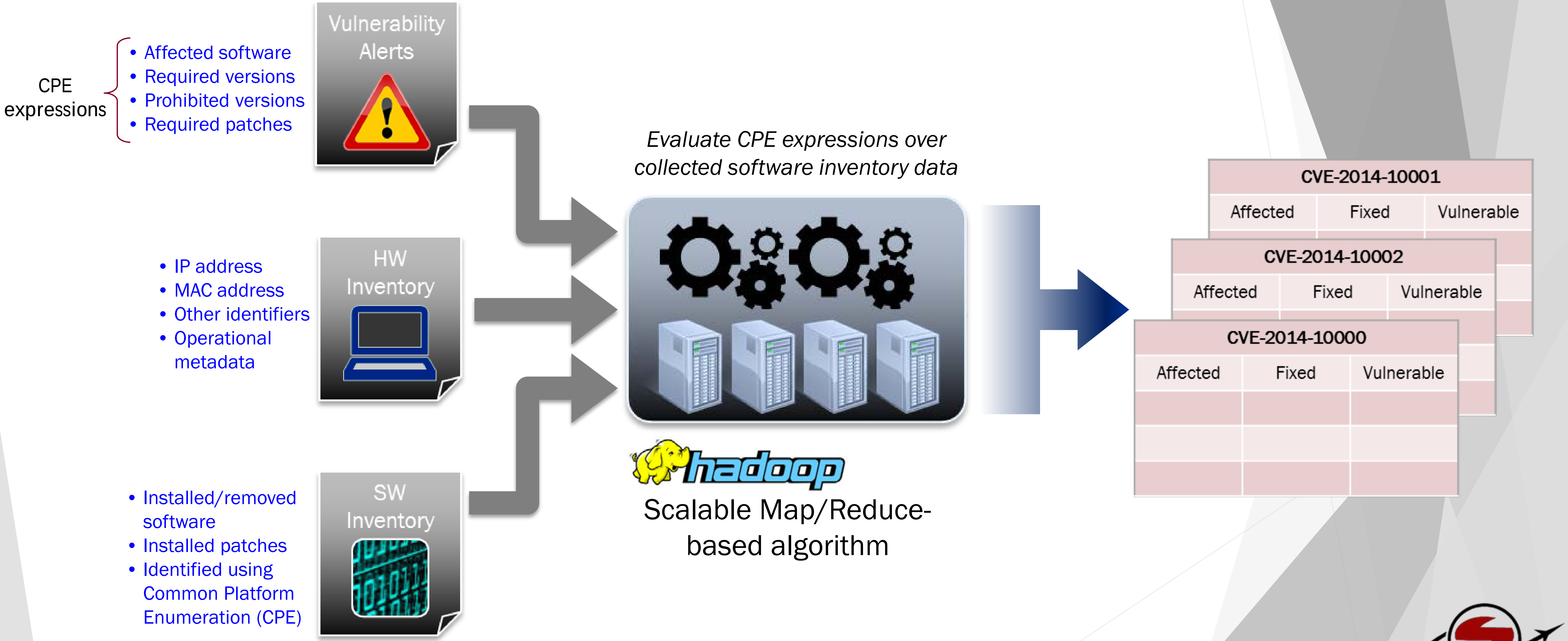
CVEs associated with CK Vip Exploit Kit:
CVE-2014-6332
CVE-2013-0634

Blog posts covering this Exploit Kit:
http://www.cysecta.com/tag/ck-vip-exploit-kit/

Vulnerabilities, weaknesses or misconfigurations that are exploited by the attacker to compromise the systems

Exploit Targets

Computation of Vulnerability Exposure and Patch Compliance



CPE expressions

- Affected software
- Required versions
- Prohibited versions
- Required patches

Vulnerability Alerts

- IP address
- MAC address
- Other identifiers
- Operational metadata

HW Inventory

- Installed/removed software
- Installed patches
- Identified using Common Platform Enumeration (CPE)

SW Inventory

Evaluate CPE expressions over collected software inventory data

hadoop

Scalable Map/Reduce-based algorithm

CVE-2014-10001

Affected	Fixed	Vulnerable

CVE-2014-10002

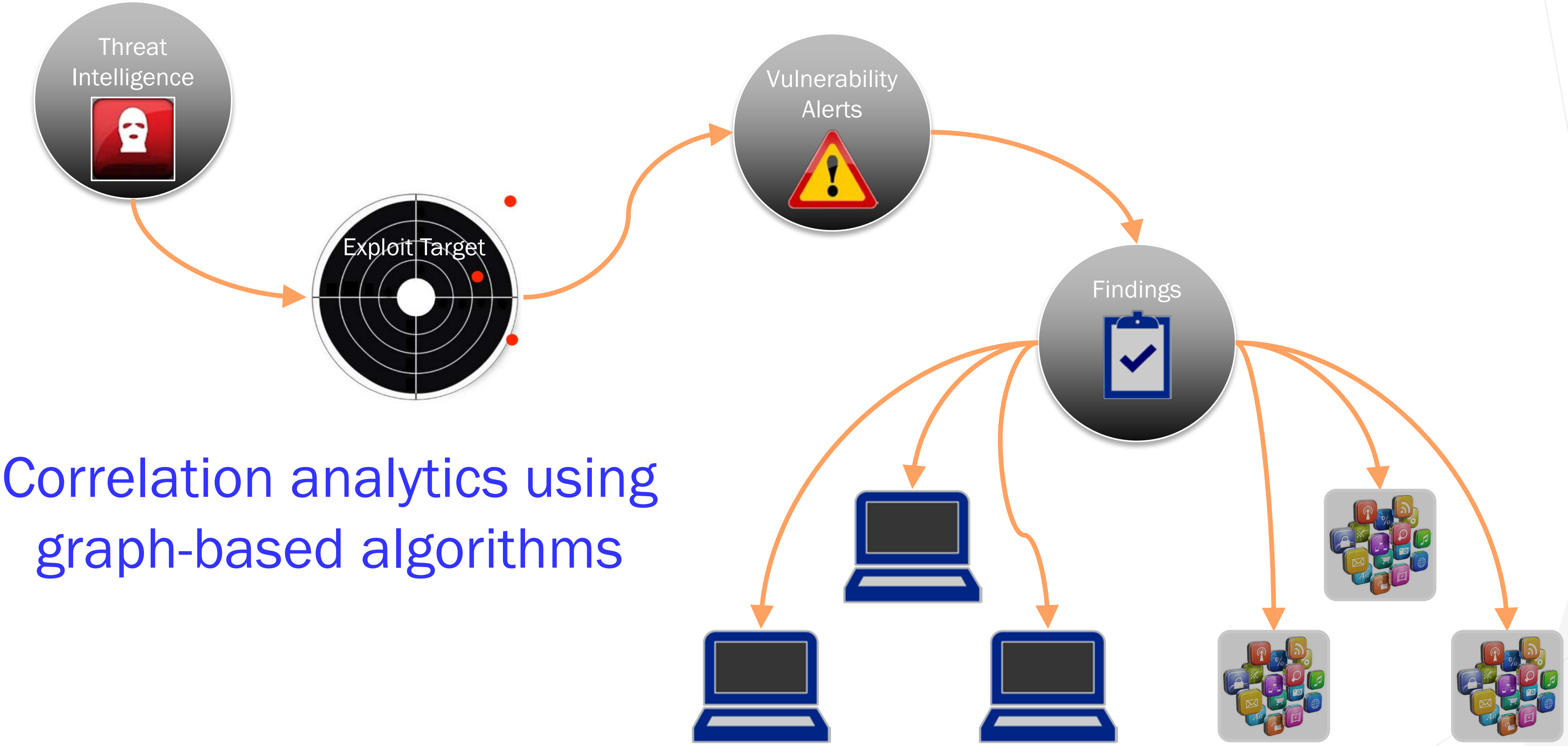
Affected	Fixed	Vulnerable

CVE-2014-10000

Affected	Fixed	Vulnerable

SUPRTEK ADVANCED TECHNOLOGY GROUP

Correlation of Exploit Targets with Findings and Identification of Exploitable Assets



Correlation analytics using graph-based algorithms

Exploitable assets (hardware & software)

SUPRTEK
ADVANCED TECHNOLOGY GROUP

Prioritization Through Scoring

Score findings based on known threats that utilize the weakness, vulnerability or misconfiguration in each finding as exploit targets.

$$Score(D) = \sum_{i=1}^{n} T_i[(a \times Ki) + (b \times Ui)]$$

D = Defect check being scored
n = Number of threats that have defect check D as an Exploit Target
T_i = Weight of Threat$_i$
K_i = Number of assets that are *known* to be exploitable by Threat$_i$
U_i = Number of assets that are *potentially* exploitable by Threat$_i$
a = Weight applied to K, constant value greater than **b**
b = Weight applied to U, constant value less than **a**

An asset is *known* to be exploitable by a threat if it fails all of the defect checks required for exploit by that threat. E.g. if a threat requires failures in three defect checks for exploit and the asset fails all three defect checks, then that asset is known to be exploitable; or, if a threat requires a failure in any one of the defect checks for exploit and the asset fails one of those defect checks, then it is also known to be exploitable.

An asset is *potentially* exploitable by a threat if it fails some of the defect checks required for exploit by that threat.

SUPRTEK
ADVANCED TECHNOLOGY GROUP

What’s Next?

- Need better threat intel – focus more on *proactive elements*, e.g. TTPs, exploit targets, rather than *reactive elements*, e.g. IoCs, malicious IPs, domains, etc.
- Machine learning to infer relevant security controls, mis-configurations, weaknesses, vulnerabilities, etc. from TTPs and exploit targets extracted from threat intel
- Validation on a larger enterprise network

SUPRTEK
ADVANCED TECHNOLOGY GROUP

Contact

- Tieu Luu
- Sr. Director Advanced Technology Group
- tluu@suprtek.com
- @TechTieu

- Jay Ruhnke
- Sr. Architect Advanced Technology Group
- jruhnke@suprtek.com
- @JRuhnke

SUPRTEK
ADVANCED TECHNOLOGY GROUP