

GE

Incident Response



Insight



Awareness



Advantage



imagination at work

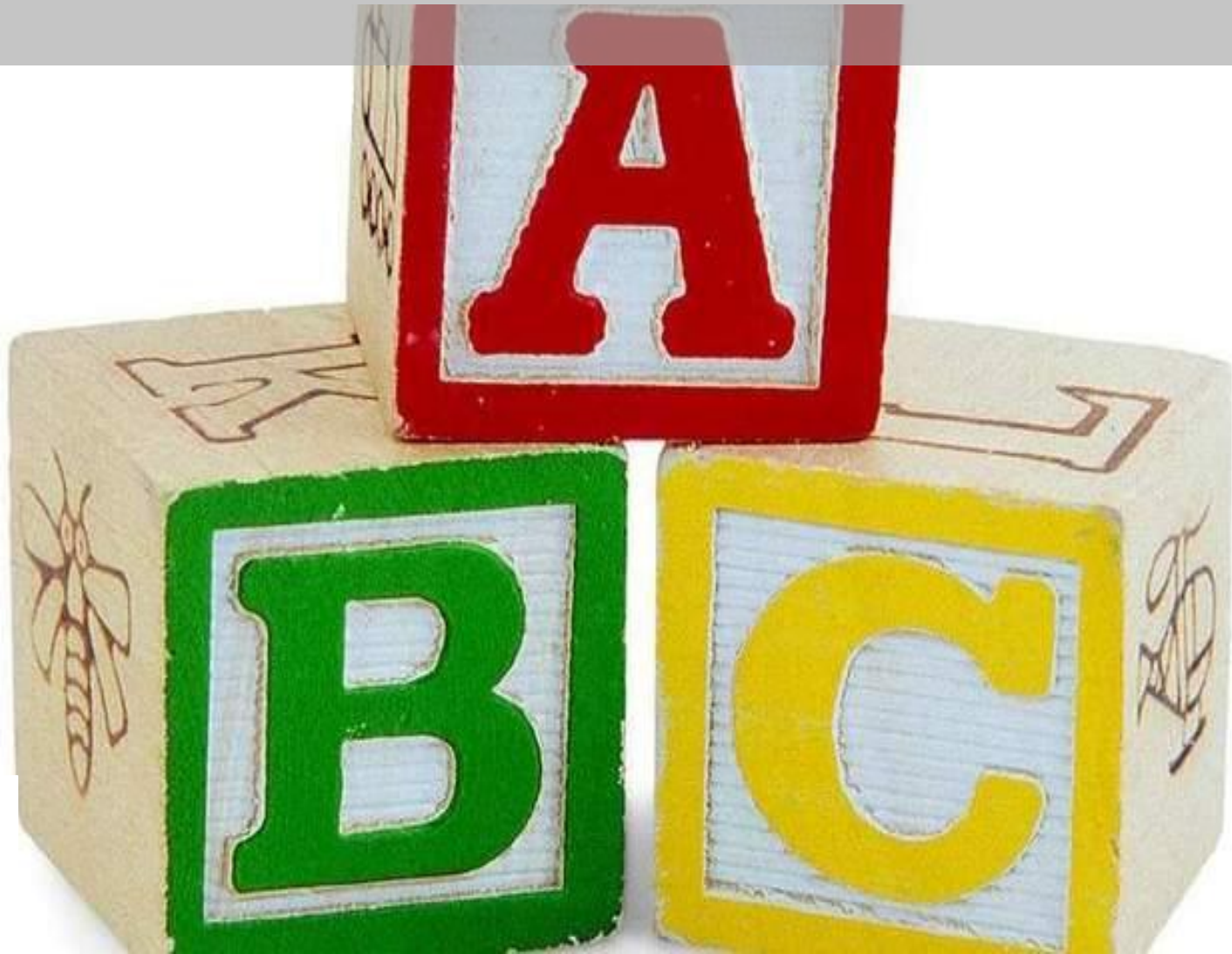
Sean Mason
Director, Incident Response

Investing in new talent & capabilities

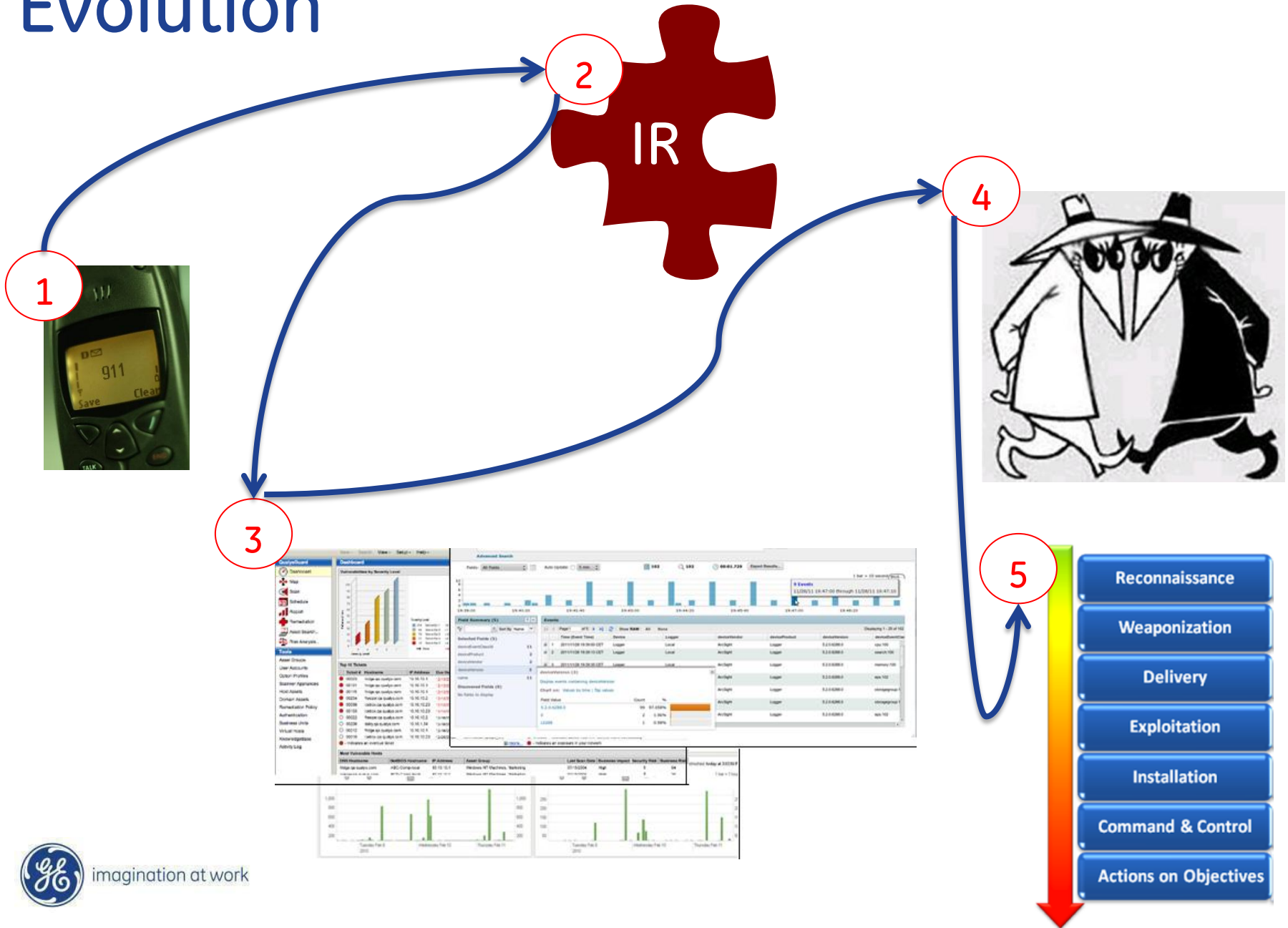
- ↑ Incident response
- ↑ Cyber intelligence
- ↑ Digital forensics
- ↑ Security architecture
- ↑ Identity management
- ↑ Compliance, controllership, IT management

Cyber Security
Fusion Center

Fundamentals



Evolution



Threats

| <u>Threat type</u> | <u>What</u> | <u>Examples</u> |
|-----------------------------------|--|---|
| Hacktivism |  <p>Highly visible attacks targeting large corporations and government agencies</p> | <ul style="list-style-type: none">• Anonymous |
| Advanced Persistent Threat |  <p>Organized and state funded groups methodically infiltrating the enterprise</p> | <ul style="list-style-type: none">• APT1 |
| Cybercrime |  <p>Organized crime rings targeting individuals and corporations for financial gain</p> | <ul style="list-style-type: none">• RBN |

Kill Chain (KC)

KC1- Reconnaissance: Collecting information and learning about the internal structure of the host organization

KC2- Weaponization: How the attacker packages the threat for delivery

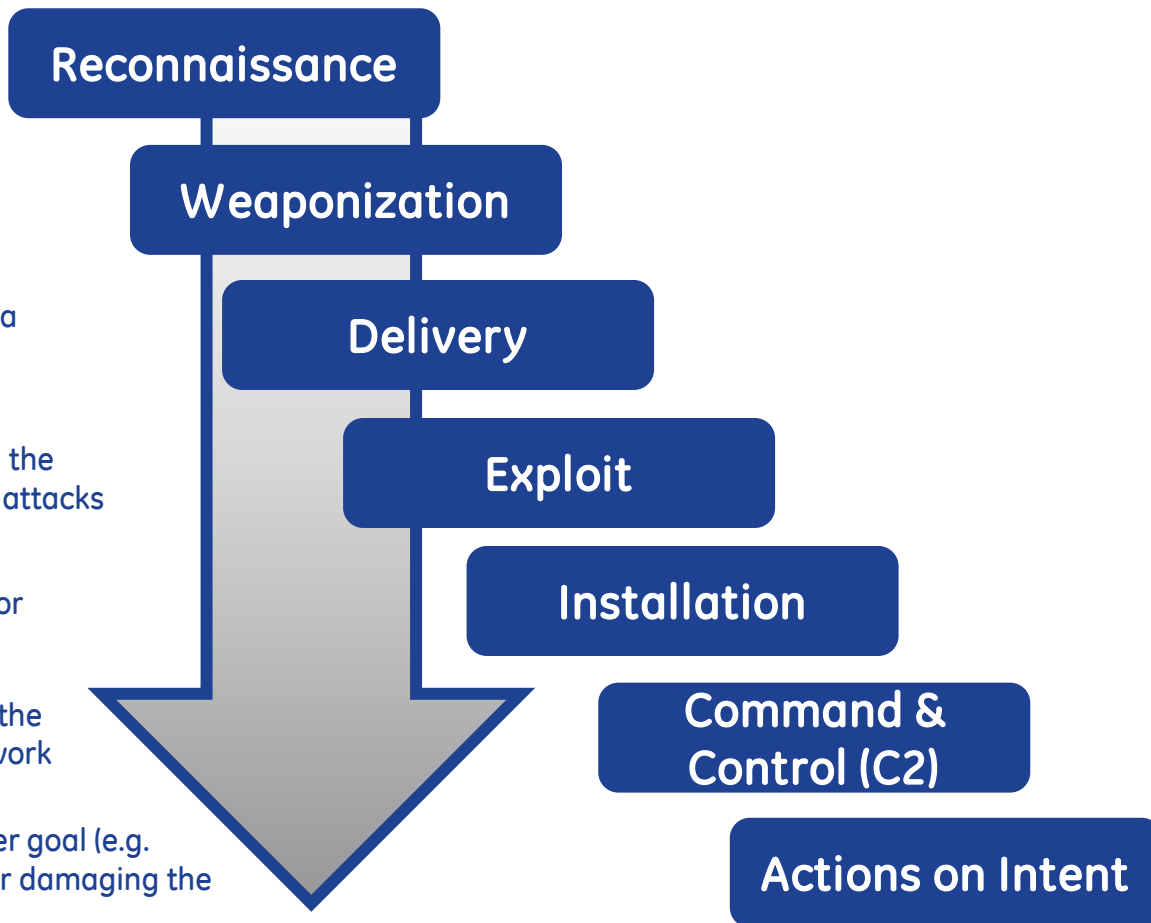
KC3- Delivery: The actual delivery of the threat (via email, web, USB, etc.)

KC4- Exploitation: Once the host is compromised, the attacker can take advantage and conduct further attacks

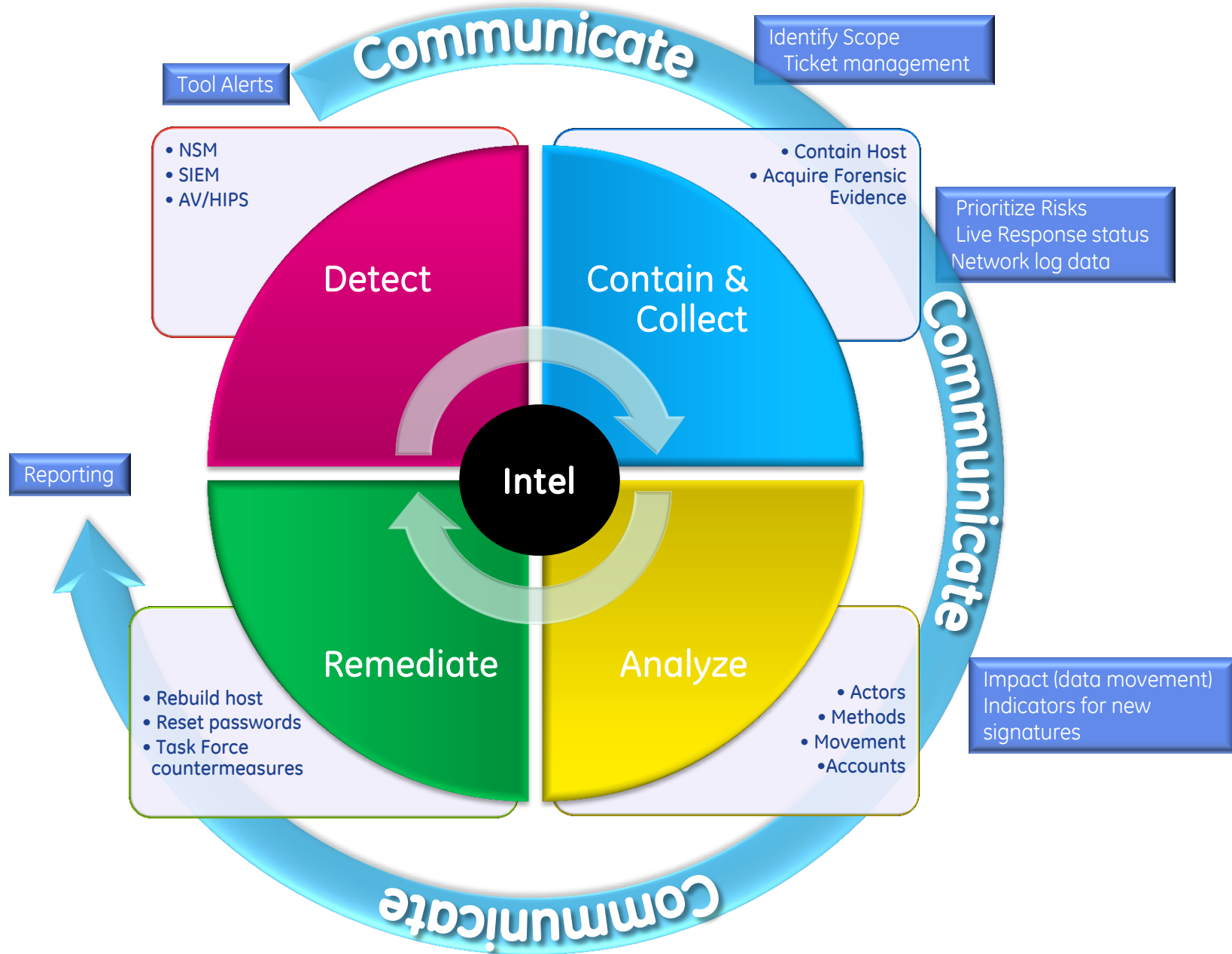
KC5- Installation: Installing the actual malware, for example

KC6- Command & Control: Setting up controls so the attacker can have future access to the host's network

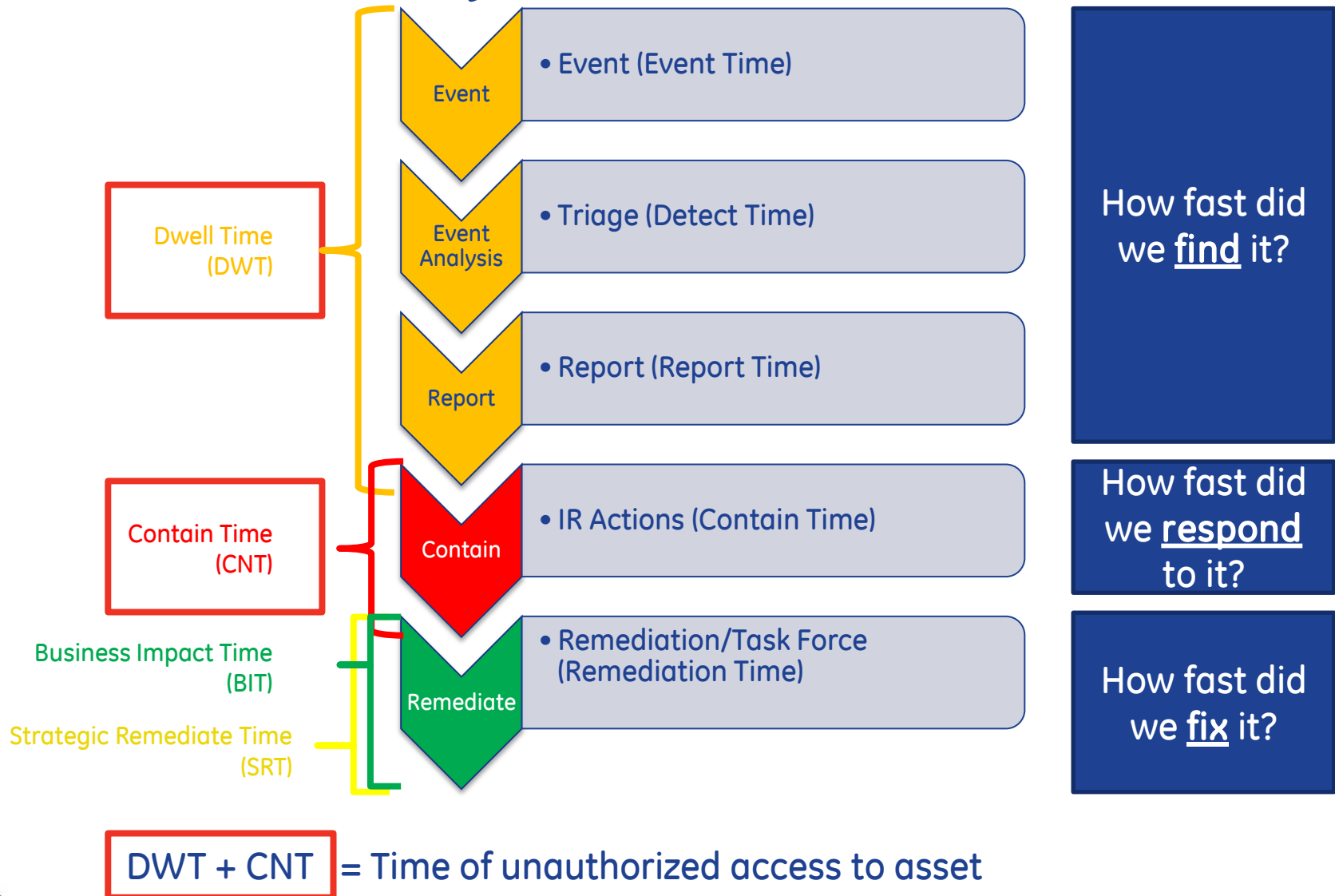
KC7- Actions on Intent: The attacker meets his/her goal (e.g. stealing information, gaining elevated privileges or damaging the host completely)



Incident Response process (DCAR+I)



IR measured cycle times



Workflow & knowledge management

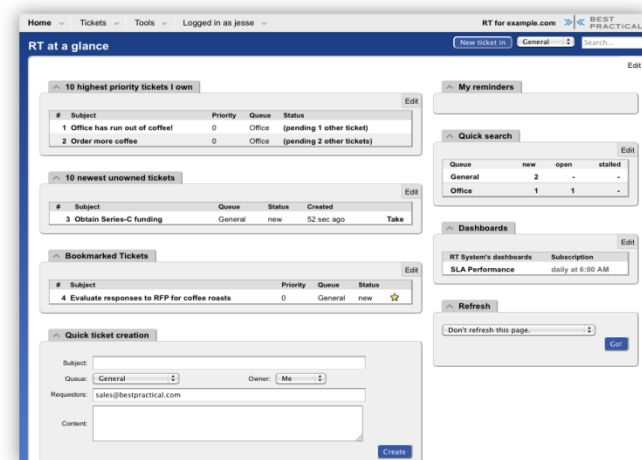


The screenshot shows the MediaWiki.org homepage. It features a 'Welcome to MediaWiki.org' message, a search bar, and a sidebar with links to various sections like 'Main Page', 'Browse categories', and 'Recent changes'. The main content area includes 'Current versions' and 'News' sections, with a 'Download' button for the latest version (1.15.1).

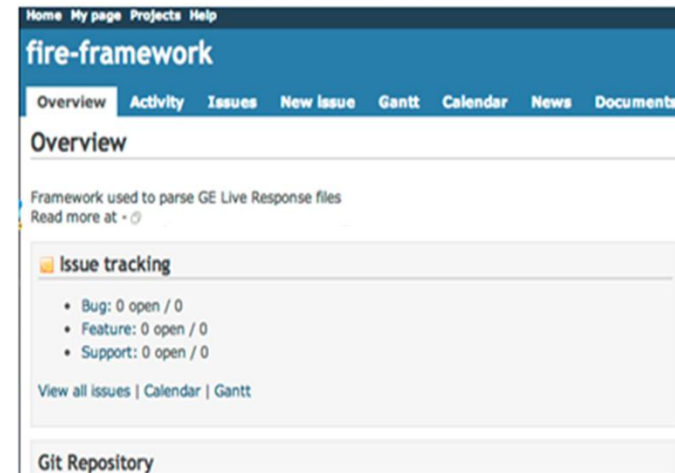


The screenshot shows the GE-CIRT Dashboard. It features a header with the GE logo and the title 'Incident Management System'. Below the header, there are tabs for 'Requests' and 'Incidents'. The main content area displays 'queue and user statistics *updated daily' and a table with incident counts and values.

| Queue Name | Incident Count | Name | Value |
|----------------|----------------|---------------------|---------------|
| Security Queue | -- | Avg. Time To Detect | 0 Minutes 0 s |
| Abuse Queue | -- | Avg. Time To Report | 0 Minutes 0 s |
| Spam Queue | -- | Total Reported | 0 Incidents |



The screenshot shows the RT (Request Tracker) interface. It features a header with 'Home', 'Tickets', 'Tools', and 'Logged in as jesse'. The main content area displays 'RT at a glance' with sections for '10 highest priority tickets I own', '10 newest unowned tickets', 'Bookmarked Tickets', and 'Quick ticket creation'. The 'Quick ticket creation' section includes fields for 'Subject', 'Queue', 'Owner', and 'Content'.



The screenshot shows the fire-framework interface. It features a header with 'Home', 'My page', 'Projects', and 'Help'. The main content area displays 'fire-framework' and 'Overview' with a table showing issue tracking statistics.

| Issue tracking |
|---------------------|
| Bug: 0 open / 0 |
| Feature: 0 open / 0 |
| Support: 0 open / 0 |

View all issues | Calendar | Gantt

Git Repository

Communication

- Tailored audience based on KC
- Standard communications rhythm
 - (~1hr after declaration; COB daily)
- More detailed PowerPoint
 - End of week
- Inclusive & transparent!

**RESTRICTED INFORMATION – LIMITED DISTRIBUTION;
ENCRYPTED TRANSMISSION ONLY**

Note: Updated information is shaded in **Green** and completed actions are struck through.

Kill Chain Phase:

Businesses & Locations Impacted:

Summary:

Impact:

Incident Status: **MM-DD-YYYY HHMM**

Host Status:

Intelligence Summary:

· Attribution

Action Items:

Next Update:

Intel



Intel



Government

Trade
Associations

Industry &
Open Source

Strong relationship with key stakeholders across all sectors

Intel storage & analysis



CRITs is a MITRE application provided to industry peers (120+ members) for:

- Indicator management
- Malware triage
- Advanced Intel analysis
- Managing the “Sharing Problem”
- Implementing threat sharing standards

Summary

Type

URI - Domain Name

Value

evil.com

Creation Date

2013-02-25 13:10:58.324000

Last Modified

2013-02-25 13:10:58.324000

Status

New

Confidence

benign

Impact

medium

Sources

3rd Party (1): 2013-02-25

Actions

Type

Begin

End

Performed

Active

Reason

Date Added

Analyst

Blacklist - DomainTracker

in progress

2013-02-25 13:11:21.943000

Tickets

Campaigns

Campaign

Confidence

Description

Analyst

Date

azCyberCrime

medium

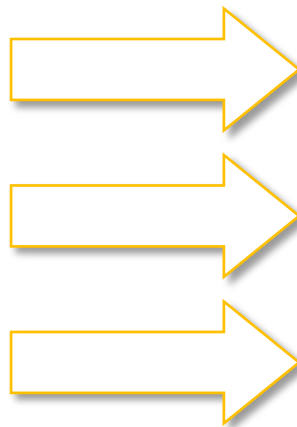
bbinkman

2013-02-25 13:11:33.868801

OSINT

Sharing
partners

Antivirus
vendors



Structured indicator storage

Summary

| | |
|---------------|--|
| Type | URI - Domain Name |
| Value | badguys.com |
| Creation Date | 2013-04-15 23:49:57.575000 |
| Last Modified | 2013-04-15 23:49:57.575000 |
| Status | New |
| Confidence | <div><div></div><div>high</div></div> |
| Impact | <div><div></div><div>medium</div></div> |
| Sources | <div><div>GE Corporate (1): 2013-04-15</div><div>Method: Reference: http://wikientry.com</div></div> |

Analyst:
Created: 2013-04-15 23:49:57.575000

Actions

| Type | Begin | End | Performed | Ac |
|------|----------------------------|----------------------------|-----------|----|
| | 2013-04-08 00:00:00.000000 | | | |
| | 2013-04-01 00:00:00.000000 | 2013-04-08 00:00:00.000000 | | |

Tickets

| Ticket Number | URL | Date | Analyst |
|---------------|-----|----------------------------|---------|
| 123456 | | 2013-04-15 23:52:15.607000 | |

Campaigns

| Campaign | Confidence | Description | Analyst | Date |
|----------|------------|--|---------|----------------------------|
| | high | This was witnessed in an internal GE event with confirmed attribution by the Cyber Intelligence team | | 2013-04-15 23:52:50.282529 |

Activity

Relationships (1)

| Type | Details |
|---------------|---|
| Indicators: 1 | <div><div>Value</div><div>Address - ipv4-addr</div></div> |

Objects (2)

| Type | Name | Value | Date | Analyst | Source |
|----------------|------------|--------------|------------|---------|---|
| Kill Chains: 1 | Kill Chain | C2 | 2013-04-15 | | <div><div>Name: Method: Reference: </div><div>GE Corporate Static Analysis None</div></div> |
| Roles: 1 | Role | Owned_Domain | 2013-04-15 | | <div><div>Name: Method: Reference: </div><div>GE Corporate Static Analysis None</div></div> |

Summary details provide the default required values about an indicator

Structured indicator storage

Summary

Type: URI - Domain Name
Value: badguys.com
Creation Date: 2013-04-15 23:49:57.575000
Last Modified: 2013-04-15 23:49:57.575000
Status: New
Confidence: high
Impact: medium
Sources: GE Corporate (1): 2013-04-15
Method:
Reference: <http://wikientry.com>

Actions can be used to show tracking of an indicator to a detection deployment. Tickets can be used to relate indicators back to our tickets.

Actions

| Type | Begin | End | Performed | Active | Reason | Date Added | Analyst |
|------|----------------------------|----------------------------|-----------|-------------|---------------------------------------|----------------------------|---------|
| | 2013-04-08 00:00:00.000000 | | on | | Auto deployment | 2013-04-15 23:51:07.755000 | |
| | | | | in progress | QA process queue | 2013-04-15 23:51:37.843000 | |
| | 2013-04-01 00:00:00.000000 | 2013-04-08 00:00:00.000000 | off | | Indicator was a FP, action turned off | 2013-04-15 23:52:03.932000 | |

Tickets

| Ticket Number | URL | Date | Analyst |
|---------------|-----|----------------------------|---------|
| 123456 | | 2013-04-15 23:52:15.607000 | |

Campaigns

| Campaign | Confidence | Description | Analyst | Date |
|----------|------------|--|---------|----------------------------|
| | high | This was witnessed in an internal GE event with confirmed attribution by the Cyber Intelligence team | | 2013-04-15 23:52:50.282529 |

Activity

Relationships (1)

| Type | Value | Type | Campaign |
|---------------|---------------------|------|----------|
| Indicators: 1 | Address - ipv4-addr | | |

Objects (2)

| Type | Name | Value | Date | Analyst | Source |
|----------------|------------|--------------|------------|---------|--|
| Kill Chains: 1 | Kill Chain | C2 | 2013-04-15 | | Name: GE Corporate Method: Static Analysis Reference: None |
| Roles: 1 | Role | Owned_Domain | 2013-04-15 | | Name: GE Corporate Method: Static Analysis Reference: None |

Structured indicator storage

Summary

| | |
|---|---|
| Type | URI - Domain Name |
| Value | badguys.com |
| Creation Date | 2013-04-15 23:49:57.575000 |
| Last Modified | 2013-04-15 23:49:57.575000 |
| Status | New |
| Confidence | <div><div></div><div>high</div></div> |
| Impact | <div><div></div><div>medium</div></div> |
| Sources | <div><div></div><div>GE Corporate (1): 2013-04-15</div></div> |
| Method: http://wikientry.com | |
| Analyst: Created: 2013-04-15 23:49:57.575000 | |

Actions

| Type | Begin | End | Performed | Active | Reason | Date Added | Analyst |
|------|----------------------------|----------------------------|-------------|-----------------------|--------|----------------------------|---------|
| | 2013-04-08 00:00:00.000000 | | on | Auto deployment | | 2013-04-15 23:51:07.755000 | |
| | | | in progress | QA process curve | | 2013-04-15 23:51:37.843000 | |
| | 2013-04-01 00:00:00.000000 | 2013-04-08 00:00:00.000000 | | FP, action turned off | | 2013-04-15 23:52:03.932000 | |

Tickets

| Ticket Number | Date | Analyst |
|---------------|----------------------------|---------|
| 123456 | 2013-04-15 23:52:15.607000 | |

Campaigns

| Campaign | Confidence | Description | Analyst | Date |
|----------|------------|--|---------|----------------------------|
| | high | This was witnessed in an internal GE event with confirmed attribution by the Cyber Intelligence team | | 2013-04-15 23:52:50.282529 |

Activity

Relationships (1)

| Type | Value | Type | Campaign |
|---------------|---------------------|------|----------|
| Indicators: 1 | Address - ipv4-addr | | |

Objects (2)

| Type | Name | Value | Date | Analyst | Source |
|----------------|------------|--------------|------------|---------|-----------------------------------|
| Kill Chains: 1 | Kill Chain | C2 | 2013-04-15 | | GE Corporate Static Analysis None |
| Roles: 1 | Role | Owned_Domain | 2013-04-15 | | GE Corporate Static Analysis None |

Campaigns show the threat actor attribution from the Cyber Intelligence teams

Structured indicator storage

Summary

| | |
|---------------|---|
| Type | URI - Domain Name |
| Value | badguys.com |
| Creation Date | 2013-04-15 23:49:57.575000 |
| Last Modified | 2013-04-15 23:49:57.575000 |
| Status | New |
| Confidence | <div><div></div></div> high |
| Impact | <div><div></div></div> medium |
| Sources | <div><div></div></div> GE Corporate (1): 2013-04-15 |
| | Method: Reference: http://wikientry.com |
| | Analyst: Created: 2013-04-15 23:49:57.575000 |

Actions

| Type | Begin | End | Performed | Active | Reason | Date Added | Analyst |
|------|----------------------------|----------------------------|-----------|-------------|---------------------------------------|----------------------------|---------|
| | 2013-04-08 00:00:00.000000 | | | on | Auto deployment | 2013-04-15 23:51:07.755000 | |
| | | | | in progress | QA process queue | 2013-04-15 23:51:37.843000 | |
| | 2013-04-01 00:00:00.000000 | 2013-04-08 00:00:00.000000 | | off | Indicator was a FP, action turned off | 2013-04-15 23:52:03.932000 | |

Tickets

| Ticket Number | URL | Date | Analyst |
|---------------|-----|----------------------------|---------|
| 123456 | | 2013-04-15 23:52:15.607000 | |

Campaigns

| Campaign | Confidence | Description |
|----------|------------|--|
| | high | This was witnessed in an internal GE event with confirmed attribution by the Cyber Intelligence team |

Activity

Relationships (1)

| Type | Details |
|---------------|--|
| Indicators: 1 | <div><div></div></div> Value: Address - ipv4-addr Type: Campaign |

Objects (2)

| Type | Name | Value | Date | Analyst | Source |
|----------------|------------|--------------|------------|---------|--|
| Kill Chains: 1 | Kill Chain | C2 | 2013-04-15 | | Name: GE Corporate Method: Static Analysis Reference: None |
| Roles: 1 | Role | Owned_Domain | 2013-04-15 | | Name: GE Corporate Method: Static Analysis Reference: None |

Relationships build out the larger picture of how various pieces of intelligence are linked

Structured indicator storage

Summary

| | | | |
|---------------|--|--|--|
| Type | URI - Domain Name | | |
| Value | badguys.com | | |
| Creation Date | 2013-04-15 23:49:57.575000 | | |
| Last Modified | 2013-04-15 23:49:57.575000 | | |
| Status | New | | |
| Confidence | <div><div></div></div> high | | |
| Impact | <div><div></div> medium</div> | | |
| Sources | + GE Corporate (1): 2013-04-15 | | |
| | Method: Reference: http://wikientry.com | | |
| | Analyst: Created: 2013-04-15 23:49:57.575000 | | |

Actions

| Type | Begin | End | Performed | Active | Reason | Date Added | Analyst |
|------|----------------------------|----------------------------|-----------|-------------|---------------------------------------|----------------------------|---------|
| | 2013-04-08 00:00:00.000000 | | | on | Auto deployment | 2013-04-15 23:51:07.755000 | |
| | | | | in progress | QA process queue | 2013-04-15 23:51:37.843000 | |
| | 2013-04-01 00:00:00.000000 | 2013-04-08 00:00:00.000000 | | off | Indicator was a FP, action turned off | 2013-04-15 23:52:03.932000 | |

Tickets

| Ticket Number | URL | Date | Analyst |
|---------------|-----|----------------------------|---------|
| 123456 | | 2013-04-15 23:52:15.607000 | |

Campaigns

| Campaign | Confidence | Description | Analyst | Date |
|----------|------------|--|---------|----------------------------|
| | high | This was witnessed in an internal GE event with confirmed attribution by the Cyber Intelligence team | | 2013-04-15 23:52:50.282529 |

Activity

Relationships (1)

| Type | Value |
|---------------|---------|
| Indicators: 1 | Address |

Objects allow us to tag intelligence with context such as the Kill Chain or what role the intelligence plays

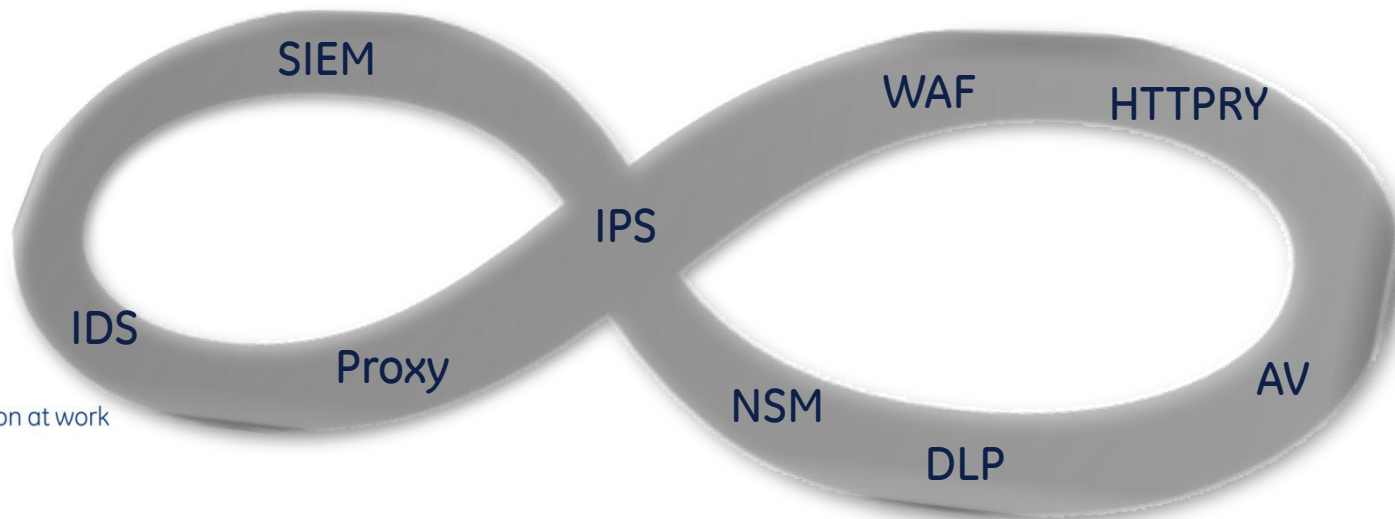
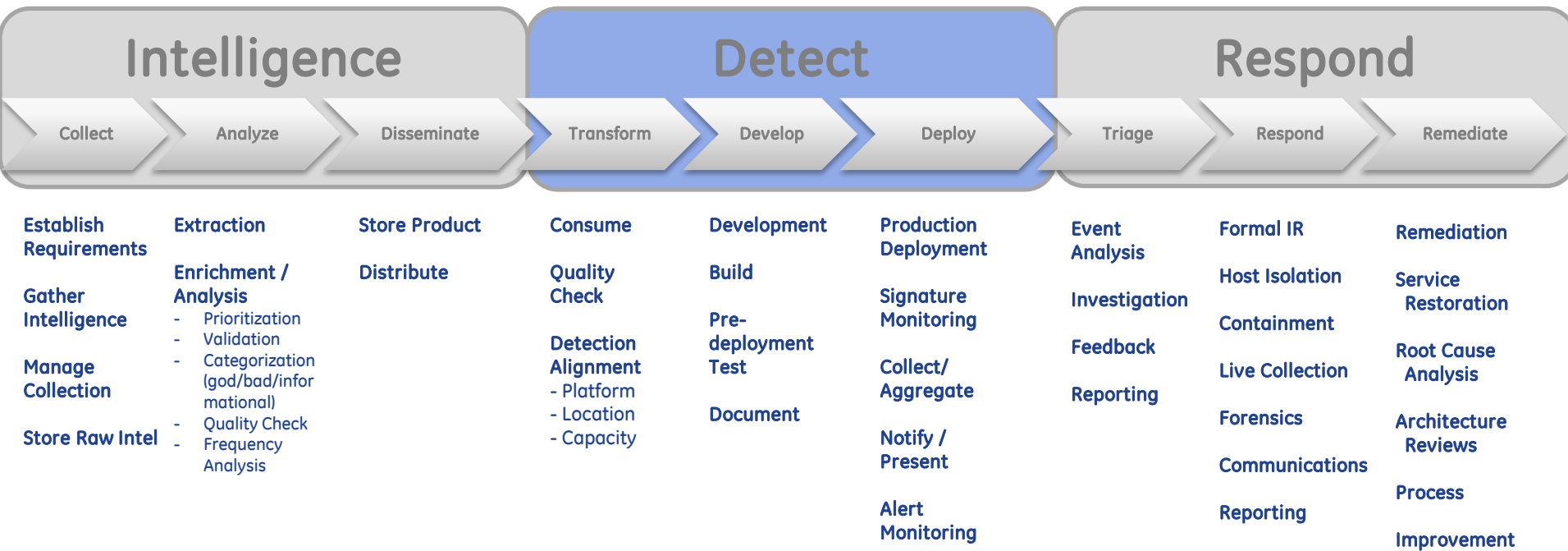
Objects (2)

| Type | Name | Value | Date | Analyst | Source |
|----------------|------------|--------------|------------|---------|-----------------------------------|
| Kill Chains: 1 | Kill Chain | C2 | 2013-04-15 | | GE Corporate Static Analysis None |
| Roles: 1 | Role | Owned_Domain | 2013-04-15 | | GE Corporate Static Analysis None |

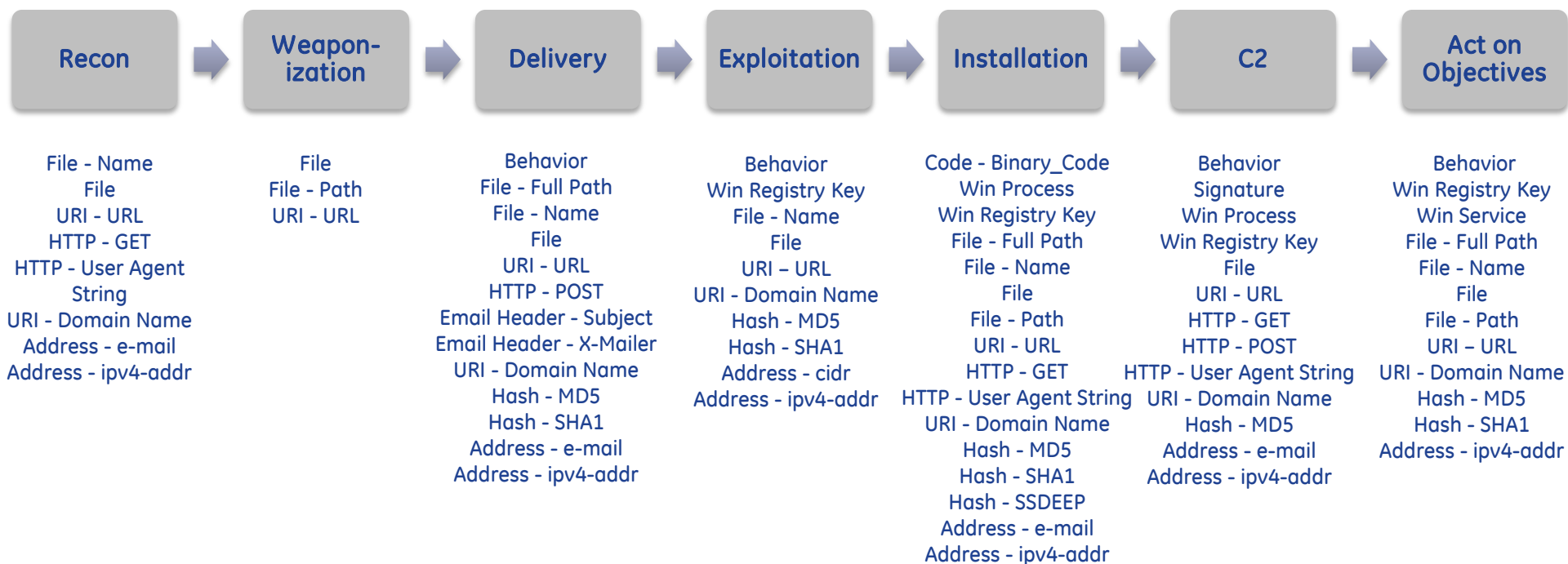
Detect



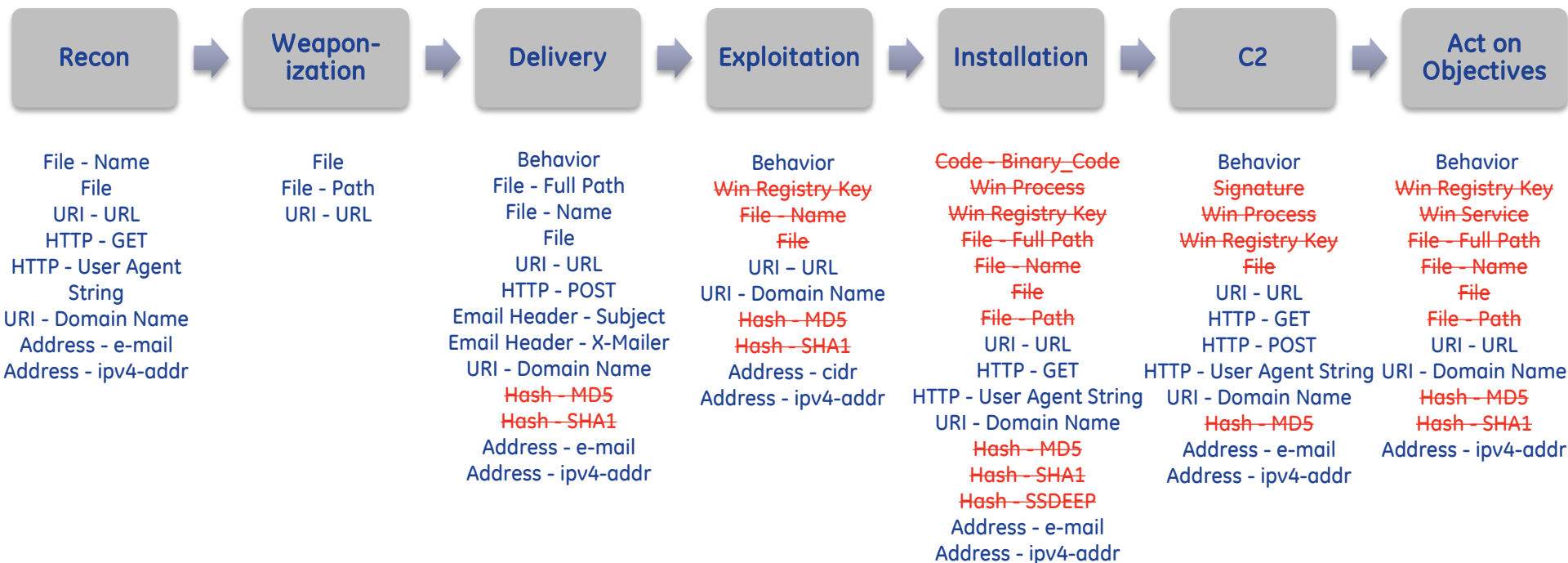
Intel driven, threat centric detection



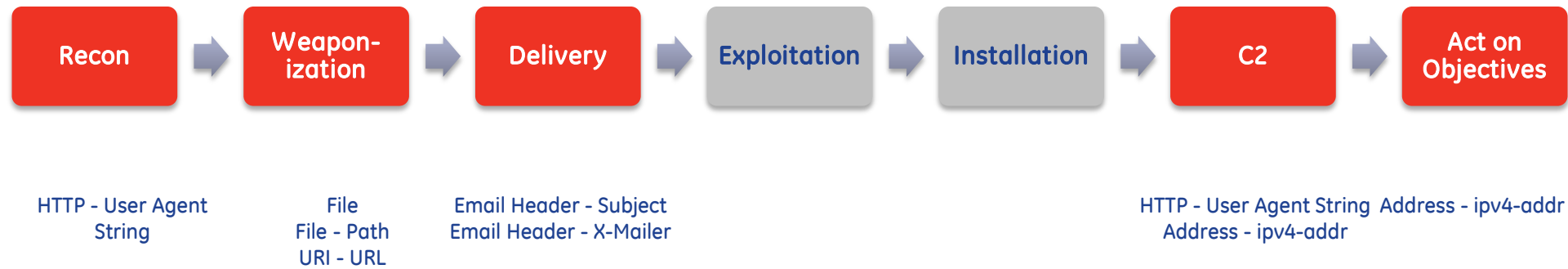
Detection scenarios



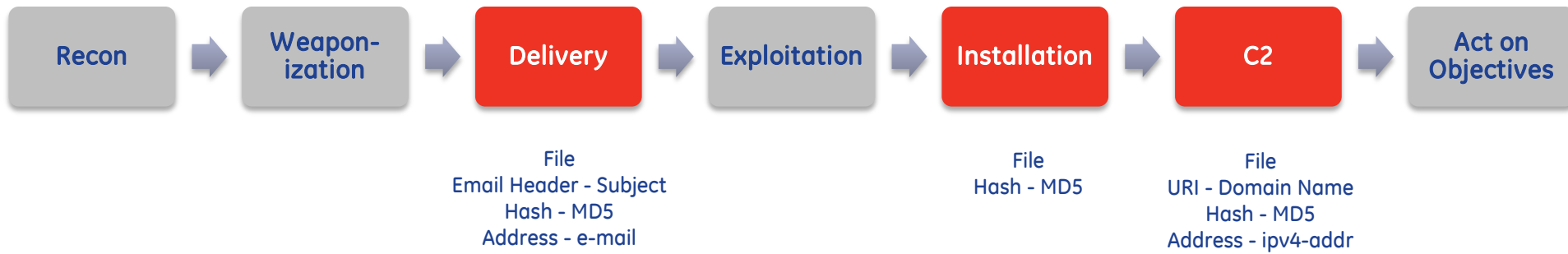
Platform strengths (IPS+)



Detection visibility gaps



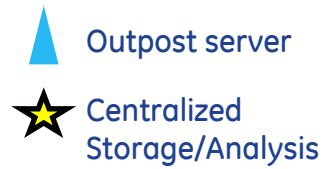
Detection gaps per actor



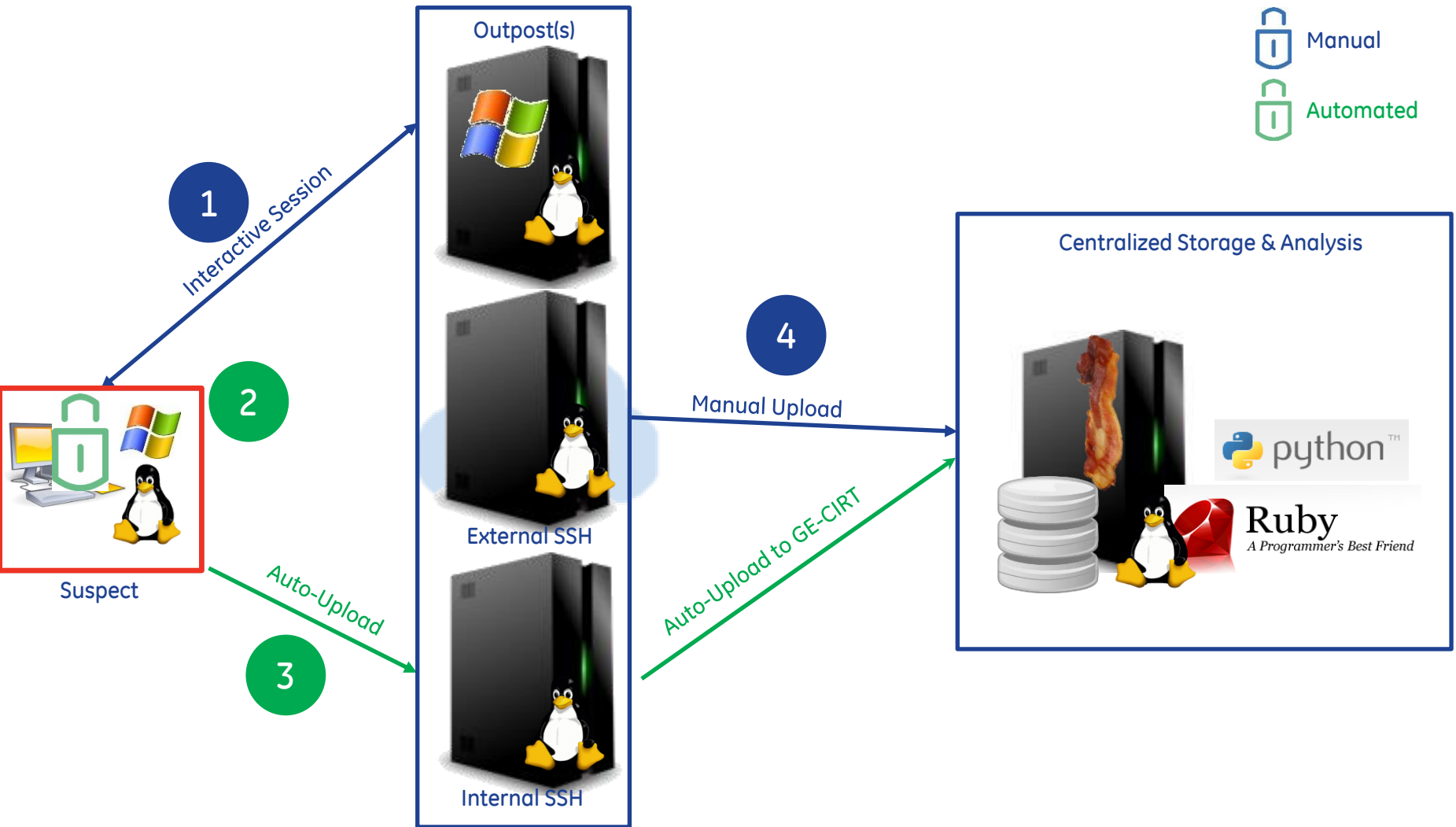
Contain & Collect



Outpost locations



Automated & centralized C&C



Containment selection

- ✓ Find host and system type
- ✓ Identify operating system
- ✓ Determine if the host is online or offline
- ✓ Identify if the system is on VPN

| Method | Time | Desktop | Laptop | Server | Windows OS | Other OS | VPN | Offline | Evidence Impact |
|-----------|------|---------|--------|--------|------------|----------|-----|---------|-----------------|
| /ACL | 2hrs | Y | N | Y | Y | N | N | | 1 |
| solator | 30m | Y | Y | Y | N | N | N | | 2 |
| Active | 15m | Y | Y | Y | N | Y | Y | | 2 |
| Directory | | | | | | | | | |

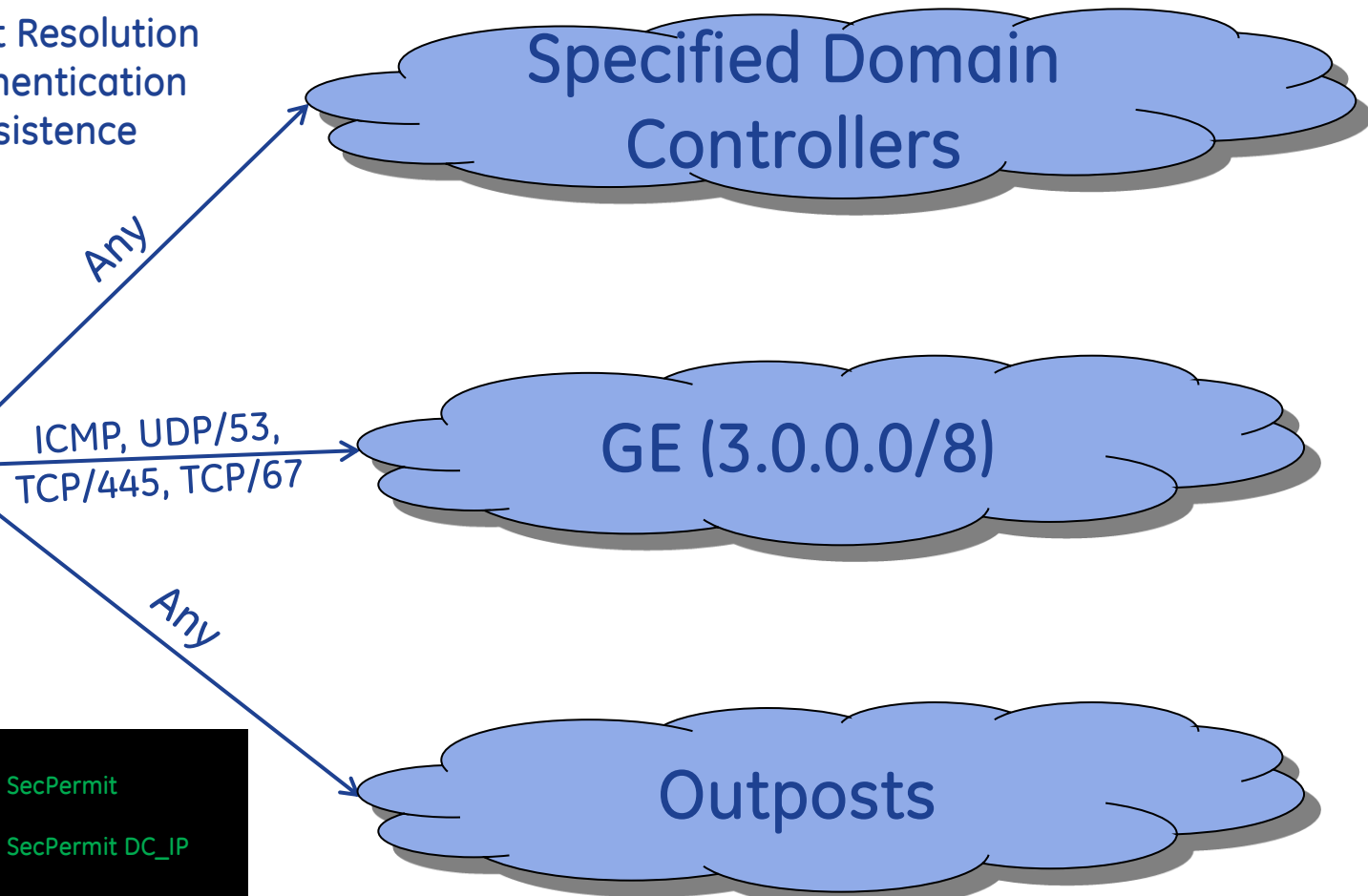


GE imagination at work

Virtual Isolation



- ICMP – Network Identification
- DNS (UDP/53) – Host Resolution
- SMB (TCP/445)– Authentication
- DHCP (TCP/67) - Persistence



```
C:\Isolator.bat
Netsh ipsec add policy "virtual isolation" SecPermit
Outpost_IP ANY ANY
Netsh ipsec add policy "virtual isolation" SecPermit DC_IP
TCP TCP
Netsh ipsec add policy "virtual isolation" SecPermit 67 TCP
TCP
Netsh ipsec add policy "virtual isolation" SecPermit 53 ANY
ANY
Netsh ipsec add policy "virtual isolation" SecPermit 445 TCP
TCP
Netsh ipsec add policy "virtual isolation" Block ANY ANY ANY
more %cd%\usernotification.txt | msg %username%
```

Quarantine



Internet Routable GE IPs

GE IP Space



Suspect

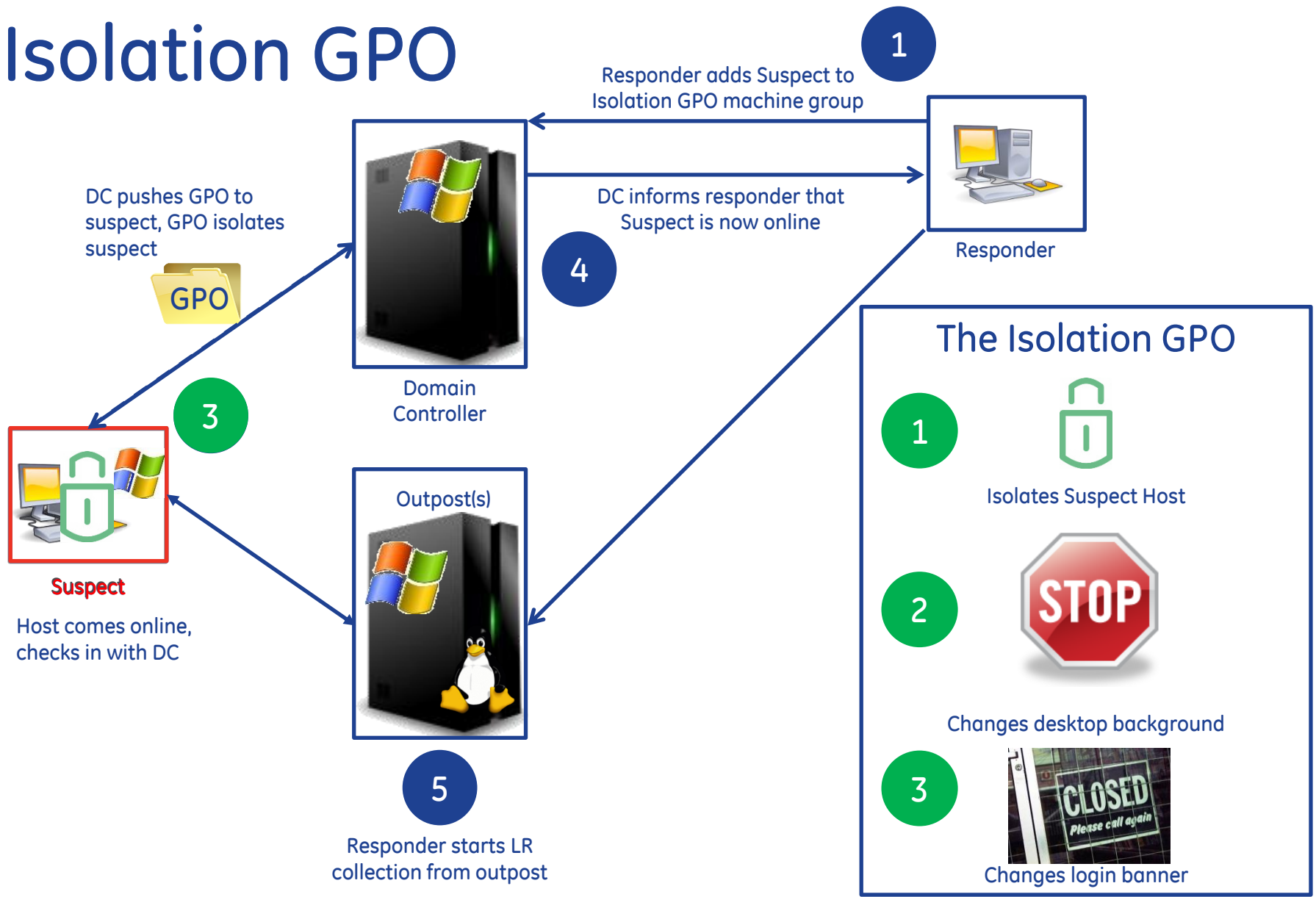
GE (3.0.0.0/8)

VPN IPs

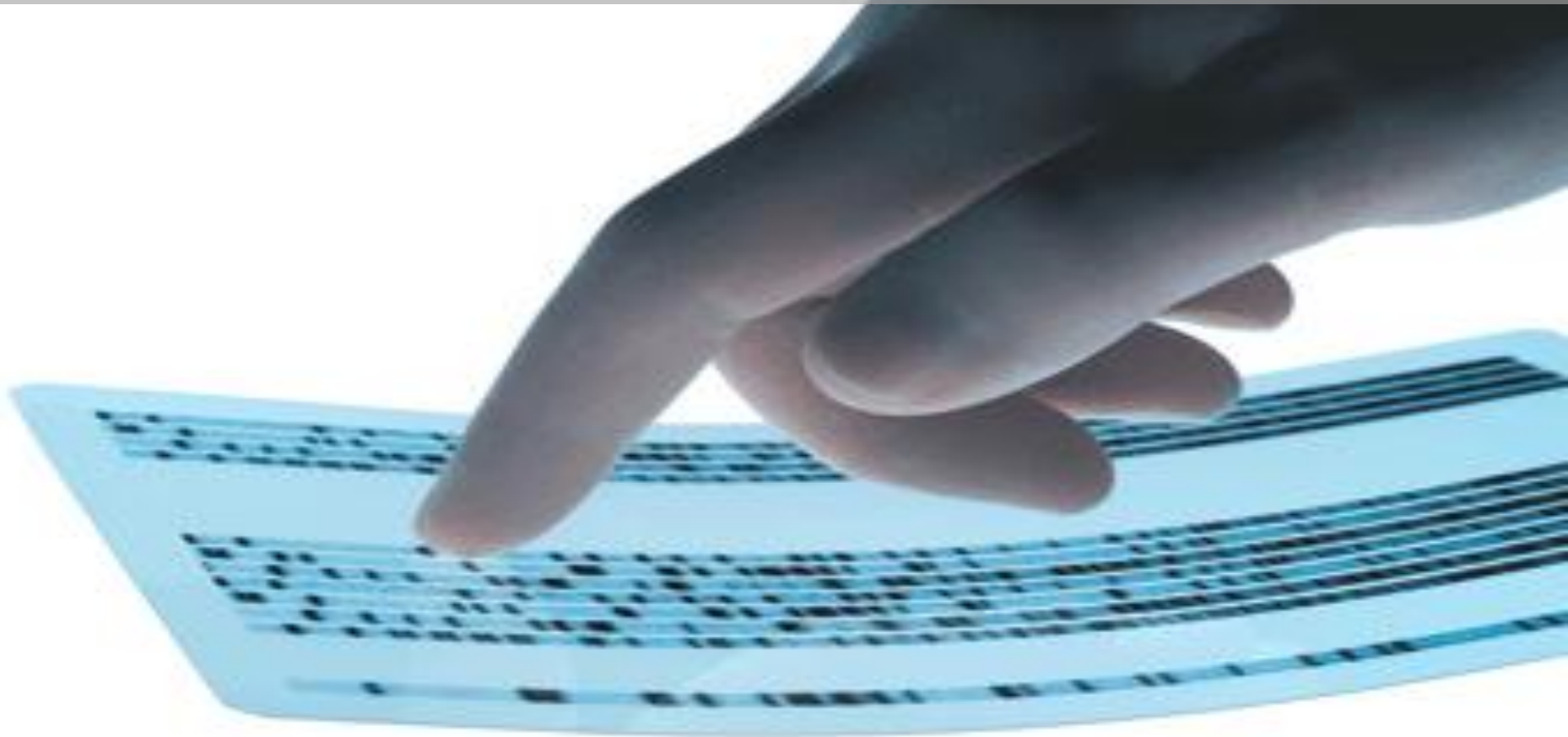
Necessary Protocols*

- *- ICMP – Network Identification
- *- DNS (UDP/53) – Host Resolution

Isolation GPO



Analysis



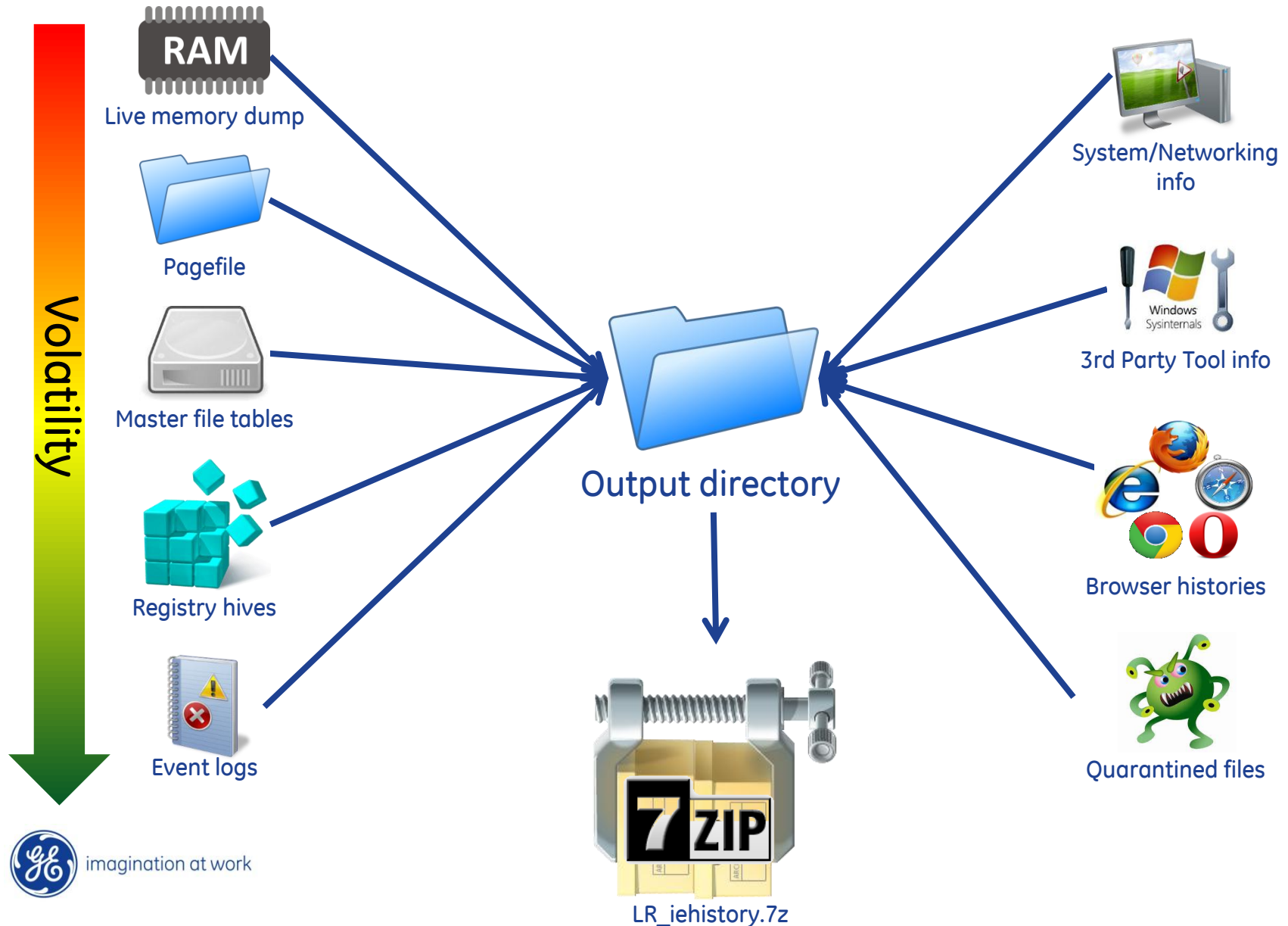
Analysis infrastructure

- 4 x Intel Xeon 2.4GHz (8 cores/ea)
- 48 x 32GB RAM (1.5TB)
- 16 x 900GB (13.5TB)

“\$MFT that used to take 6hrs to parse took only 30 minutes”



Live Response (LR)



Automated analysis processing

```
( ( . )
) ( . ' . ' . ' .
( , ) ( . ) ( ' , (
.' ) ( . ) , ( , ) )
). , ( . ( ) ( , ' ) . ' ( , (
( , ) . ) , ) _ _ , ' ) ( , ) ' . ) , )
`7 MM""""YM db ( ' ( ' ' ' ( ,
MM ) ' ) ( ) (
MM d `7MM `7Mb,od8 .gP"Ya n , 0
MM""MM MM MM' "' ,M' Yb | '---`_/_>
MM Y MM MM 8M"""""""" '-----`_/|
MM MM MM YM. J J
.JMML. .JMML..JMML. `Mbmmd'
=====
Forensic Incident Response Extractor
```

- ✓ Execute tasks in parallel as sub process
- ✓ Each module can be run “standalone”

1. Extract compressed LR
2. \$MFT processing
3. HPAK & memory processing
4. Yara scanning
5. Greps/master timeline/wiki

| | | | | |
|------------------------------|-----------------------|-----------------------|---------------------------------------|-------------------|
| browser_chrome_history.csv | combined_timeline.err | memdump.bin.str | sessions_log.txt | volatility |
| browser_firefox2_history.csv | dumpfile.sys | raw_data | aliced | wiki.txt |
| browser_firefox3_history.csv | dumpfile.sys.str | reg_ntuser_timeline | T00741986.20130213_C.mft.residentevil | yara_bin.log |
| browser_ie_history.csv | greps | reg_sam_timeline | T00741986.20130213_C.mft.timeline | yara_csv.log |
| browser_opera_history.csv | log_evt_timeline.csv | reg_software_timeline | T00741986.20130213_log.txt | yara_lr.log |
| browser_safari_history.csv | log_evtx_timeline.csv | reg_system_timeline | T00741986.20130213_SchedLgU.txt | yara_tdt.log |
| combined_timeline | memdump.bin | sessions7_log.txt | T00741986.20130213.txt | yara_timeline.log |

Remediation



Prevention

- Leverage Intel, Detect, & Response to support prevention
- Root Cause Analysis
- Failure Mode Analysis

Task Force template

(What did the actor do?)

(Why did it work?)

(What should we do?)

| Kill Chain | Actor Action | Failure Mode | Mitigation Action |
|-------------------|--|---|---|
| Reconnaissance | Used web commercial scanner | Potential gaps in threat tool & scanning capability | Establish detection capability |
| Weaponization | | | |
| Delivery | SQL injection on vulnerable ASP page to gain admin user access | Could not detect SSL traffic; vulnerable to SQL injection | Explore Secure Development and Application Security Assessments |
| Exploitation | | | |
| Installation | IIS web service used to upload web shell | Failure to restrict file upload types or configure web server to not execute uploaded files | Explore Secure Development and Application Security Assessments |
| Comm & Control | Used web shell on initially compromised host | Could not detect SSL traffic | |
| Actions on intent | Accessed "id.txt" which held account information with admin access | Management scripts failed to delete "id.txt" after running | Scripts retired and environment scanned. |

Task Force
initialization

IR
Knowledge
Transfer

Task Force
kick-off

Failure
Mode
Analysis

Mitigation
Action Plan

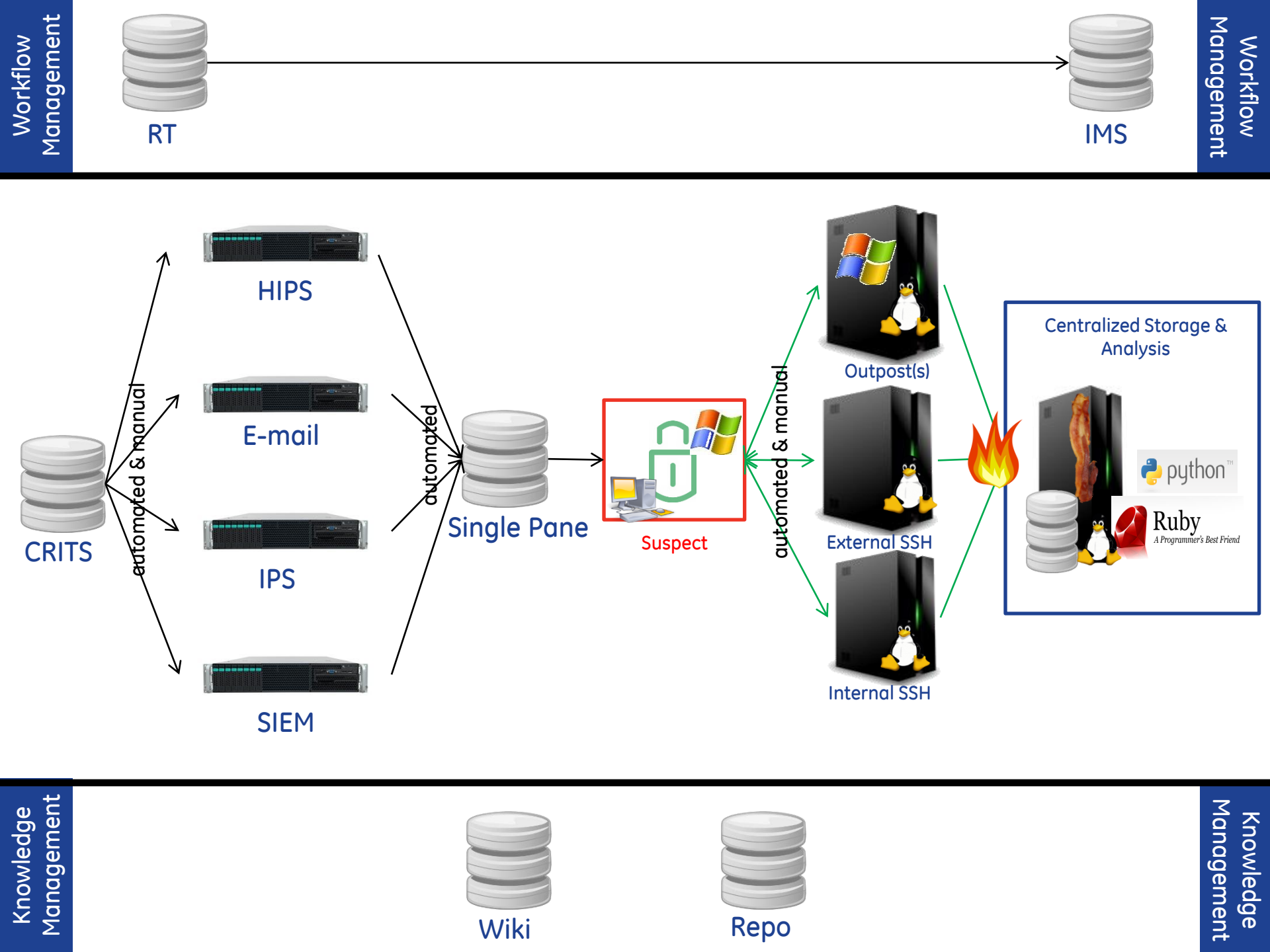
Transition to
long-cycle
tracking

Example data

Putting it all together...



imagination at work



In conclusion...

1. Intel & IR work is a process that can be measured, evolved and simplified.
2. Partnerships & open source intel collection are critical to success.
3. Detection should be based on a foundation of prioritized intel; understand your capabilities and gaps.
4. Risk based approach to containment. No one size fits all model.
5. Invest in your analysis infrastructure- it will reduce response time.
6. Communicate findings and learning back into other functions.

Build a thriving Intel & IR ecosystem for your company.

QUESTIONS



imagination at work

#contact
@SeanAMason