SANS SEC 450.1 Blue Team Tools and Operations summary

1. SOC Overview

Blue team components:

1. **People:** Performing analysis and investigation, design and run processes.
2. **Process:** The defined sequence of events performed to achieve an end goal.
3. **Technology:** Hardware and software used to accomplish the mission

Cyber security operations means protecting the CIA of information systems through **proactive design** and **configuration**, **ongoing monitoring** of system state, **detection** of unintended actions, and **minimizing damage** from unwanted effects.

❖ we should make balance between security and productivity.

SOC functions:

- Collection
- Detection
- Triage & investigate
- Incident response

SOC Roles and Duties:

- **Analyst:** Investigate and triage alerts, incident response.
- **Threat Intel:** Collect info for tactical and strategic advantage over adversaries.
- **Engineering and Infrastructure:** Design and implement SOC infrastructure.
- **System Administrator:** Care and upkeep of SOC tools.
- **Manager:** Responsible for work prioritization and communication upwards.
- **Incident Lead:** Designated coordinator and communicator.

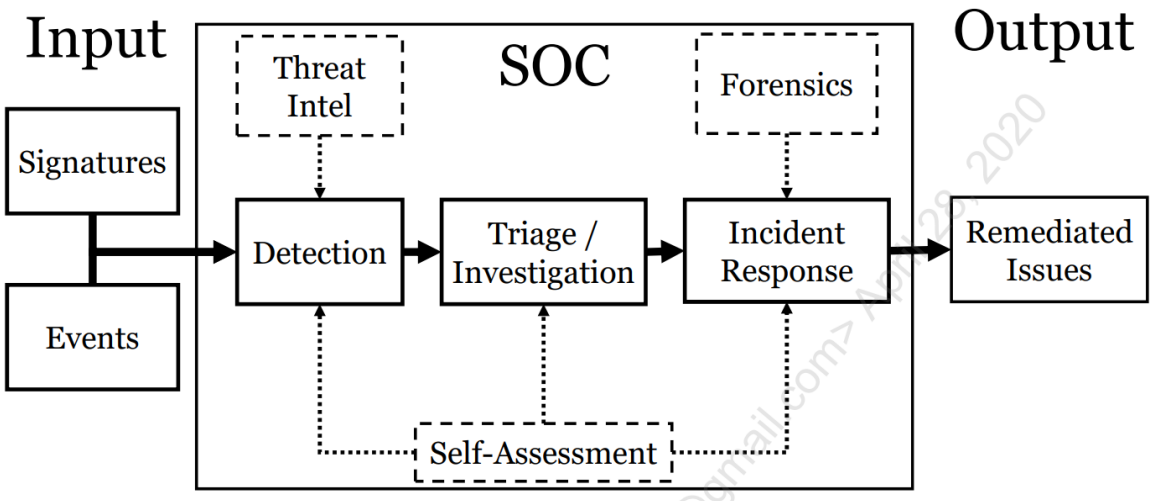
Tiered SOC & Tierless SOC:

- **Tiered SOC:** each one within the team has his own tasks, the team divided 3 tiers:
  - **Tier 1:** Initial triage and analysis, ticket generation, it may also involve restrictions on which tools an analyst is allowed to use, and which data can be viewed.
  - **Tier 2:** Attack scoping, further analysis, tactical and remediation support.
  - **Tier 3:** Deep analysis, methodology development, strategic support, hunting.

❖ Tiers 2 and 3 typically involve increasing amounts of freedom, less process and more complex tasks.

- **Tierless SOC:** Everyone works together to get everything done, Even new analysts can use all available data and tools.

Inside the SOC System



Documents Analysts Must Be Familiar With:

- **Policies:** high level, they generally answer the "what" must be done. Mandatory.
- **Standards:** standards give more specifics in that they specify "how" something gets accomplished or how much of something should be applied. Mandatory.
- **Procedures:** Procedures explain the step-by-step instructions for completing a specific task.
- **Guidelines:** suggestions and recommended actions. Not mandatory.
- **Baselines:** Highly detailed and itemized checklists.
- **Playbooks / Use Cases:** they are pre-configured steps that the analysts follow to accomplish a specific task, its always useful for newer analysts.

2. Defensible Network Concepts

a defensible network is:

- **Monitored:** Network and host data is captured and centralized.
- **Inventoried:** Knowing your network.
- **Controlled:** Traffic ingress/egress, network connection access.
- **Claimed:** knowing the owners of services, and put polices, standards and procedures.
- **Minimized:** System attack surface is reduced.
- **Assessed:** Weaknesses identified.
- **Current:** Patched and known vulnerabilities addressed.
- **Measured:** SOC and IT measure progress against previous steps.

monitoring divided into 2 types:

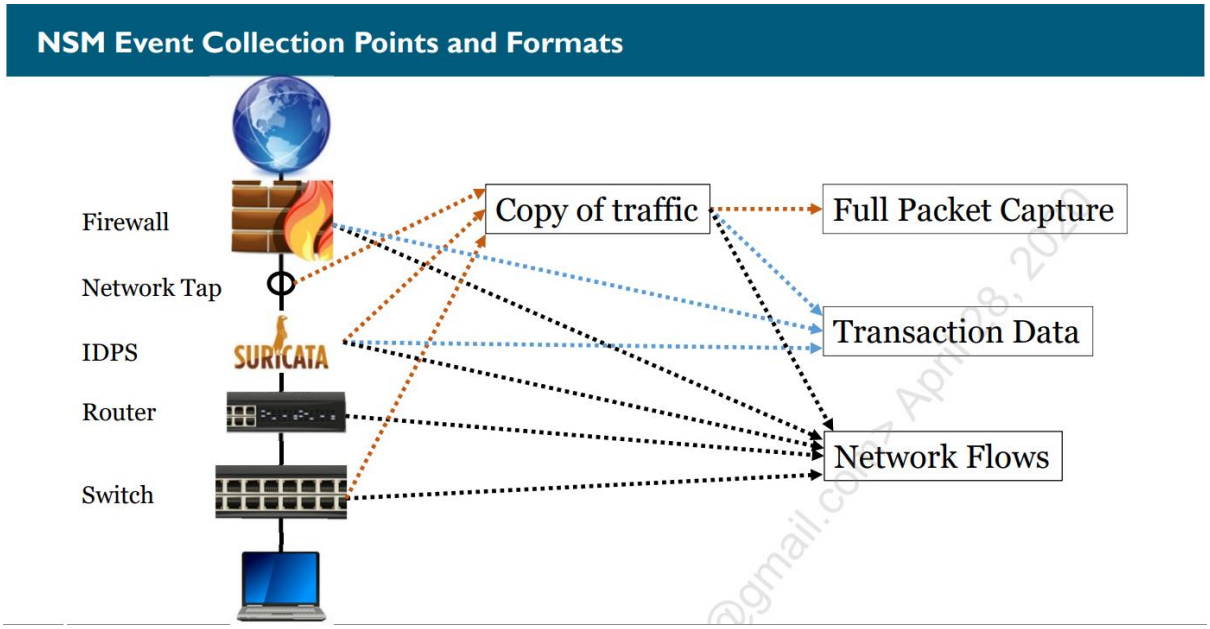
- Network security monitoring (NSM).
- Continuous security monitoring (CSM). → end points monitoring.

❖ **NSM collection sources:** firewall, NIDS, NIPS, router, switch.

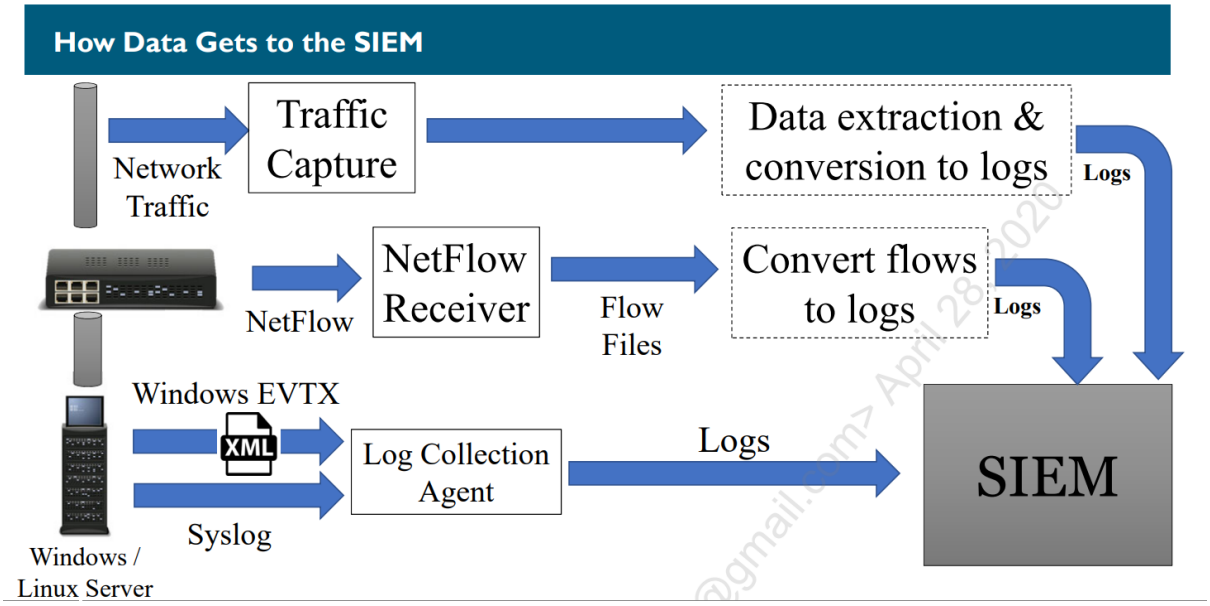
❖ **CSM collection sources:** OS/Application logs, Sysmon, antivirus, whitelisting, HIDS, HIPS, vulnerability scanner.

NSM by Layer

- **Layer 3/4 (IP/Port):** NetFlow, Statistical Data, Firewall Logs, almost anything
- **Layer 7 Transaction Data:** Service Logs, NSM Sensor Data
- **Layer 7 Full Payload:** Packet Capture, IDS alerts



- **SIEM** is a centralized data collection which holds all the data collected from network and endpoints.
  - some data that is recorded is not in the format of text logs by nature and must be converted, there should be converted into text that could be parsed and saved by the SIEM.
  - Without a SIEM centralizing logs, if you had to investigate activity for a given IP address, you would have to log into every application individually and try to put all the pieces of an incident together.



3. Events, Alerts, Anomalies, and Incidents

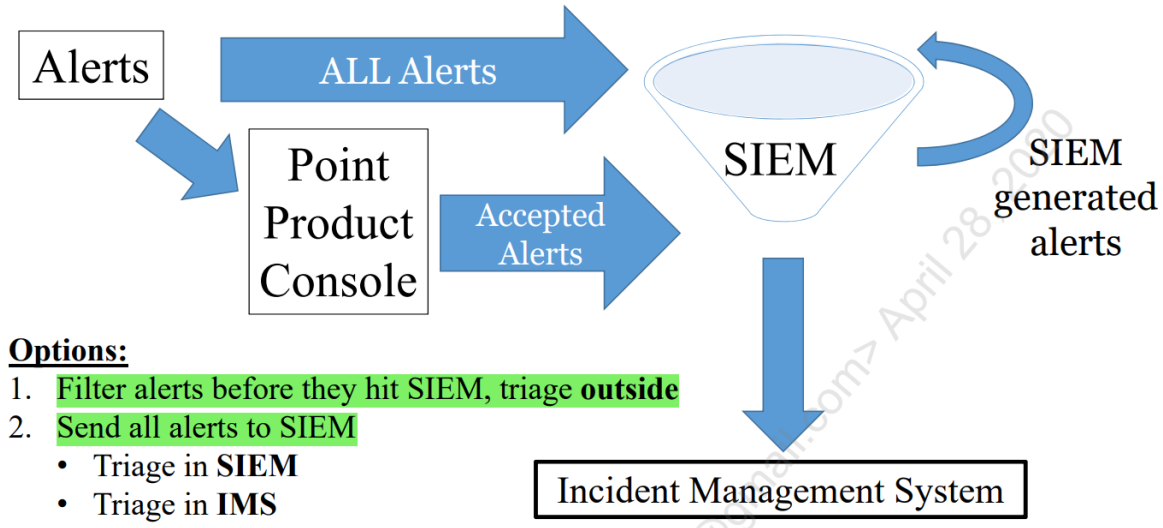
- **Events:** Any observable occurrence in a system or network.
- **Alerts:** An event of interest that may be unwanted or unauthorized.
- **Incidents:** A violation or imminent threat of violation of computer security policies.

❖ All observable occurrences are events, and some of those events that are interesting will be alerted upon. Alerts are then collected (often in a SIEM) and triaged by an analyst that can confirm them as incidents. Once an alert has been confirmed to be an incident, it will be worked in an incident management system.

❖ While collecting data it's not necessary to collect everything within the network not to slow down the SIEM, if you can show that a subset of them are providing no value, don't be shy cutting them out.

❖ Triaging alerts in a separate interface before they reach the ticketing system will reduce the chance to make false positive alerts.

Alert Log Flow Options:

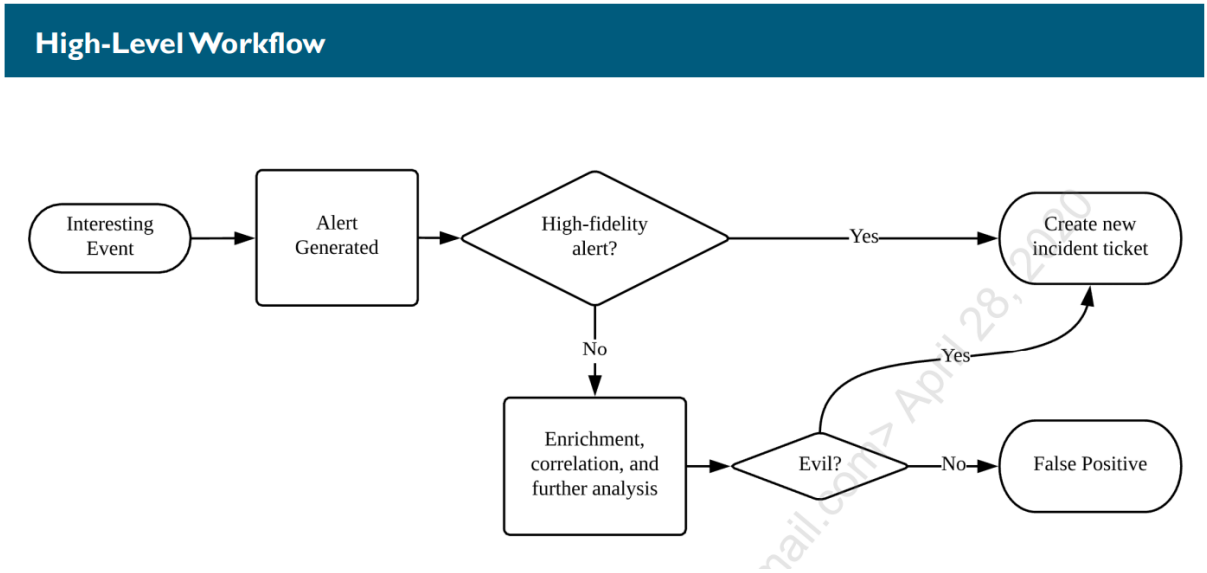


1. **Filter alerts before they hit SIEM, triage outside** For low-fidelity alerts/anomalies (alerts that have not been yet confirmed as malicious), false positives reduction early in the process.
2. **Send all alerts to SIEM** and we can triage alerts using :
   - SIEM built-in alert triage system.
   - Incident management system with alert dashboard.

Flavors of alerts:

1. **Signatures:** blacklist-based which will alert on any observed indicators such as URLs or IPs that are known bad.
   - ➢ IDS/IPS, Firewall, AV
2. **Anomalies:** will alert when it notice things that are unusual to the network such moving executables from one unexpected source to another, large file uploads, a user logging in from a new computer that they've never used before, this type will create false positives alerts more than signature-based.
   - ➢ User Behavior Analysis, ILP, some IDS

When an Alert Fires



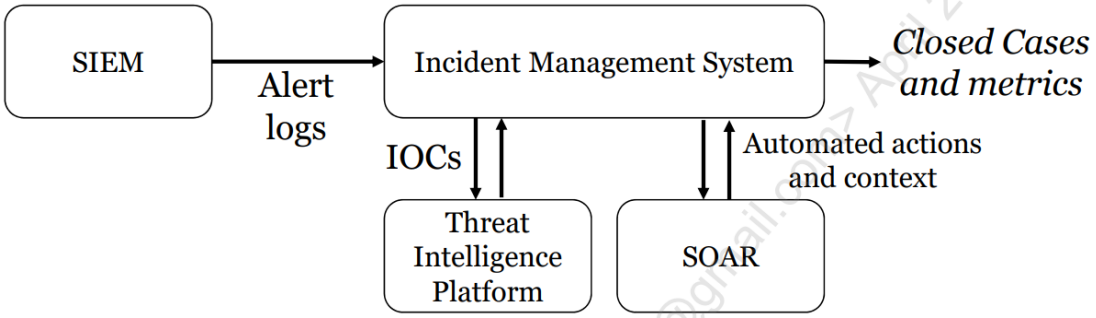
4. Incidents management systems

Tools for SOC Data Organization and Search:

- **Incident Management System (IMS):** the system where all recorded incidents will be investigated and worked, like TheHive.
- **Threat Intelligence Platform (TIP):** the system where the collected information about adversaries will be stored.
- **Security Information and Event Management (SIEM):** Log collection, indexing, search, correlation and alerting.
- **Security Orchestration, Automation and Response (SOAR):** Automation of common tasks, orchestration of workflow.
- **Knowledge Database:** playbooks, and use cases.

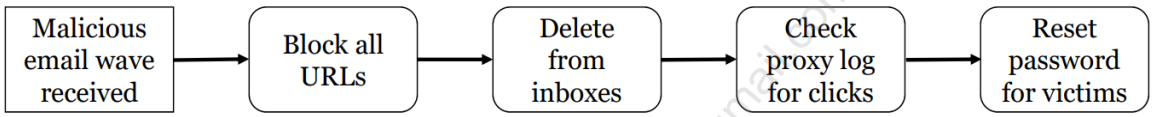
Incident Management System (IMS)

- ❖ after the IMS receives an evil event (incident) it creates an incident ticket (queue).
- ❖ When processing these cases, incident management systems may be integrated with multiple other tools like the threat intelligence platform or a security orchestration, automation, and response platform. The connection allows the data related to the ticket such as malicious domain names to be stored into the TIP, as well and are used by the SOAR platform for enrichment and additional context gathering.



Playbook

- ❖ a set of expected actions for alert response.
- ❖ Contain required and optional steps for analysis and closure.
- ❖ Guide analysts toward standardized analysis and completeness.
- ❖ Unique for each type of case (phishing vs. malware playbooks).



TheHive tool supports alert input, case creation, playbooks in a form it calls "case templates", and tasks inside those playbooks that each individually have their own "worklog" where notes can be taken. Indicators associated with a case are all stored in what is called "observables" and these can be automatically sent to threat intelligence platforms, as well as enriched through a complementary piece of software called the Cortex engine.

- ❖ observables like IP addresses, usernames, hostnames, URLs, or hashes can be added to the case. Then applies a modular set of analysers to these observables, which will further enrich the data and give the analyst additional information to help understand them.

Case and Alert Naming Convention

Format: {$UNIQUE_ID}-{HF,INV}-{$EVENTSOURCE}-{$REPORT_CATEGORY}: $DESCRIPTION

- **$UNIQUE_ID**
- **HF,INV** = High fidelity (almost sure it's not false positive) or investigative alert (one that isn't yet matured or isn't very reliable)
- **$EVENTSOURCE** = The source of the data, This would be IDS, Antivirus, Firewall, etc.
- **$REPORT_CATEGORY** = Threats Snort ruleset – Malware, Policy, etc.
- **$DESCRIPTION** = A short but meaningful description of what condition the alert identifies

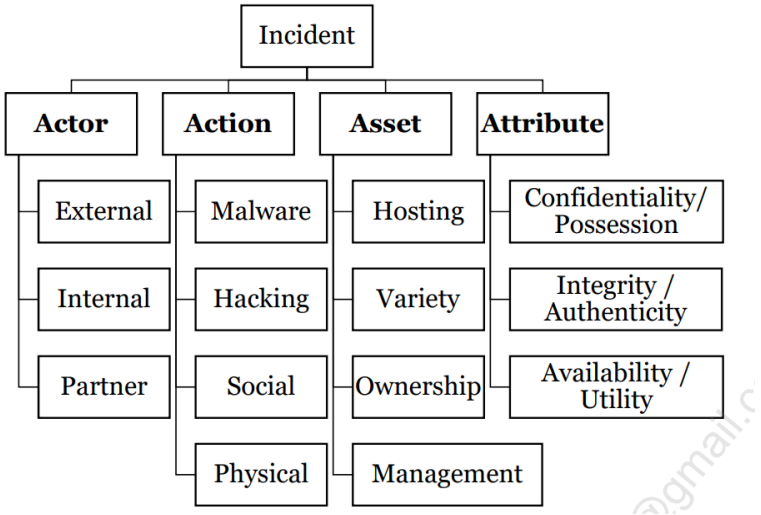
Case and Task Assignment

Multiple analysts can work in the same case if it is complicated, a complicated ticket with advanced steps such as malware or memory analysis may be still be taken by a newer analyst, but the steps that analyst is unfamiliar with can be individually passed on to someone who has the experience to complete the task. Both people can easily work the ticket in parallel and when complete, the original analyst can review the worklog for the tasks completed by others, which over time will act as instructions on how to perform that task.

Incident Categorization Frameworks

There are many options for categorization, like VERIS (Vocabulary for Event Recording and Incident Sharing), which categorize the incident into Actor, Action, Asset, and Attributes.

- **Actor:** Whose actions affected the asset?
- **Action:** What actions affected the asset?
- **Assets:** Which assets were affected?
- **Attributes:** How was the asset affected?



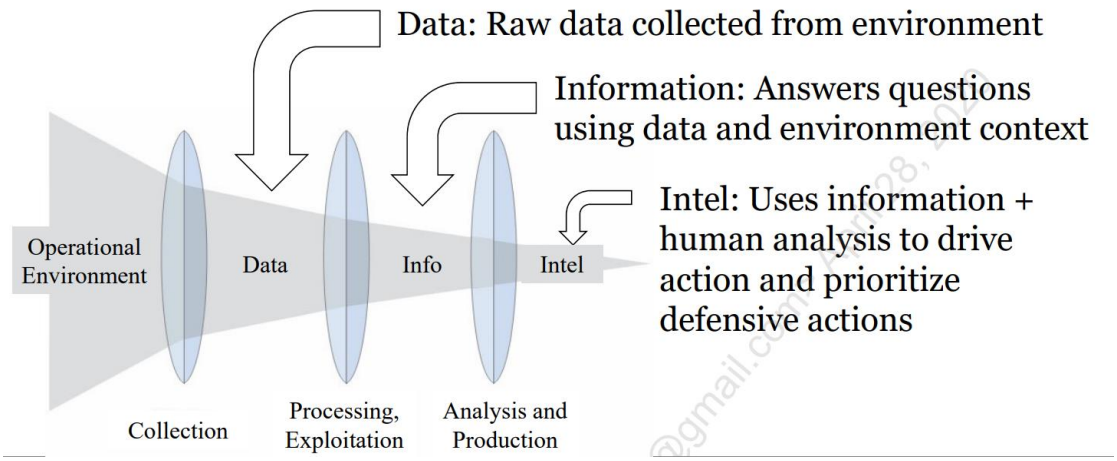
5. Threat Intelligence Platforms

1. **Intelligence:** Taking in external information from a variety of sources and analysing it against existing requirements in order to provide an assessment that will affect decision making.
2. **Threat intelligence:** The process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm.
3. **Cyber threat intelligence:** Threat intelligence is the analysis of adversaries – their capabilities, motivations, and goals; and cyber threat intelligence (CTI) is the analysis of how adversaries use the cyber domain to accomplish their goals.

❖ The main goal of cyber threat intelligence is to analyse cyber threat data to create information about a threat actor that helps us understand their tactics, techniques, and procedures and what their goals might be.

Threat data vs. threat information vs. threat intelligence

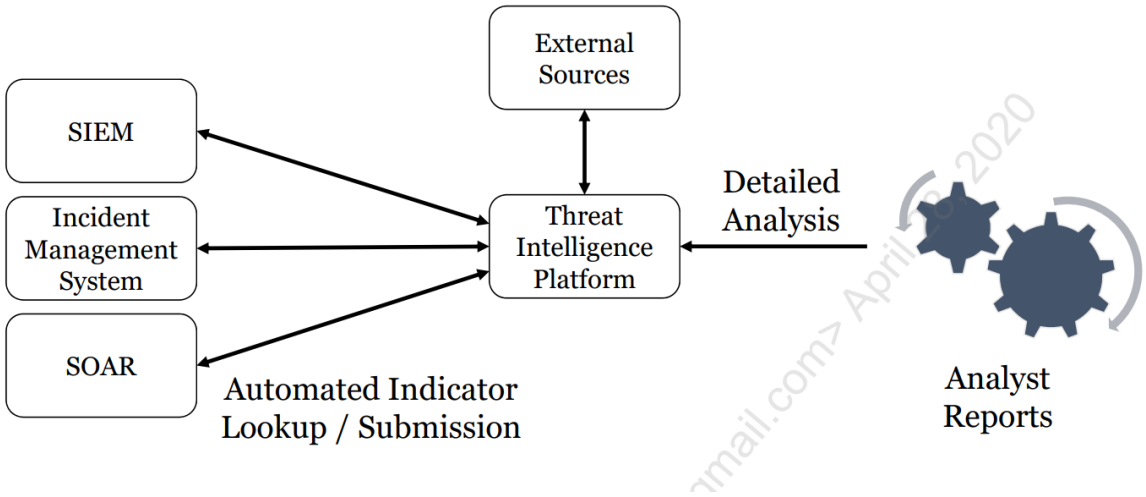
- **Threat data:** the raw information collected from the environment.
- **Threat information:** using analysis to answer a question using the threat data as input. For example, is a system on the network compromised? We could answer that question using threat data collected from the environment, possibly by looking for signs of malware communication or execution.
- **Threat intelligence:** analysis of multiple bits of threat information that drives an organization's security policy, spending, and defensive posture.



- ❖ Threat intel group produces intelligence, while analysts consume it.

Threat Intelligence Platforms: A threat intelligence platform's main purpose is to store the body of threat information, analysis, and indicators you have collected and then make it available in an easy-to-search way. The database will be manually searched as part of incidents, IMS and SIEM can send and pull information from it through an API of some sort.

Threat intelligence platform workflow

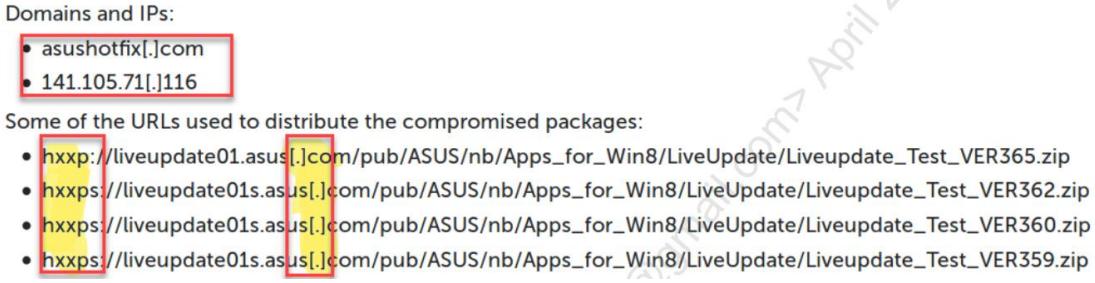


- ❖ the more sources you have of malicious indicators and threat information, the more likely you are to catch attackers in your own network.

De-fanged Indicators

Since many solutions will take valid URLs and IP addresses and make them "live", analysts often need to take extra precaution that this does not happen inside their own notes and tools.

To combat this issue, square brackets are often used before the TLD in URLs and in IP addresses so that links are invalid and will not become clickable. You may also see http or other protocols written with "x" instead to accomplish the same, this process is called indicators defanging.


Domains and IPs:

- asushotfix[.]com
- 141.105.71[.]116

Some of the URLs used to distribute the compromised packages:

- hxxp://liveupdate01.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER365.zip
- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER362.zip
- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER360.zip
- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER359.zip

Threat Intelligence Platform Products

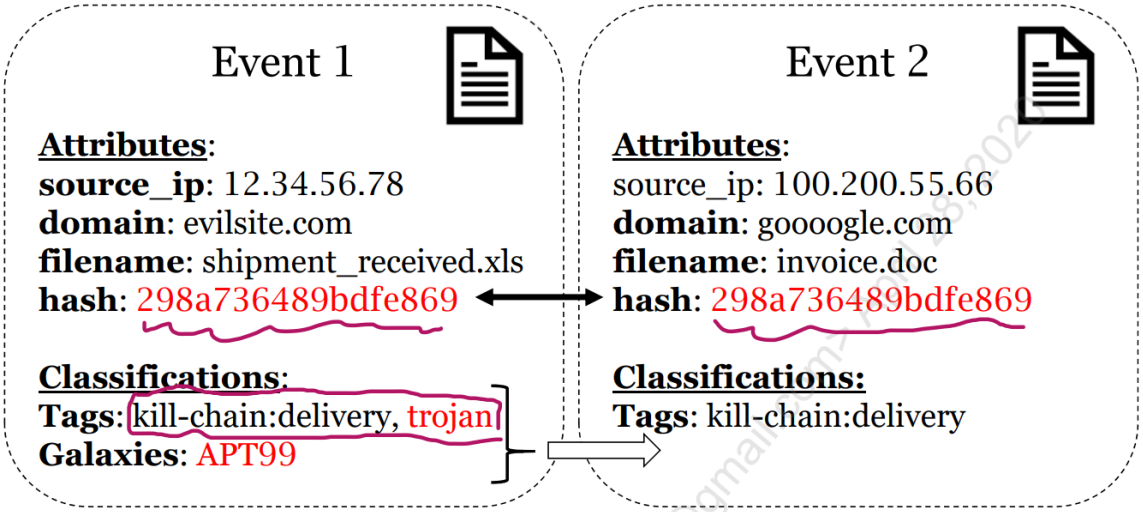
Self-Hosted, Free:

- MISP (Malware Information Sharing Platform)
- CIF (Collective Intelligence Framework)
- YETI (Your Everyday Threat Intelligence)
- CRITS (Collaborative Research Into Threats)

Cloud, Commercial:

- ThreatConnect
- AlienVault OTX
- Threat Quotient
- Anomali

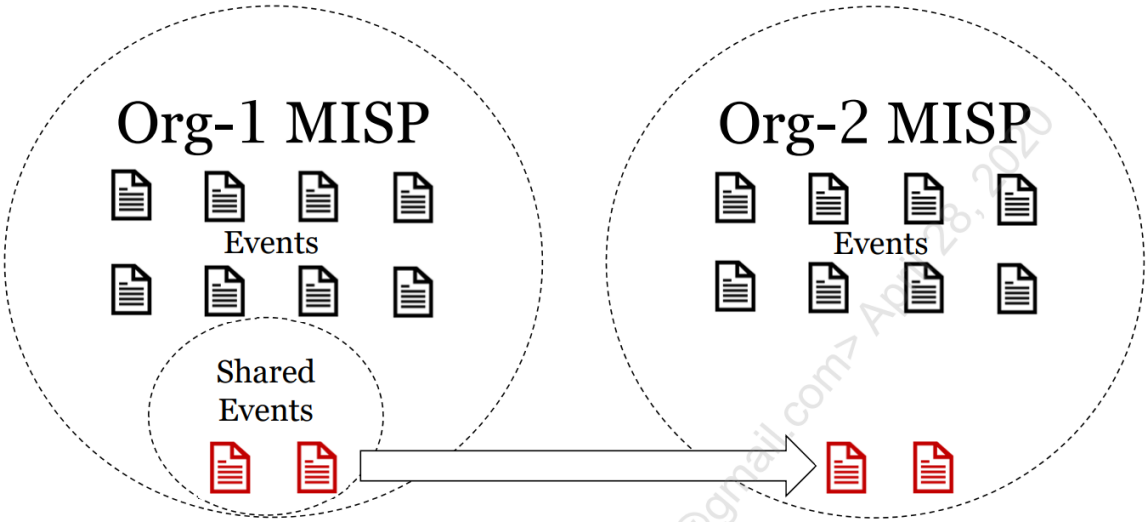
MISP Events



threat intelligence platform should highlight any other events that have the same values for indicators, allowing you to tie events 1 and 2 together and conclude that they are likely part of the same campaign from the same attacker, even though their filenames and source is different.

Notice that event 1 has already been classified as a trojan from APT99. An analyst entering the items for event 2 would ideally recognize that this hash has been seen before and not have to repeat the work done to identify event 2 as another attempt to deliver a trojan, since it has already been classified during event 1.

MISP Sharing

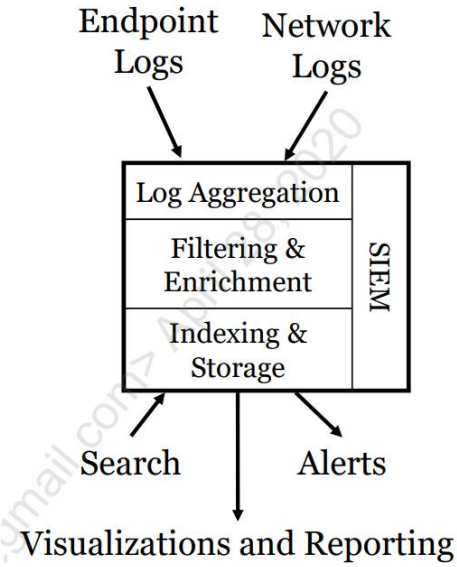


Each organization that runs their own instance of MISP can designate which events they are willing to share, and link their copy of MISP up with others, allowing bidirectional sharing of events across multiple organizations.

6. SIEM and Automation

SIEM duties:

- Receive all log data
- Parse it correctly
- Filter unwanted events
- Enrich useful events with additional data
- Index log into database
- Fast searching
- Visualization and dashboard creation
- Analytics and correlation for alerting



❖ the input to the system is logs, and the output of the SIEM is visualizations, alerts, reports and search results.

SIEM Features:

- High-performance logging agent for data collection
- Multi-format log compatibility
- High performance ingestion and indexing

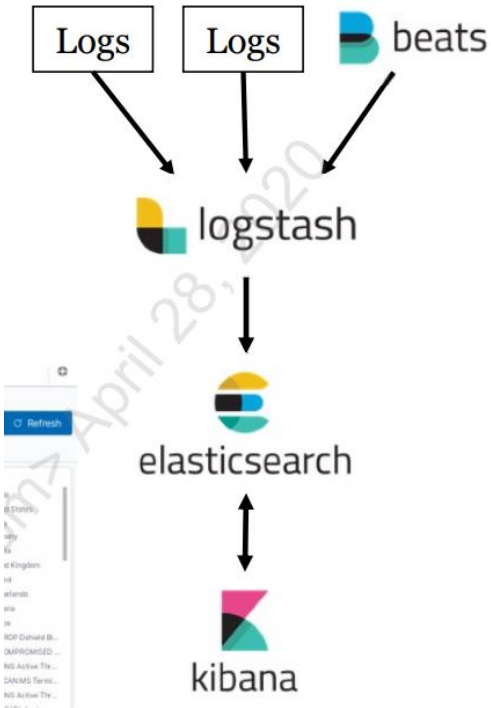
- Multiple types of log enrichment
- Fast search with easy query language
- Multiple visualization types
- Well thought out UI
- Flexible and expressive alerting options

SIEM Products:

- Splunk
- QRadar
- Elasticsearch
- Solarwinds
- logRhythm

Elastic Stack

- Logs ingested through Logstash
- Stored in Elasticsearch database
- Searched and visualized in Kibana



- ❖ Logstash takes the logs and parses, filters, and enriches them with additional information before sending them on to Elasticsearch to be stored.
- ❖ Elasticsearch stores every log as a JSON formatted.
- ❖ Kibana is the frontend web-based search interface we will use to query the logs stored in Elasticsearch.
- ❖ You will not need to configure or interact with Beats, Logstash, or Elasticsearch directly , only Kibana.

Kibana Query Language Examples:

open search for "string"

- string

response field containing "string"

- response:string

destination_port field above 1024

- destination_port > 1024

Searching for multiple matches

- response:string and destination_port:80

Searching for one of two things

- response:string or destination_port:80
- response:(200 or 404)

SIEM Use Cases : The way the Blue Team defines what they want the SIEM (and other tools) to do is the "use case." All Blue Teams have analytics like "if a failed login occurs 10+ times, send us an alert"

Creating a New Use Case

- What is the situation we're trying to identify
- Define the conditions to detect it
- Write logic, analytic, and expected outputs
- TEST IT to ensure it functions as expected
  Ideally, automate periodic testing
- Document details in use case database

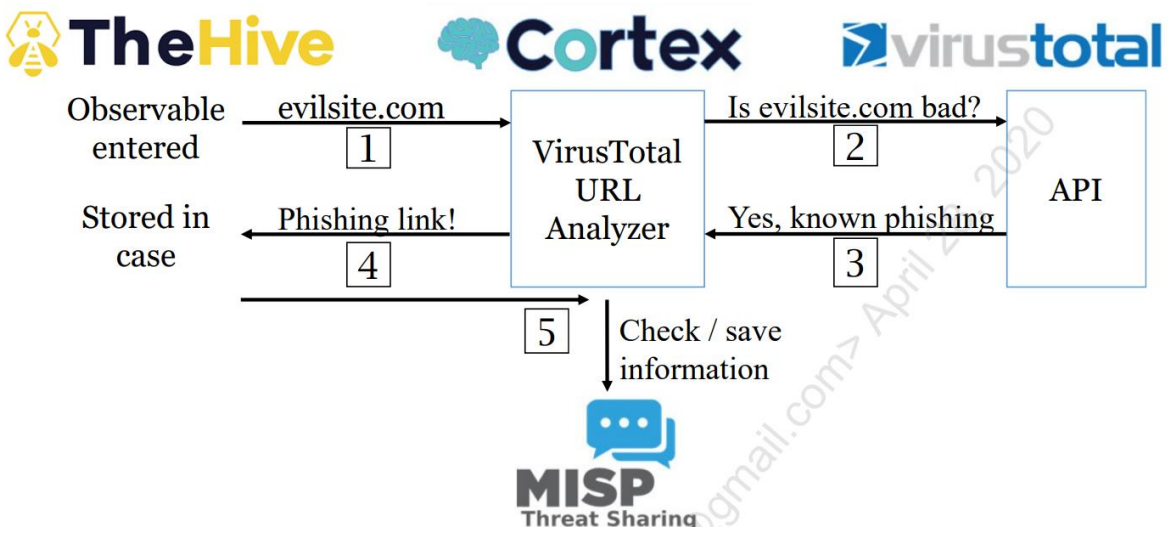
Automation and Orchestration Definition

- **Automation** accomplishes a specific task automatically through a software instead of doing it manually.
- **Orchestration** is taking the tasks that have been automated and deploying them in a series of events.

❖ **SOAR** takes all the painful, non-value-added parts of the job people don't like doing and makes it fast and easy.
❖ **Cortex** is a SOAR platform.
❖ **Cortex** is a separate program bundled with TheHive that is meant to work closely with it to perform automated lookups and other enrichment actions.

- **Analysers** reduce repetitive enrichment actions for indicators
  - ➢ VirusTotal, Passive DNS lookups, etc.
- **Responders** provide automated response actions
  - ➢ New functionality more directly aimed at SOAR

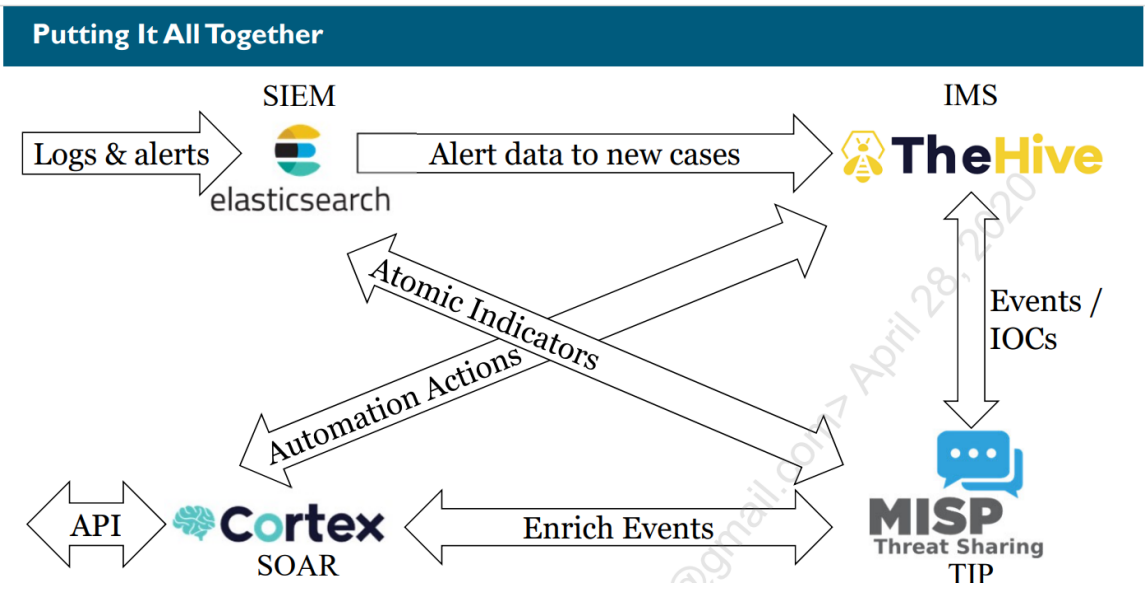
Cortex Automated Analysis



Here's an example of how data can flow when a new "observable" is entered into Cortex.

- First, the domain 'evilsite.com' is entered into TheHive as a new observable, and the analyst is asked if they want to run any analyzers on it.
- The analyst can select a VirusTotal lookup, which will pass the domain name to Cortex and will, in turn, use the VirusTotal API to programmatically get the answer.
- The results are then pulled back into the case in TheHive for context.

❖ Without Cortex, the analyst would have had to manually go to VirusTotal, copy and paste the information to do the look, type the returned results, and manually generate an event in MISP to track the indicators.



7. Know Your Enemy

❖ To put up a strong defense, we must understand our enemy.

Who's Attacking Us? Hackers-For-Hire and Insiders

Hackers-for-Hire

- Outsourcing hacking to others
- Ransomware-as-a-service
- Exploit-as-a-service

Malicious Insiders

- Making money
- Stealing intellectual property
- Hurting organization reputation

Opportunistic Attackers vs. Targeted Attackers

1. **Opportunistic Attackers**
- **Adversary Goal:** untargeted compromise.
- **Strategy:** Collect infected computers, control as botnet, use them for financial gain.

2. **Targeted attackers**
- **Goal:** Target people/organizations, get specific info, access specific systems, or disrupt YOUR business.
- **Strategy:** Attacks tailored to you and your organization.