

SOC Foundation

Gianluca Peco
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova

SOC

People X technology (automation) ~K

- Ente di media grandezza (10k utenti) 16x5 SOC (8x5x2 turni):
 - No automation: 8 FTE (analisti) + 2FTE (coordinatori)
 - SIEM (Security Information Event Mangement) gestito da 4 + 0.5 FTE
- Tecnologie da implementare:
 - Centralizzazione dei log ed eventi di sicurezza
 - Integrazione con threat intelligence, vulnerabilità. OSINT, EDR, ...
 - Prioritizzazione eventi
 - Connessione con asset management, vulnerability management, intrusion prevention, firewall, trouble ticketing, ...
 - Automazione risposte a eventi predefiniti

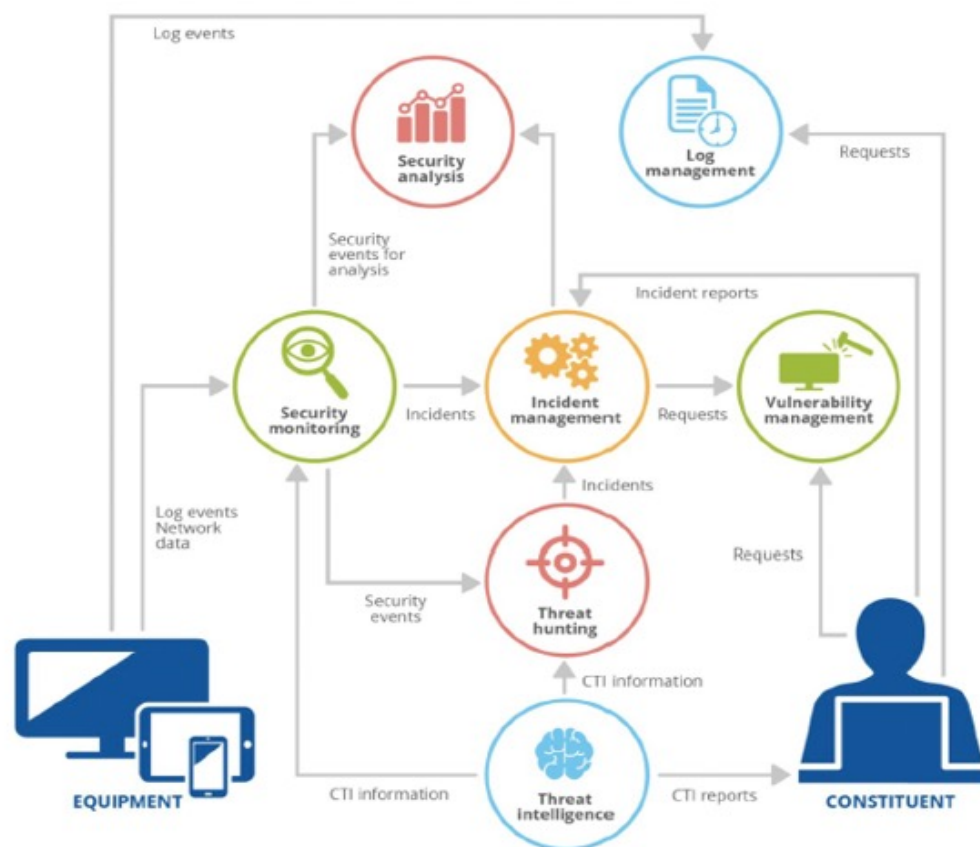
Dall'introduzione di Luca

SOC Foundation

- Per tentare di approfondire gli ultimi punti sarò tedioso e prolisso
- Sicuramente impreciso, ma il tentativo andava fatto !
- Le slide saranno fitte, ve le leggete a casa (doc like)
- Cos'è un SOC e cosa deve fare di preciso ?
- Quali strumenti utilizza ?
- Quali dati analizza ?

CSIRT Design Examples

service/processes interrelationship



Process name	Security incident management
Description	Security incident management covers incident report registration, triage, incident resolving and incident closing
Process owner	Security incident manager
Purpose	To ensure that every incident detected is handled according to defined quality requirements and that response activities are carried out to mitigate any incidents, followed by actions to improve security measures; and to increase the maturity of the constituent's security processes so that it is more resilient to cyberthreats in the future
Service input/triggers	<ol style="list-style-type: none"> Events detected by security monitoring service activities Incident reports registered by: <ol style="list-style-type: none"> 2.1. Phone 2.2. E-mail 2.3. Online web form 2.4. Service desk self-service interface
Service output/deliverables	<ol style="list-style-type: none"> Assistance to constituents to mitigate security incidents Provision of guidelines for improving the security of the constituent's infrastructure
Service activities	<ol style="list-style-type: none"> Triage of the security incident Analysis of the security incident Guide the containment of the security incident Guide eradication and recovery after the incident Close the incident Lessons learned

incident management
process workflow
description and
diagram

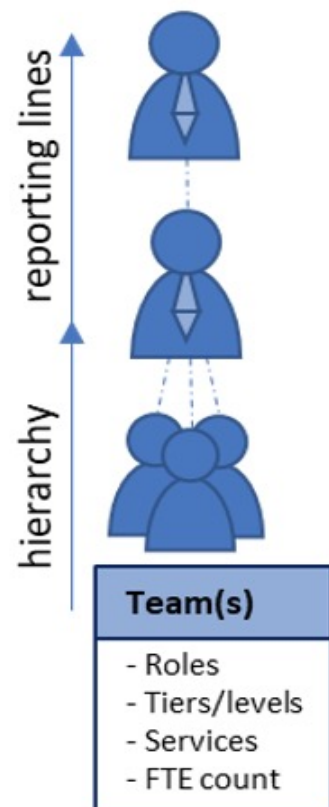


SOC Management

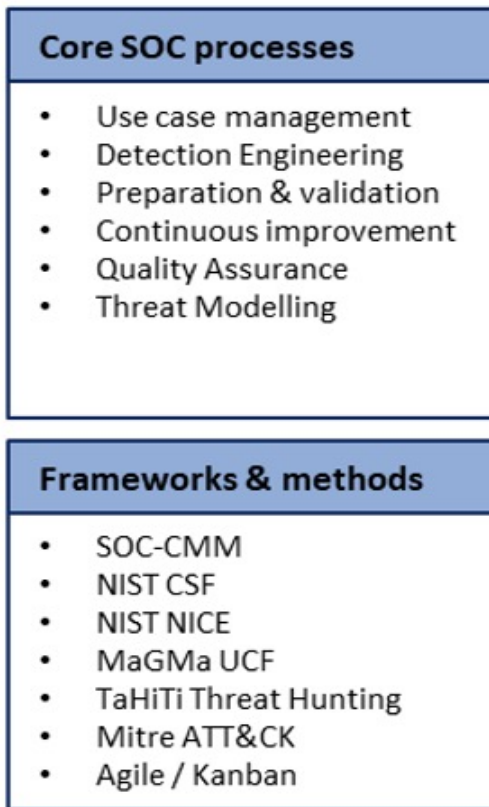
SOC Operations

SOC Governance

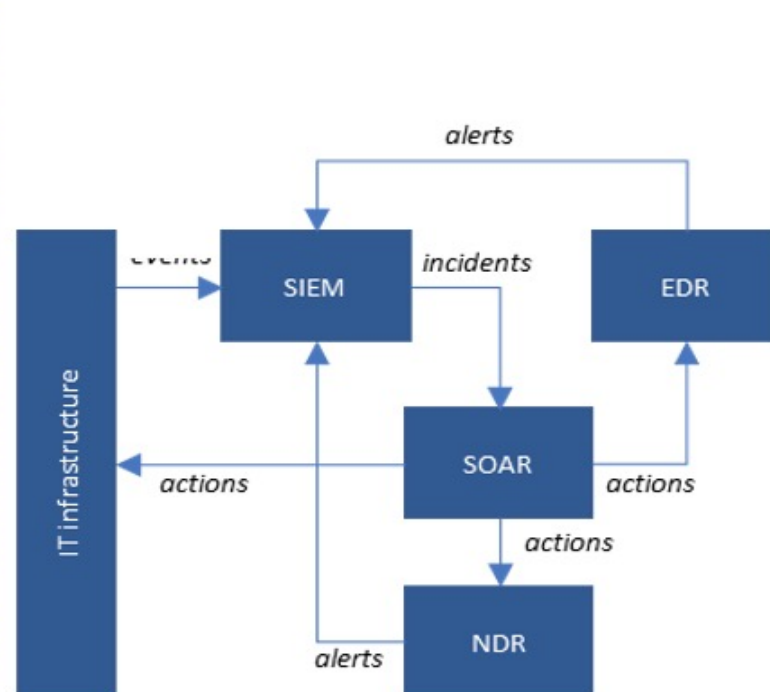
PEOPLE



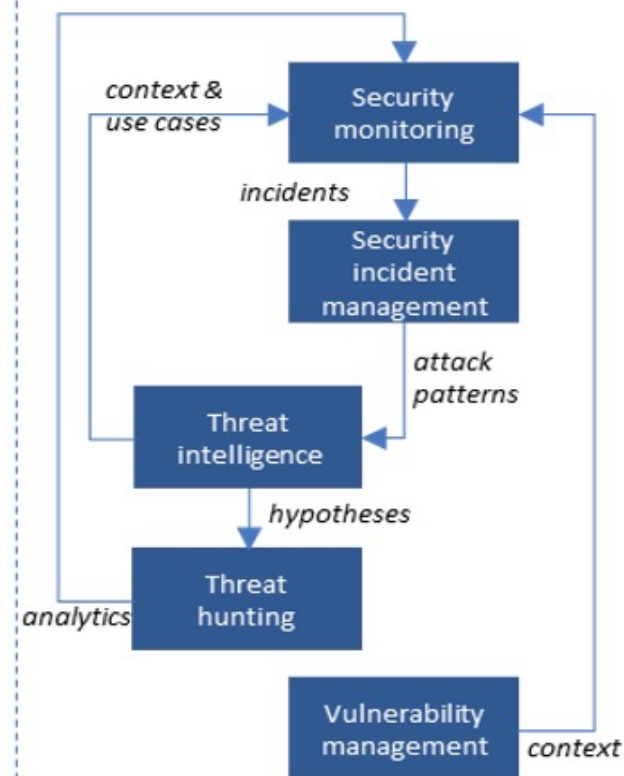
PROCESS



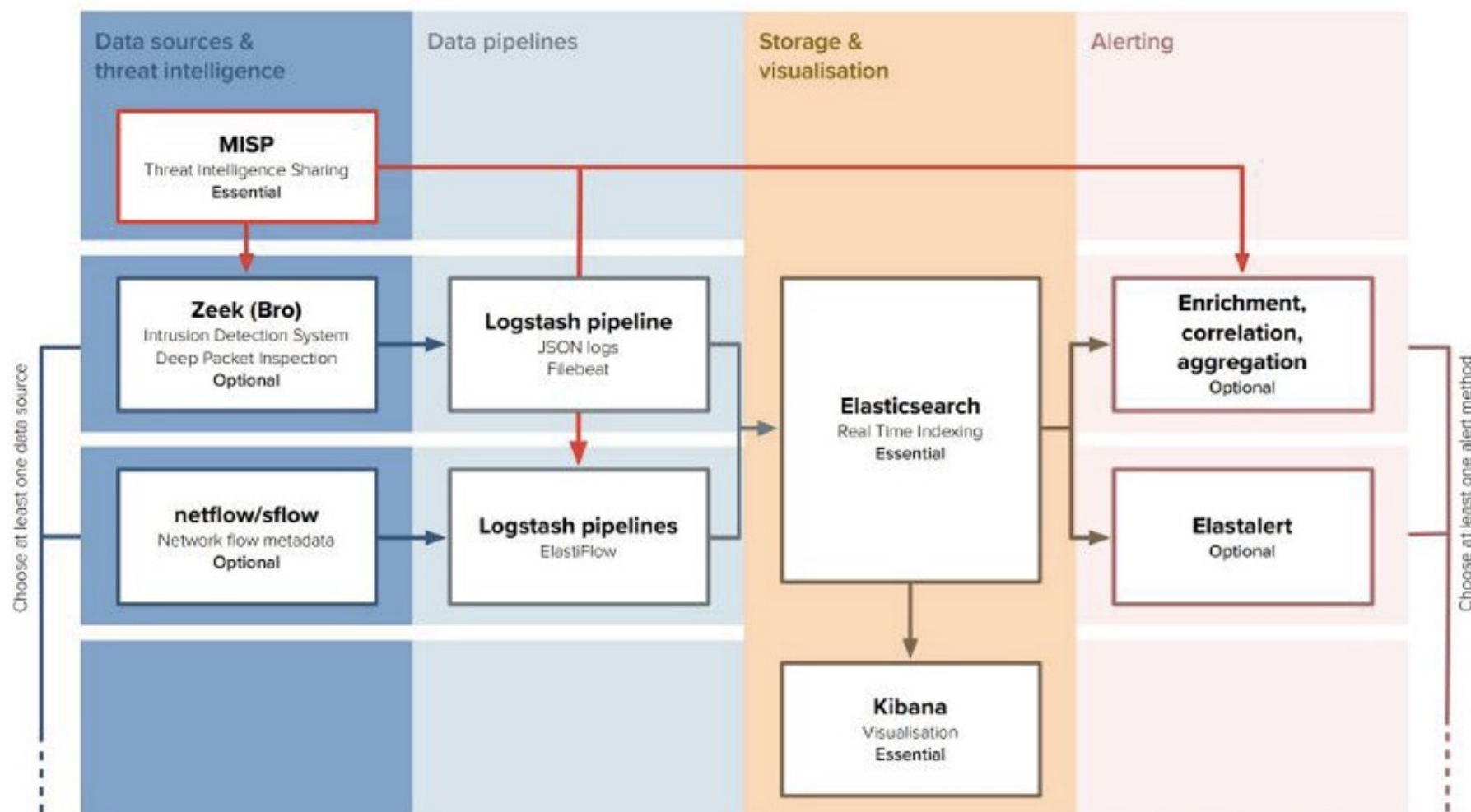
TECHNOLOGY



SERVICES

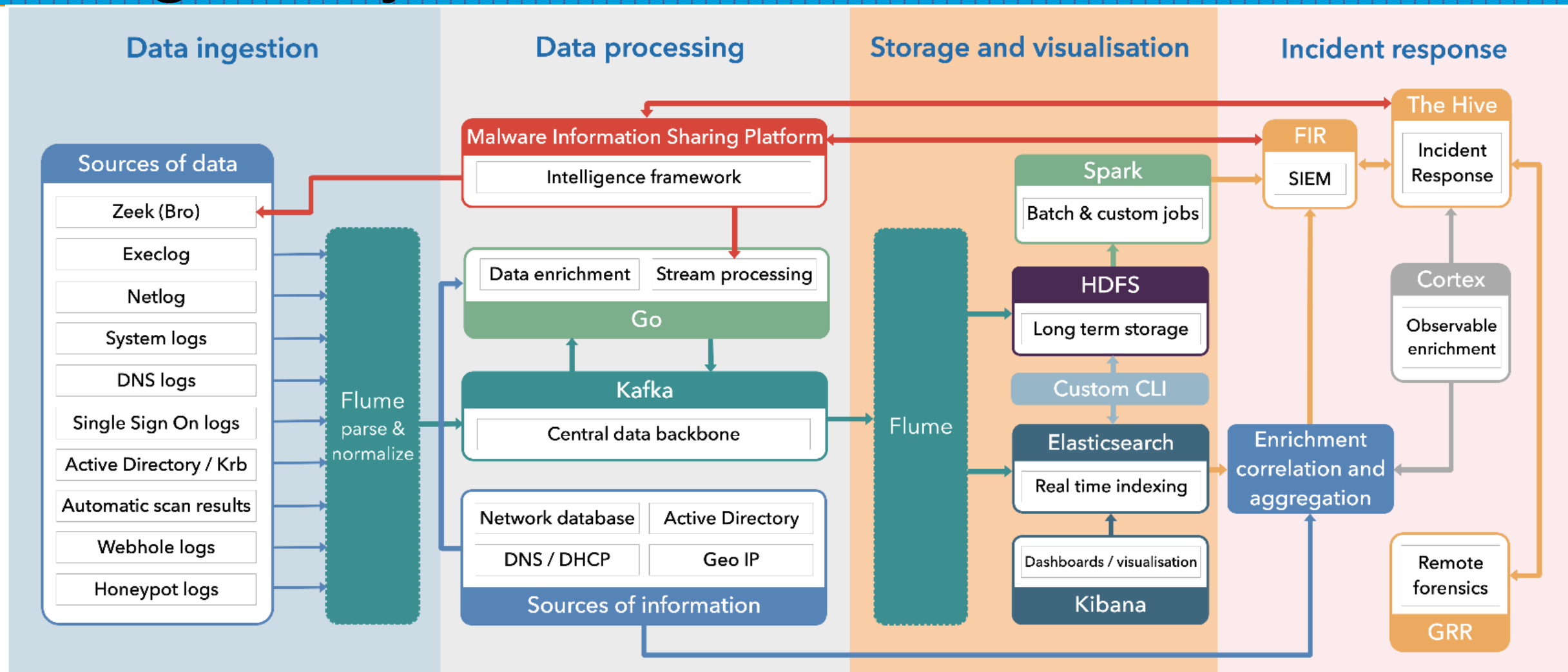


WLCG SOC WG Reference Model



D Crooks, et al. DOI 10.22323/1.351.0010

Log Analysis Platform Reference Model



Cos'è un SOC

- Un SOC è un team, composto principalmente da specialisti in sicurezza informatica, organizzato per prevenire, rilevare, analizzare, rispondere e segnalare incidenti di sicurezza informatica
- Fornire alla comunità un mezzo per segnalare sospetti incidenti di sicurezza informatica
- Fornire assistenza per la gestione degli incidenti
- Diffondere informazioni relative agli incidenti alla comunità e alle parti esterne

Cos'è un SOC

Un tipico SOC di medie dimensioni include in genere i seguenti compiti:

Prevenire gli incidenti di sicurezza informatica attraverso misure proattive, tra cui:

- **Analisi continua delle minacce**
- Analisi delle vulnerabilità
- Implementazione di contromisure coordinate
- Consulenza sulla politica e l'architettura della sicurezza

Monitoraggio, rilevamento e analisi di potenziali intrusioni in tempo reale e attraverso la caccia degli avversari, utilizzando una varietà di fonti di dati rilevanti per la sicurezza (Threat Hunting, Threat Intelligence)

Rispondere agli incidenti confermati, coordinando le risorse e indirizzando l'implementazione di contromisure tempestive e appropriate

Fornire consapevolezza situazionale e reporting sullo stato della sicurezza informatica, sugli incidenti e sulle tendenze nel comportamento degli avversari

Implementare tecnologie appropriate come sensori host, sensori di rete, raccolta dei log e sistemi di analisi

Cosa non è un SOC

Un NOC o un centro operativo IT perché un SOC è principalmente alla ricerca di attacchi informatici, mentre un NOC (e in genere altro personale IT) si occupa di operare e mantenere la rete e altri dispositivi IT

Un Chief Information Officer (CIO) o Chief Information Security Officer (CISO) perché il SOC è una capacità operativa in tempo reale e **i suoi sforzi di monitoraggio non sono solitamente focalizzati su altre aree della sicurezza informatica come la politica e la governance**, la gestione del rischio o l'ingegneria di sistemi sicuri (sebbene alcuni SOC riferiscano direttamente a un CISO o CIO).

Un programma di monitoraggio continuo della sicurezza delle informazioni (ISCM) perché il SOC è responsabile del rilevamento e della risposta agli incidenti, mentre l'ISCM è generalmente focalizzato sulla conformità alla sicurezza e sulla misurazione del rischio

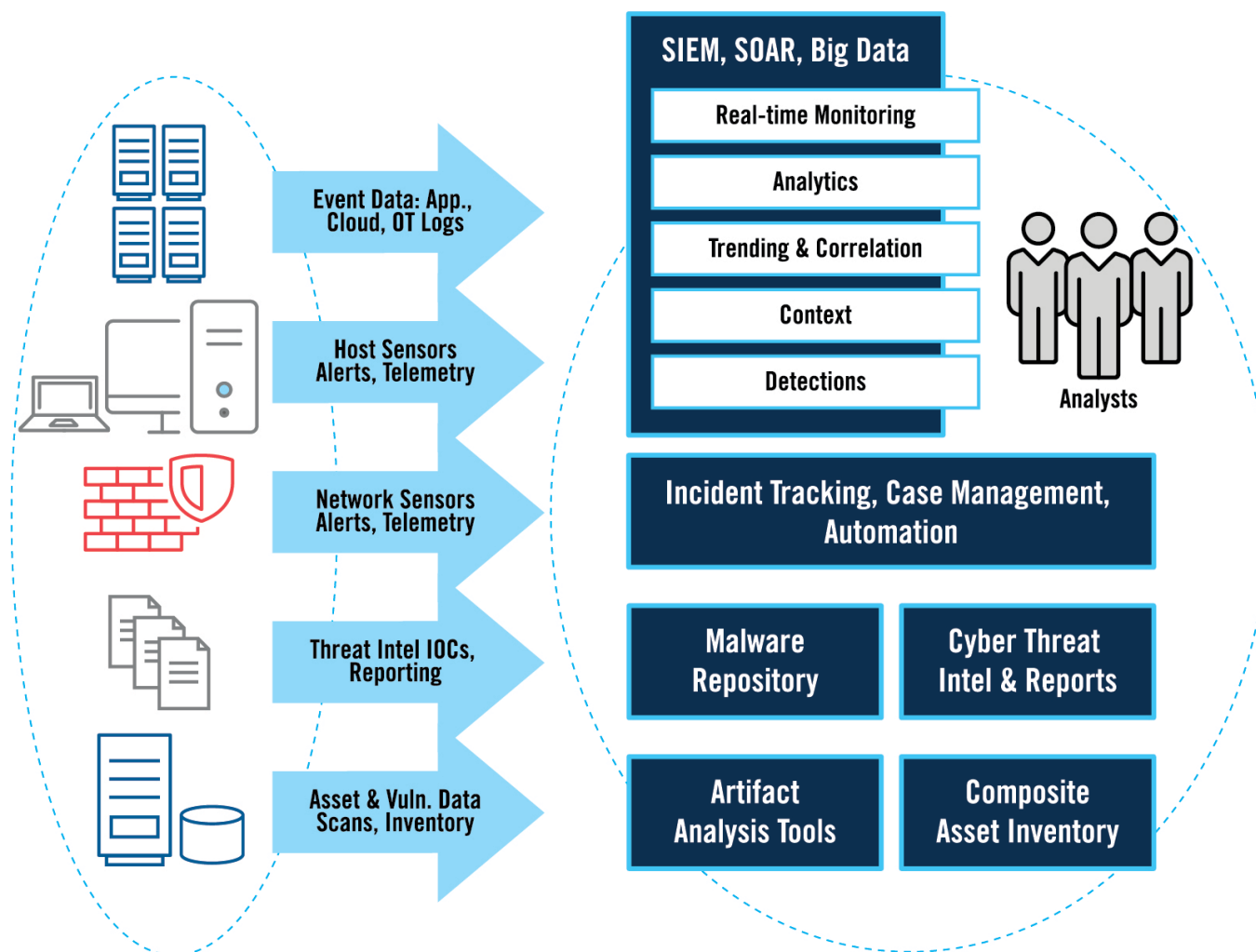
Un'organizzazione ISSO (Information Systems Security Officer) o Information Systems Security Manager (ISSM) (ad esempio nel governo) perché il SOC è responsabile del monitoraggio e della risposta alla minaccia informatica di portata in tutta la circoscrizione, mentre gli ISSO sono spesso più focalizzati sulla conformità IT e sulla garanzia della sicurezza di sistemi specifici.

Monitoraggio della sicurezza fisica (ad esempio, "cancelli, varchi, guardiania, etc") perché un SOC si occupa del dominio cibernetico, mentre il monitoraggio della sicurezza fisica si occupa principalmente di proteggere le risorse fisiche e garantire la sicurezza del personale.

Applicazione della legge perché i SOC raramente detengono autorità investigative legali. Mentre i SOC possono trovare intrusioni che si traducono in azioni legali, il loro compito principale di solito non è la raccolta, l'analisi e la presentazione di prove che verranno utilizzate nei procedimenti legali.

Cosa fa un SOC

- SOC's must be able to collect and understand the right **data** at the right **time** in the right **context**
- Virtually every mature SOC employs several different technologies, along with automation processes, to generate, collect, enrich, analyze, store, and present tremendous amounts of security-relevant data to SOC members
- Among the data sources a SOC is likely to ingest, the most prominent are host sensors such as endpoint detection and response (EDR) capabilities, network traffic metadata, and various log sources such as application or operating system (OS) logs from on-prem devices, the cloud, or OT
- These sensors are placed on either the host or network, or cloud to detect potentially malicious or unwanted activity that warrants further attention by a SOC analyst
- Combined with security audit logs and other data feeds, this data will then be sent to a variety of systems within the SOC such as security information and event management (SIEM) or security orchestration, automation, and response (SOAR) technologies or specialized capabilities for performing functions such as malware analysis



Definizioni – Events/Alerts

Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Events do not necessarily indicate good or bad behavior, they simply are things that happened

An event is “any observable occurrence in a system and/or network”

In contrast, the term **Alert** is typically used to reference an event that generated with the implication it may be a potential attack. Intrusion detection systems (IDS) and SIEM systems are typical generators of alerts

An alert is a technical notification that a particular event, or series of events, has occurred

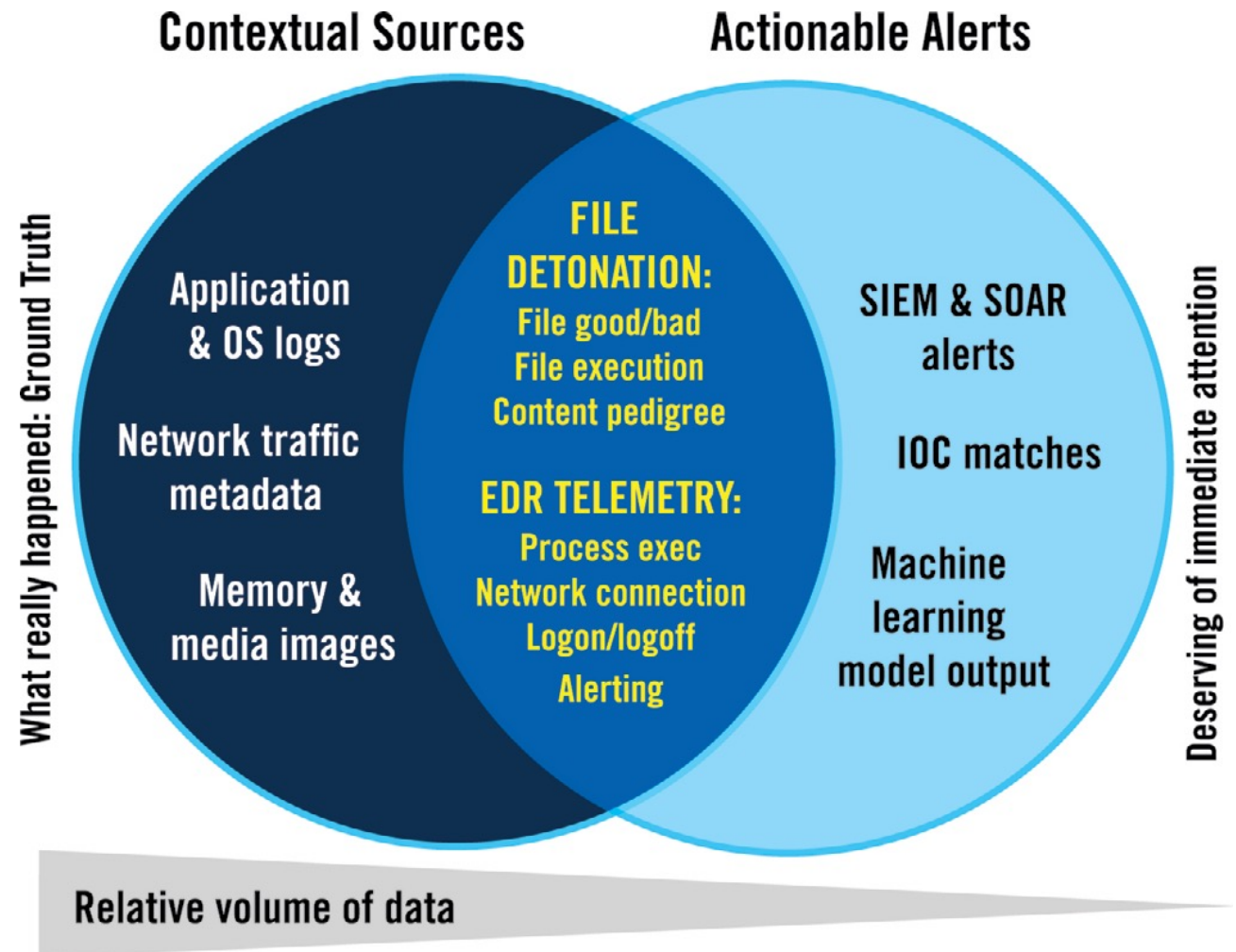
Definizioni – Signature/Anomaly

- Alerts will often come in two forms, signature-based and anomaly detections
 - Signature-based detection is where *the system has prior knowledge of how to characterize and therefore detect malicious behavior*, such as with an Indicator Of Compromise (IOC) matching
 - IOCs are forensic artifacts from intrusions that are identified on constituency systems at the host or network level.
 - Anomaly detection is where the system characterizes normal or benign behavior and *alerts whenever it observes something that falls outside the scope of that behavior*
 - Anomaly detections are based on discrete pieces of information, such as IP addresses, hashes/checksums, malware characteristics, URL, DNS probe

Definizioni - Contextualization

Without supporting context,
the alert is worth little

***No matter how severe it
may seem, a single alert
generally does not
provide sufficient
evidence that an incident
occurred***



Basic SOC workflow

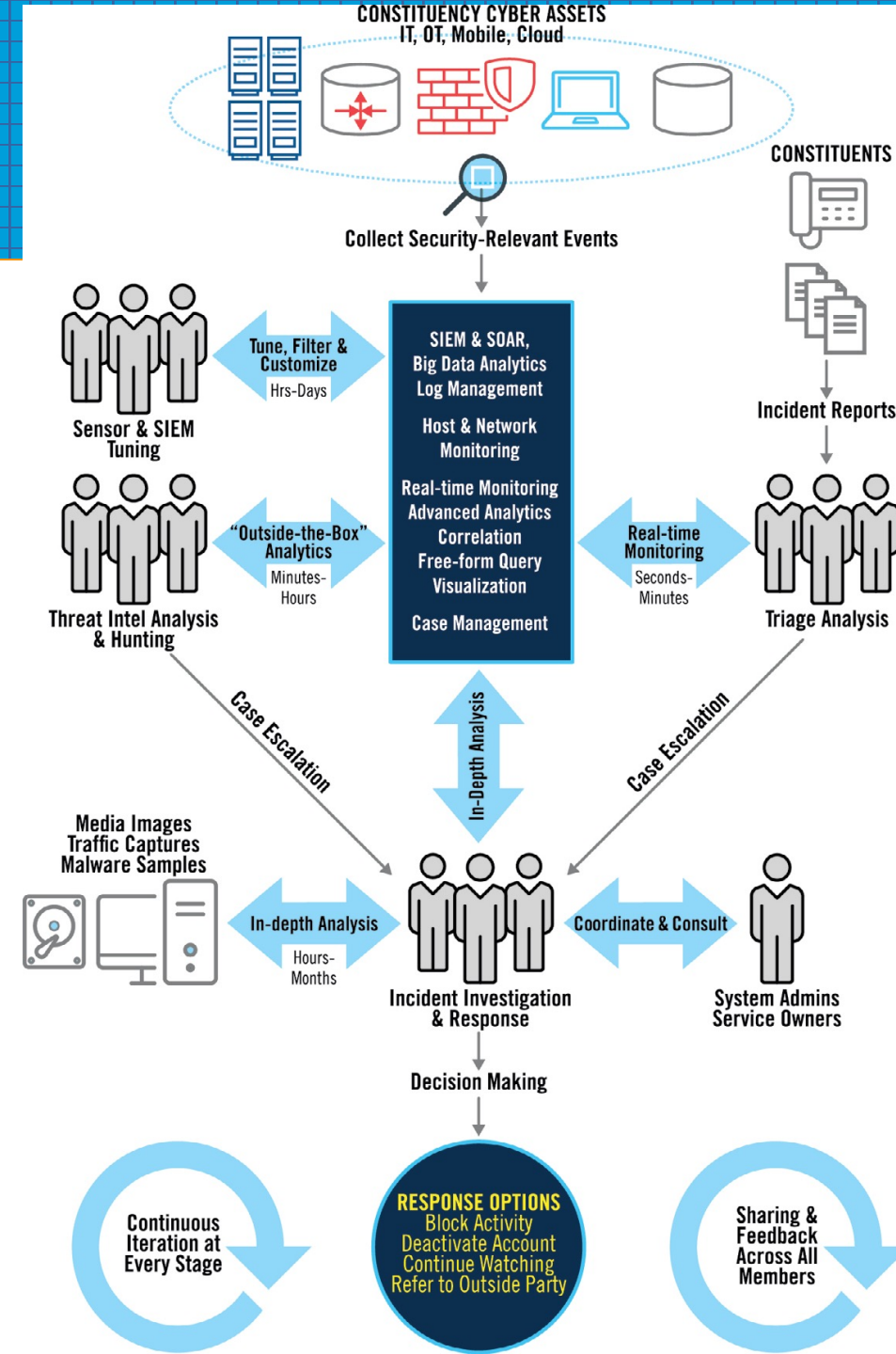
Many sources of information coming into the SOC including

- security-relevant events from constituency assets
- information from constituents themselves
- cyber threat intelligence

These inputs are filtered and assessed by both humans and machines with the goal of being able

- to take a response action
- or deciding that no action is needed

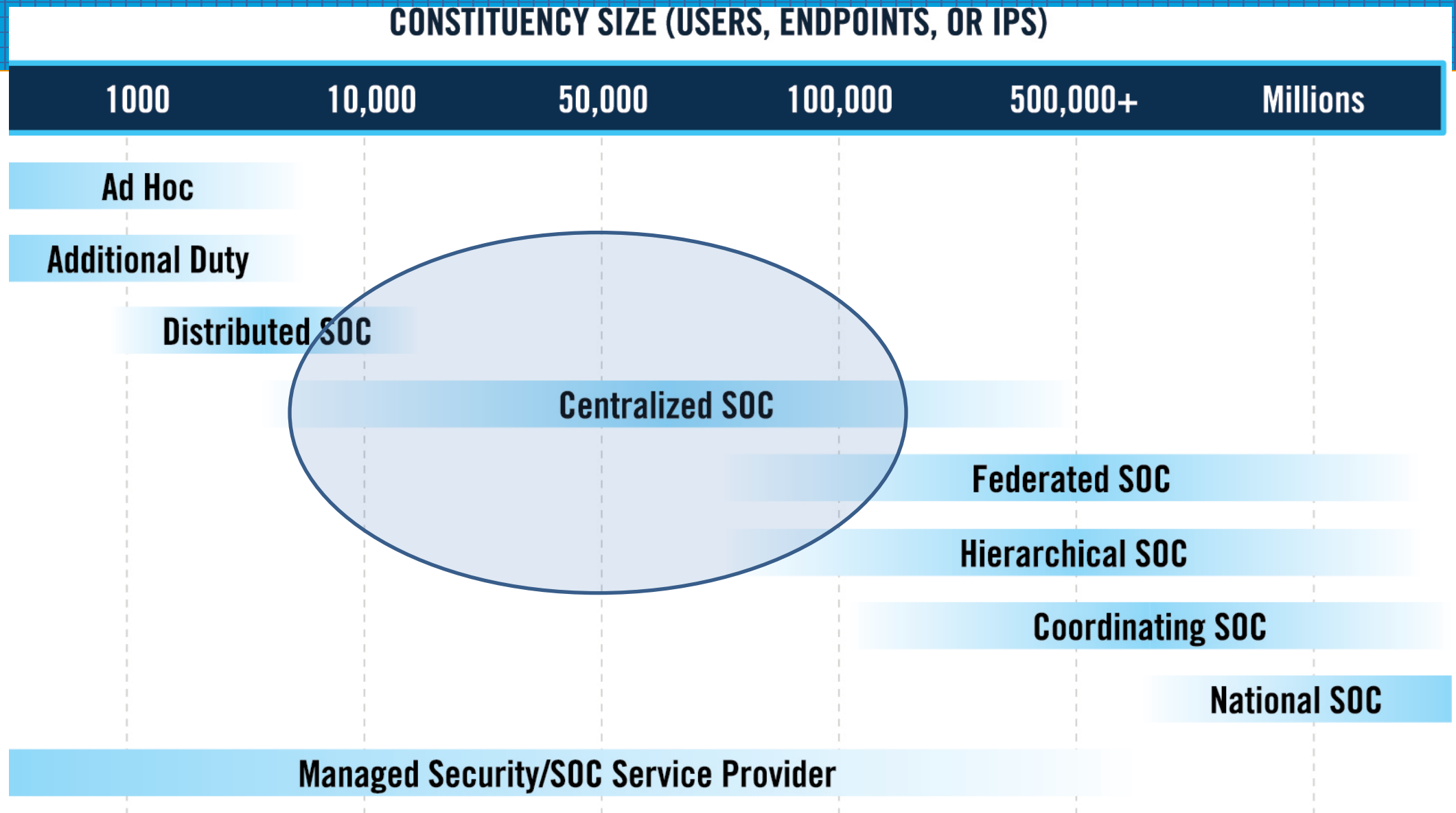
Throughout the process the SOC will coordinate and consult with many others such as system administrator and service owners to ensure that any response actions taken are done in the context of the business environment the SOC supports



SOC Organizational Models

Organizational Model	Example Organizations	Remarks
Ad Hoc Security Response	Small Businesses	No standing incident detection or response capability exists. In the event of a computer security incident, resources are gathered (usually from within the constituency) to deal with the problem, reconstitute systems, and then stand down. Results can vary widely as there is no central watch or consistent pool of expertise, and processes for incident handling are usually inadequately defined.
Security as Additional Duty	Small businesses, small colleges, or local governments	No formal SOC organization. However, SOC-like duties are part of other duties. For example, a system administrator that also looks for unusual activity in system logs. Some procedures for incident response may exist.
Distributed SOC	Small to medium-sized businesses, small to medium colleges, and local governments	Formal SOC authorities. Comprised of a decentralized pool of resources housed in various parts of the constituency. Staff may have other duties as well.
Centralized SOC	Wide range of organizations including medium to large-sized businesses, educational institutions (such as a university), or state/ province/federal government agencies	Resources for security operations are consolidated under one authority and organization. SOC personnel have dedicated roles in the SOC. The most frequent operating model, and the simplest way to think about how most SOC's operate.
Federated SOC	Organizations with distinct operating units that function independently of one another such as businesses that have acquired other businesses but have not integrated them together	A SOC, likely centralized but could also be hierarchical, that shares a parent organization with one or more other SOC's, but generally operates independently. It may have some shared policies and authorities.
Coordinating SOC	Large businesses or government institutions	A SOC responsible for coordinating the activities of other SOC's underneath it. Focuses primarily on SA and overall incident management. Does not direct the day-to-day operations of the SOC's it coordinates.
Hierarchical SOC	Large businesses or government institutions	Similar to the Coordinating SOC structure; however, the parent organization plays a more active role. The parent organization may offer SOC services to lower-level SOC's and has greater responsibility for coordinating a wider range of SOC functions (such as engineering, CTI, malware analysis, etc.)

Model vs Size



SOC Organizational Models

By placing all SOC services within **one centralized organizational structure**, the SOC gains many benefits when compared to ad-hoc or distributed organizational models, including:

- **Dedication of resources and focus:** Security operations for the centralized SOC is what they do, and not treated as an additional duty or distraction
- **Ownership and shared identity:** The team comes together with a shared sense of mission and purpose
- **Centralized visibility and management of incidents:** Synchronize elements of security operations so all elements are working in concert toward the same goal, especially during a critical incident
- **Better collaboration and unity of effort and integration among SOC service elements:** There will be fewer organizational barriers to working together
- **Potential for cost savings and economy of force:** A centralized model can reduce duplication of effort and maximize the use of technologies
- **Stronger SOC authority:** Limits the likelihood an external organization will take it upon themselves to perform SOC like functions, which reduces the potential for conflict or disorganization during a response
- **Staff growth:** Allows the SOC to build its own staff over time by having more opportunities for growth and advancement
- **Self-reinforcing progress toward maturity and effectiveness:** With the elements of the SOC working toward the same goal, as one, generally they progress much faster toward greater capability than a distributed or decentralized capability
- **Unambiguous area of responsibility and mission:** The SOC is responsible for a given set of organizations, assets, and networks (the constituency); the lines between who are responsible for what should be clear and not subject to controversy

This is not to say that ad-hoc or distributed SOC functions might not be the right choice for very small constituencies with limited security risks or resources. However, at a certain point, bringing together SOC resources into one organization likely makes the most sense.

Differences in Roles for Hierarchical SOCs

RESPONSIBILITY	CENTRAL SOC ROLE	SUBORDINATE SOC ROLE
Real-time Alert Monitoring and Triage	Across constituency assets not covered by subordinates, such as Internet gateways or constituency-wide services such as email	Within assigned constituency
Incident Analysis and Response	Cross-constituency coordination, operational direction. Receives summary information and incident reports from subordinates; analysis and retention of data from assets not covered by subordinates, such as Internet gateways. May provide fly-away incident response support during significant incidents.	Intra-constituency response. Analysis and retention of own data, augmented with data from other organizations
Cyber Threat Intelligence	Strategic across enterprise, reporting to subordinates, trending of adversary TTPs	Tactical within constituency, consumer of central threat analysis, focused on supporting SOC detections
Expanded SOC Operations	Maintain a cadre of SOC staff that can support hunting, malware analysis, red-teaming or other expanded operations that are not needed on a day-to-day basis by subordinate SOCs	Maintain a cadre of SOC staff for expanded operations if the subordinate SOC is of sufficient size or has more frequent needs for these functions
Situational Awareness and Communications	Strategic across entire enterprise and with external parties	Tactical within own constituency
Training	Coherent program for all analysts in constituency	Execution of general and specialized training for own SOC
Reports to	Constituency executives, external organizations	Own constituency executives, central SOC
Security Architecture, Engineering, and Administration	Enterprise architecture, enterprise licensing, and lead on tool deployment and refresh	Chooses monitoring placement, specialized capabilities when needed

SOC Organizational Models (1/3)

Instead of focusing on direct reporting of raw event feeds or promulgating detailed operational directives, the coordinating SOC may better achieve its goals by providing a unique set of capabilities that its subordinates usually cannot.

Performing strategic analysis on adversary TTPs: Coordinating SOC may have access to a larger set of finished incident reporting and therefore are uniquely positioned to focus on observing and trending the activity of key actors in the cyber realm

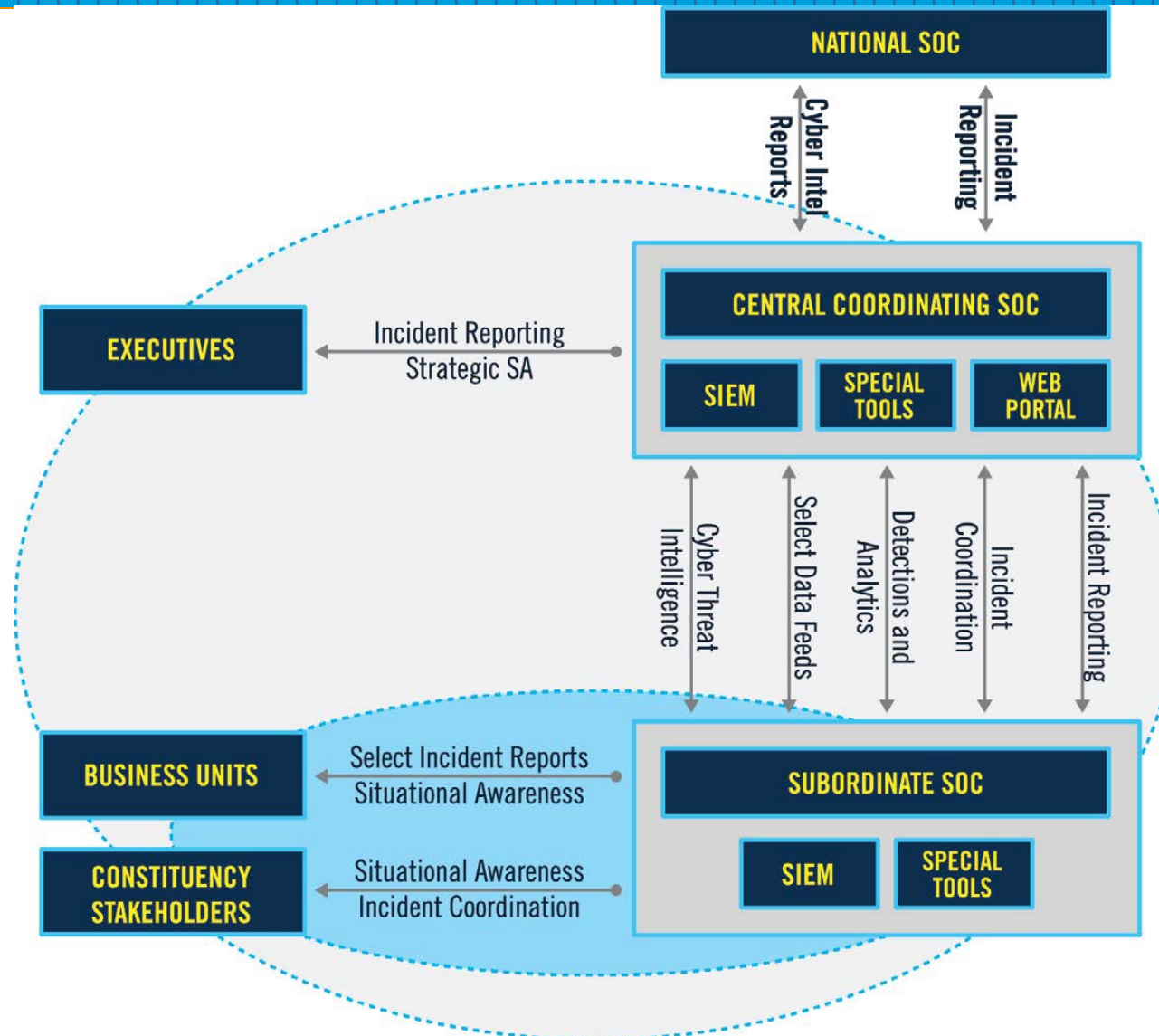
Providing a clearinghouse of tipplers, sensor signatures, ML models, and SIEM analytics that other SOC can leverage: A coordinating SOC could harvest indicators from human-readable cyber threat intelligence and provide it back out in both human and machine-readable form for ingest by subordinates' analysts and SIEM, respectively, such as through Structured Threat Information eXpression (STIX) /Trusted Automated eXchange of cyber threat Intelligence Information (TAXII). For this to work, however, CTI should be turned around in a timescale and with detail that is beneficial to its recipients. This will likely mean processing and redistributing CTI in timeframes of hours or perhaps a few days, and in so doing preserving as much original detail and adversary knowledge as possible.

Providing malware analysis, forensic services, and emergency incident response to constituent SOC: These areas either require advanced skills that hard to staff and maintain currency in or are only needed intermittently by any particular subordinate SOC. In this fashion, some coordinating SOC act in a capacity like an outsourcing MSSP. Malware services can include an automated Web-based malware detonation "drop box" or in-depth human analysis of media or hard-drive images.

SOC Organizational Models (2/3)

- **Aggregating and sharing SOC best practices, process documents, and technical guidance:** This can include enterprise guidance the coordinating SOC develops itself or best practices developed by subordinate SOCs that it helps propagate across the larger organization
- **Providing secure forums for collaboration between subordinate SOCs:** This may include collaboration hubs, persistent chat, message boards, and wikis.
- **Providing enterprise licensing on key SOC technologies:** This can include network and host monitoring tools like EDR, vulnerability scanners, network mapping tools, and SIEM, provided the following two conditions are met:
 - subordinates are not forced to use a specific product
 - there is enough demand from subordinates to warrant an enterprise license.
- **Providing SOC training services:**
 - On popular commercial and open-source tools such as SIEM and malware analysis
 - On the incident response process
 - On vulnerability assessment and penetration testing
 - Leveraging a virtual “cyber range” where analysts can take turns running offense and defense on an isolated network built for Red Team/Blue Team operations
 - Running SOC analysts through practice intrusion scenarios, using real tools to analyze realistic intrusion data

SOC Organizational Models (3/3)



Capability Template SOC Models

	Security As Additional Duty	Distributed SOC's Small/Young Centralized & Federated SOC's	Large/Mature Centralized & Federated SOC's	Hierarchical SOCs	Coordinating & National SOCs
Incident Triage, Analysis, and Response					
Real-Time Alert Monitoring and Triage	b	b	a	a	n
Incident Reporting Acceptance	b	b	a	a	a
Incident Analysis and Investigation	b	b	a	a	a
Containment, Eradication, and Recovery	b	b	a	a	a
Incident Coordination	b	b	a	a	a
Forensic Artifact Analysis	n	o	b	a	a
Malware Analysis	n	o	a	a	a
Fly-Away Incident Response	o	o	b	a	a
Cyber Threat Intelligence, Hunting, and Analytics					
Cyber Threat Intelligence Collection, Processing, and Fusion	o	b	a	a	o
Cyber Threat Intelligence Analysis and Production	n	o	b	a	a
Cyber Threat Intelligence Sharing and Distribution	n	o	b	a	a
Threat Hunting	o	o	a	a	o
Sensor and Analytics Tuning	b	b	a	a	o
Custom Analytics and Detection Creation	o	o	a	a	o
Data Science and Machine Learning	n	o	b	a	o
Expanded SOC Operations					
Attack Simulation and Assessments	n	o	b	a	a
Deception	n	n	o	o	o
Insider Threat	n	n	o	b	o

Basic (b): SOC's in this category typically offer this capability/service at a basic level of performance inside the SOC.

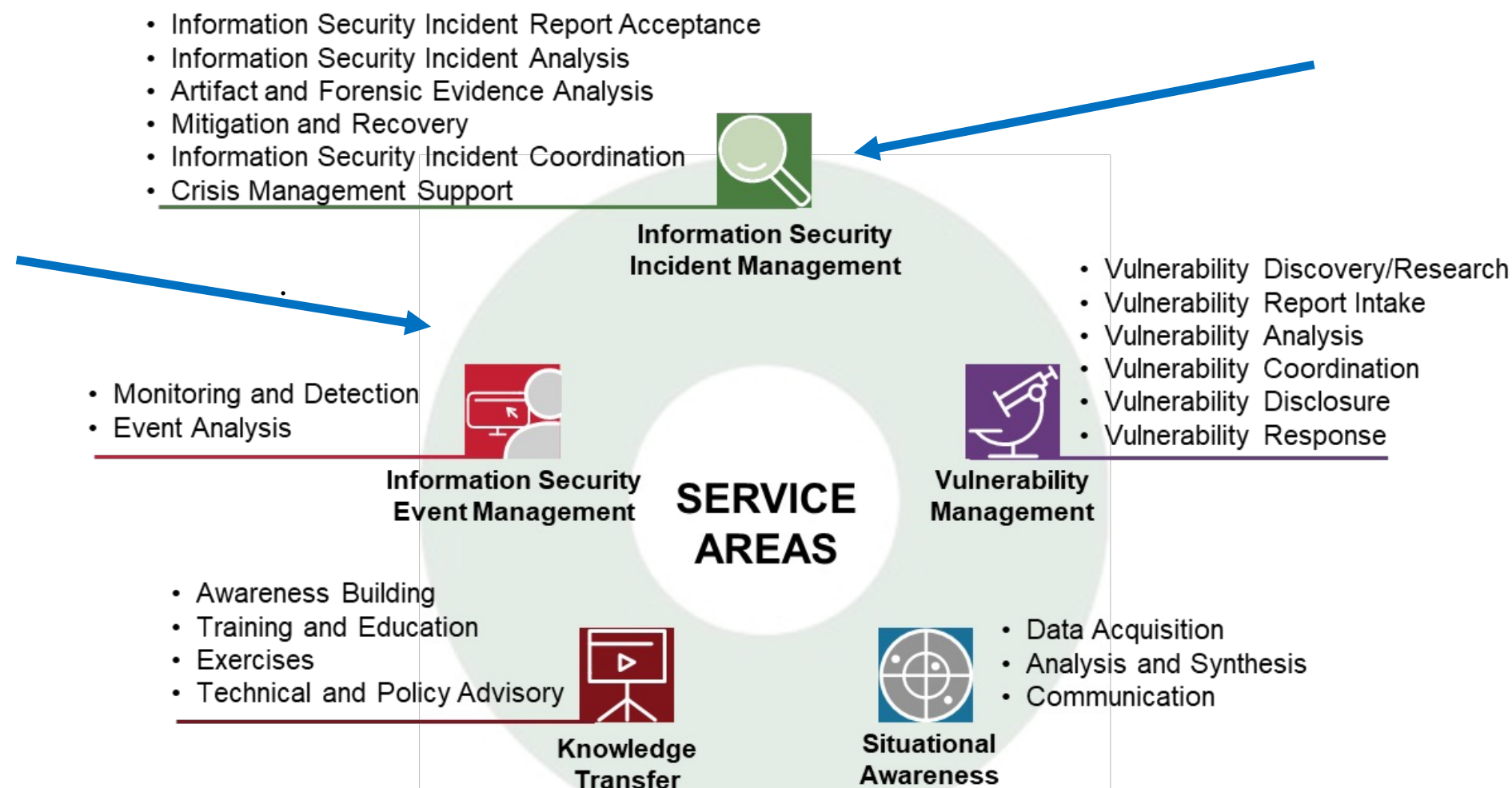
Advanced (a): SOC's in this category offer this capability/service at a more advanced, mature level of performance inside the SOC.

Optional (o): SOC's in this category may or may not offer this capability or function. Their choice to do so usually has more to do with their maturity, resourcing, focus, and external requirements than necessarily their organizational model.

Not recommended (n): SOC's in this category are unlikely to offer this capability or function in house. This is usually due to foundational capability and competency not being present, resources being limited, or scoping the focus to what is most appropriate for the organizational model type.

	Security As Additional Duty	Distributed SOC's Small/Young Centralized & Federated	Large/Mature Centralized & Federated SOC's	Hierarchical SOCs	Coordinating & National SOCs
Vulnerability Management (if performed by the SOC)					
Asset Mapping and Composite Inventory	b	b	a	a	o
Vulnerability Scanning	b	b	a	o	o
Vulnerability Assessment	n	o	b	a	b
Vulnerability Report Intake and Analysis	b	b	b	a	a
Vulnerability Research, Discovery, and Disclosure	n	n	o	b	a
Vulnerability Patching and Mitigation ⁴	b	o	o	n	n
SOC Tools, Architecture, and Engineering					
Sensing and SOC Enclave Architecture	o	b	a	a	o
Network Security Capability Engineering and Management	o	b	a	o	o
Endpoint Security Capability Engineering and Management	b	b	a	o	n
Cloud Security Capability Engineering and Management	o	b	a	a	n
Mobile Security Capability Engineering and Management	o	o	b	o	n
Operational Technology Security Capability Engineering and Management	o	o	o	o	n
Analytic Platform Engineering and Management	o	b	a	a	a
SOC Enclave Engineering and Management	o	b	a	a	a
Custom Capability Development	n	o	b	a	a
Situational Awareness, Communications, and Training					
Situational Awareness and Communications	b	b	a	a	a
Internal Training and Education	o	b	a	a	a
External Training and Education	o	o	o	o	a
Exercises	o	o	b	a	a
Leadership and Management					
SOC Operations Management	b	b	a	a	a
Strategy, Planning, and Process Improvement	o	b	a	a	a
Continuity of Operations	o	b	b	a	a
Metrics	o	b	a	a	a

Analizziamo I vari compiti utilizzando il modello Enisa/FIRTS



Information Security Event Management

Information Security Event Management aims to identify information security incidents based on the correlation and analysis of security events from by a wide variety of event and contextual data sources. In larger organizations, this service area is sometimes fully or partially assigned to a Security Operations Center (SOC), which might additionally also perform first or even second-level Information Security Incident Management such as initiating mitigations or adjustments of security controls. As any Information Security Incident Management service depends on qualified and accurate data about information security events, the interface between a SOC and the assigned CSIRT is crucial.

The following services are considered as offerings of this particular service area:

Monitoring and detection

- Log and sensor management
- Detection use case management
- Contextual data management

Event analysis

- Correlation
- Qualification

Information Security Incident Management (1/2)

This service area is at the heart of any CSIRT and consists of services that are vital in helping constituents during an attack or incident. CSIRTs must be prepared to help and support. Through this unique position and expertise, they are able to not only collect and evaluate information security incident reports, but also to analyze relevant data and perform detailed technical analysis of the incident itself and any artefacts used.

From this analysis, mitigation and steps to recover from the incident can be recommended, and constituents will be supported in applying the recommendations. This also requires a coordination effort with external entities such as peer CSIRTs or security experts, vendors, or PSIRTs to address all aspects and reduce the number of successful attacks later on.

- *Information security incident report acceptance*
 - *Information Security Incident Report Receipt*
 - *Information Security Incident Triage and Processing*
- *Information security incidents analysis*
 - *Information security incident triage (prioritization and categorization)*
 - *Information collection*
 - *Detailed analysis coordination*
 - *Information security incident root cause analysis*
 - *Cross-incident correlation*

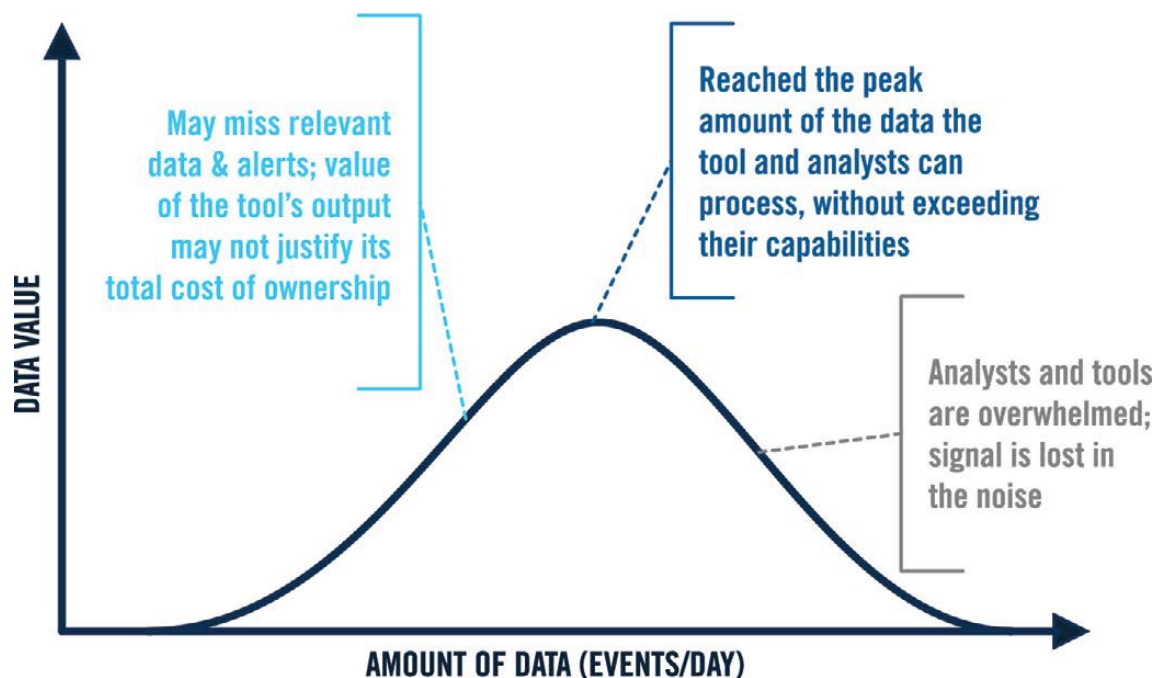
Information Security Incident Management (2/2)

- *Artefact and forensic evidence analysis*
 - *media or surface analysis*
 - *reverse engineering*
 - *runtime or dynamic analysis*
 - *comparative analysis*
- *Mitigation and recovery*
 - Response plan establishment
 - *Ad hoc measures and containment*
 - Systems restoration
 - Other information security entities support
- *Information security incident coordination*
 - Communication
 - Notification distribution
 - Relevant information distribution
- *Crisis management support*
 - *Information distribution to constituents*
 - Information security status reporting
 - Strategic decisions communication

Monitoring and detection (1/3)

One of the most frequent questions posed by SOC is, "What log and sensor data should we gather?"

Most importantly, the SOC needs to be deliberate in their planning, not just taking in any data they can, but selectively targeting the data that is most relevant and ensuring appropriate policies are in place to allow them to collect that data



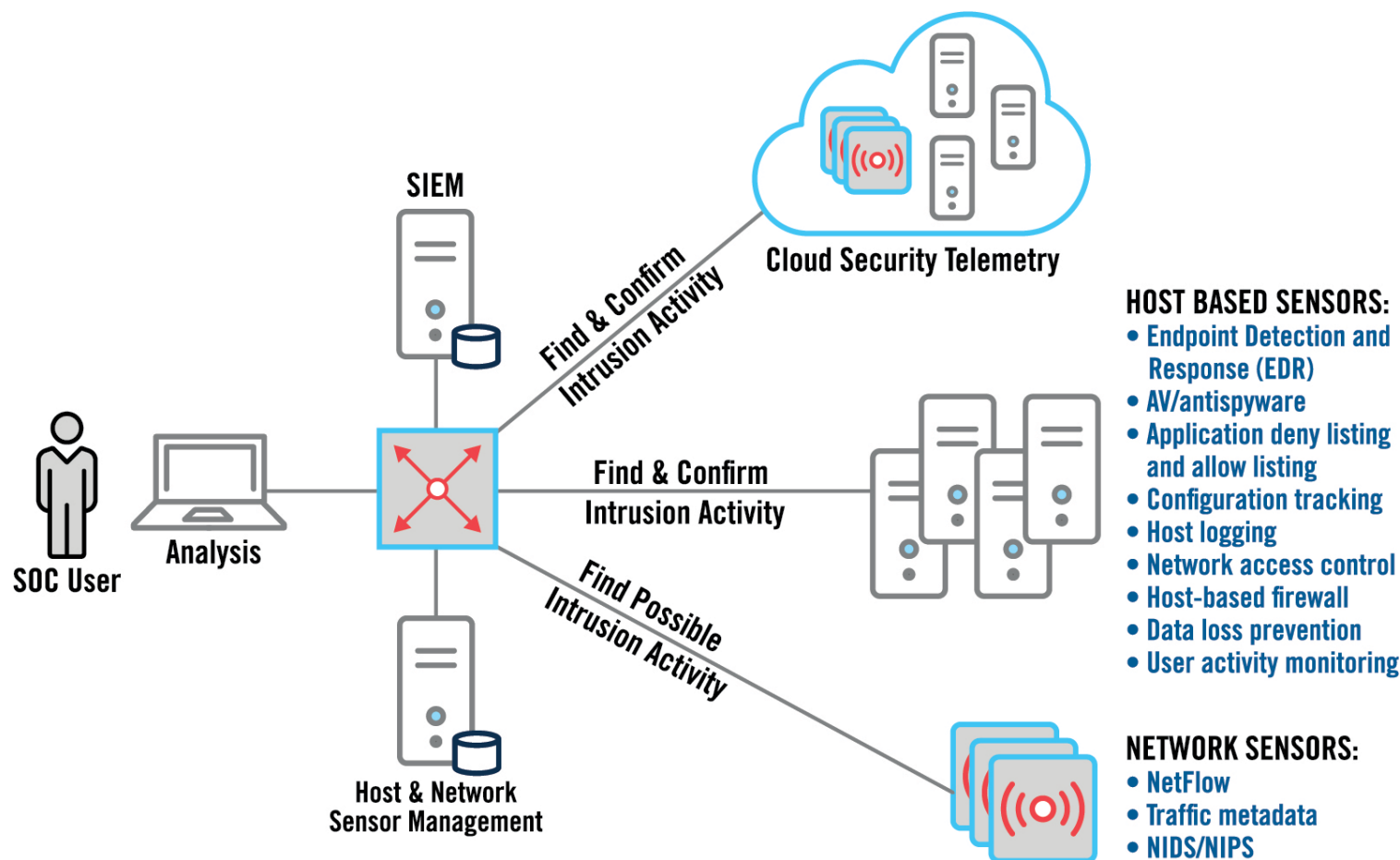
There are several drivers for collection of security-relevant telemetry, many of which overlap between the SOC and traditional IT operations.

- Defending networks, systems, cloud resources, and other digital assets
- Insider threat monitoring and audit collection
- Performance monitoring
- Maintenance troubleshooting and root-cause analysis
- Configuration management

When considering threat-based use cases, it is helpful to combine threat intelligence with the use of a threat framework, to guide collection choices !

Monitoring and detection (2/3)

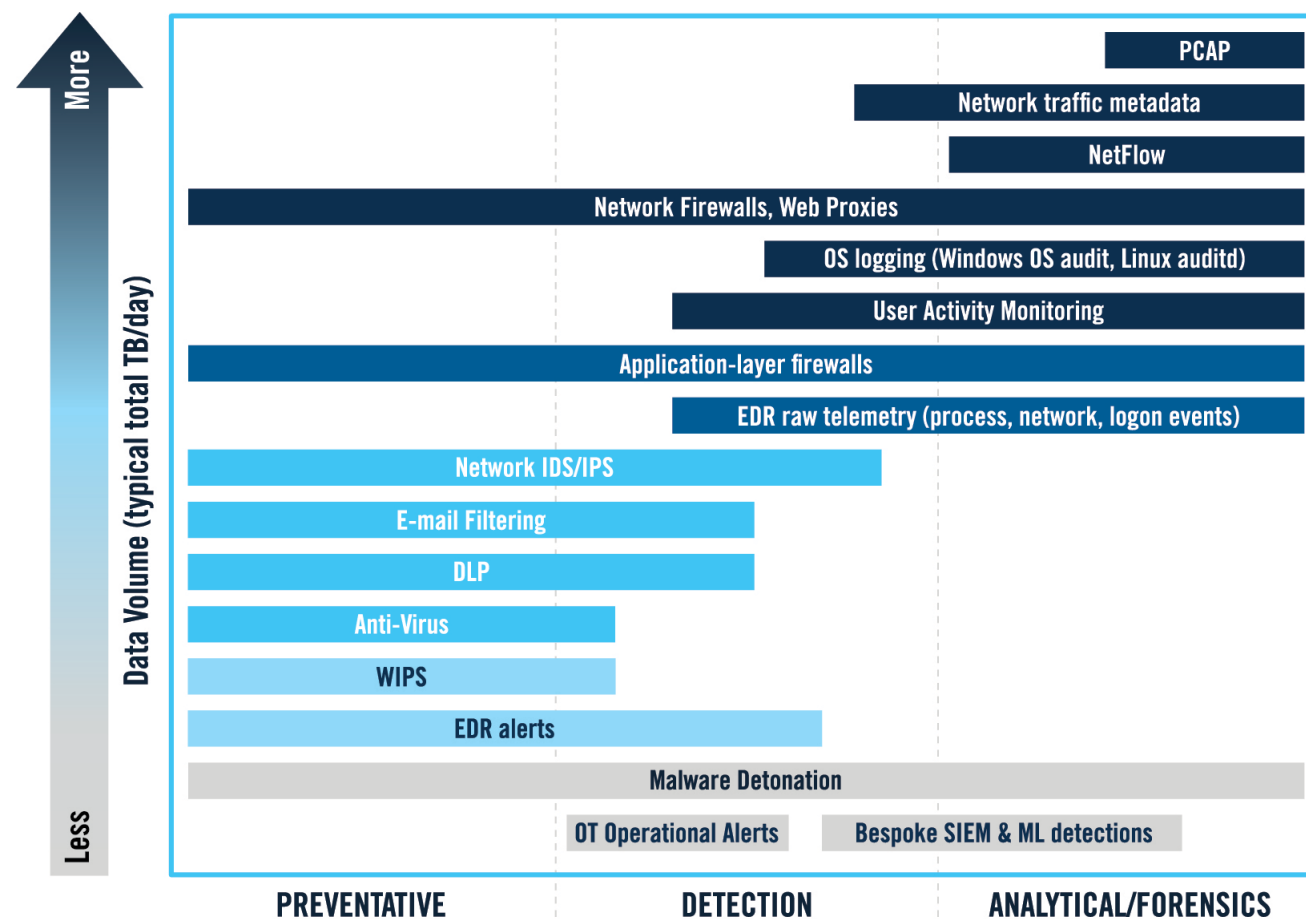
- Once the SOC understands the situations for which it wants to collect data, it next needs to consider the types of data available.
- Each SOC will choose data feeds to best illuminate the enterprise for preventing and detecting intrusions and other monitoring activities.
- Figure shows one way the SOC could leverage host, cloud, and networking sensor data and logs to support detection and investigation activities



Monitoring and detection (3/3)

Data sources available to an IT enterprise; these potential data sources vary in value and volume for prevention, detection, or analytics/forensics.

For example, some data, such as PCAP, is extremely resource intensive, whereas traffic metadata collection analysis, given its comparatively lower volume, provides improved bang for the buck in both detection and analysis.



Tuning approaches

- There are two classic approaches that SOC's may take in selecting and tuning data sources:
- tune up from zero
- tune down from everything

This table also includes a third, somewhat orthogonal approach: **leverage data in place**

Approach	Pros	Cons
Start with the entirety of a given data feed and tune down to a manageable data volume that meets common needs.	<ul style="list-style-type: none"> • Requires little foreknowledge of the data being gathered. • Easiest to implement. • Enables SIEM tools to leverage full scope of data features and event types offered. 	<ul style="list-style-type: none"> • May overwhelm tools and analysts if data feed is too voluminous. • If methodology is used for many data feeds, poses exponential risk of "data overload." • "Default open" filtering policy toward data collection may pose long-term risk to data aggregation systems as feeds change over time.
Start with a candidate data feed, and tune up from zero, focusing only on what is deemed useful or important.	<ul style="list-style-type: none"> • Keeps data volume low. • Focuses systems and analysts only on what is deemed to be of interest. • Less problematic for SOC's with limited budgets. 	<ul style="list-style-type: none"> • Carried to its extreme, limits value given time/effort granting SOC access to given data feed. • Analysts blind to features of data feeds not explicitly set for input into data collection systems. • Approach may require more labor to implement.
Leverage data closer to its source, such as in an intermediate log management or big data platform, rather than ingesting it directly into the SOC's data pipeline.	<ul style="list-style-type: none"> • Keeps latency, performance low. • Context of local data is retained. • Usually lower costs due to fewer copies of the data and less impact on network utilization. 	<ul style="list-style-type: none"> • Can be complicated to configure and maintain; as traffic changes, local processing needs to be updated. Recommended for large enterprises and datasets. • Analysts still need to pivot into the remote data store, which can vary from easy to impossible, depending on the specific scenario. • Analysts need to keep up to date access to remote data; in the presence of dozens or 100 disparate stores, this can become error-prone and time consuming. • This data usually only supports forensics and not detections, as ability to process that data for detections is usually predicated on centralized collection and processing like in a SIEM. • Ensuring chain of custody and anti-tampering of the data may be a concern, depending on where it has kept, who is control, and surrounding security controls, such as data left on end hosts.

Local versus centralized processing

There are many options for determining which data is collected and processed locally, compared to bringing data to a central SIEM for correlation. In general, when tuning datasources, larger, **geographically distributed constituencies** design collection with a combination of local and central techniques for processing and collection

With large, disperse datasets, process data locally, analyze globally

Processing locally can greatly assist in **limiting network traffic and bogging down centralized systems**; **on the other hand, it can also be implemented in a way such that the SOC does not benefit from the data.**

Using local collection and retention is most frequently used in large enterprises with multiple regions and diverse data lakes with many stakeholders.

Local retention does not necessarily mean leaving it on the source host or cloud service, but rather pulling it to a log store local to the region, application, or service in question. This is particularly the case as :

- a) SOC's leverage more sources of data that were not originally meant for security purposes
- b) more services, applications, and cloud resources have a local logging store.

Tuning failure and success auditing

It's also important to avoid a common pitfall when defining audit policies: **generating messages only on a “fail” but not on a “success.”** Failure events include users typing in the wrong password or being blocked from visiting a website. Failures mean a security control did its job: it stopped someone or something from doing what it should not do, which is *usually* a good thing. Successes, such as file modification granted, file transfer completed, and database table insert, are often where the SOC is most interested when performing investigation and analysis. This leads to an important point:

Do not log just the “denies”; the “allows” are often more important

This is because in most situations, a “deny” is an attempt by definition; it did not get through, at least on this attempt. An “allow” is either a legitimate transaction, or it is an attacker or unwanted activity that got past some access controls. Consider situations in which “allows” are often more important than “denies” such as malware beaconing, RATs, data exfiltration, and insider threat. With only failure attempts logged, the SOC will not understand what happened. Failure, block, and deny events are frequently an analytic dead end. Successes events are necessary for both investigation and correlation.

Data Retention – Technical Point of view

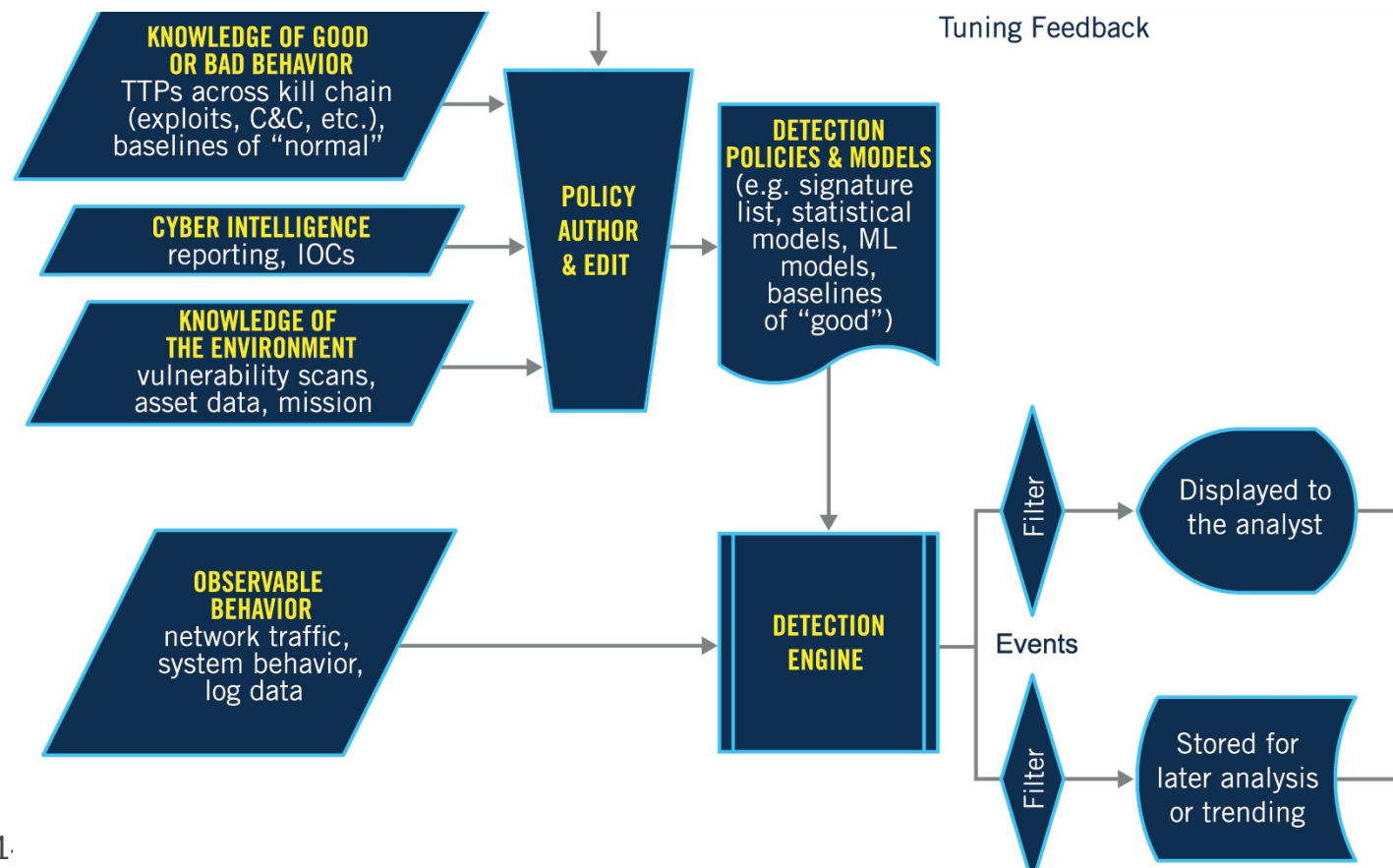
The length of time the SOC needs to retain data is driven by a combination of legal and regulatory requirements, the risk profile of the constituency, and financial constraints. Table above suggests guidelines for minimum online log retention within the SOC, recognizing the distinct needs of SOC triage analysts, SOC forensics/investigations analysts, and external audit and investigation support.

These time frames are primarily based on retention within the constituency's environment. Note that bulk long-term retention of PCAP data is no longer regarded as widely necessary, given the rising importance and comparative value of traffic metadata and host telemetry.

What	SOC triage	SOC forensics & investigations	External Support
EDR, network sensor alerts, and SIEM-correlated alerts	2 weeks	6 months	2+ years
NetFlow & traffic metadata logs	1 month	6 months	2+ years
Full-session PCAP	as needed*	as needed*	as needed*
System, network & application audit logs	2 weeks	6 months	2+ years
Emails	2 weeks	2 years	As needed

Intrusion Detection Overview

Although EDR, network sensors, anti-virus, and SIEM operate at different layers of abstraction, they all generally fit this model. The network sensor observables are network traffic; host observables feed EDR. Network sensor alerts and logs feed SIEM and SOAR, which treats these events as cyber observables, as the sensor did.



- **Misuse or signature-based detection:** Where the system has a priori knowledge of how to characterize and therefore detect malicious behavior, such as with IOC matching
- **Anomaly detection:** Where the system characterizes what normal or benign behavior looks like and alerts whenever it observes something that falls outside the scope of that behavior

Host Monitoring and Defense

Host sensor instrumentation is used by the SOC to detect, analyze, understand, monitor, prevent, and respond to security incidents. These tools generally take the form of a software agent installed on the host connected to a central management system.

In the early days of intrusion detection and incident response, there tended to be a huge emphasis on network-based sensing. Network sensors have many virtues; one sensor provides situational awareness and tip-offs for potential incidents across thousands of systems. **But insight is only as deep as what can be seen in network traffic !**

With the expansion and maturation of host-based monitoring, along with the proliferation of network traffic encryption, emphasis has shifted to host-based instrumentation and prevention. In general, if you are trying to positively confirm an attacker was successful in hacking an account, generally data retrieved from end point sources, such as EDR, will be more effective than network traffic sources such as NetFlow

Data from an endpoint is generally more informative than network traffic data for confirmation of intrusion

User activity monitoring	Data loss prevention
EDR	Host-based firewall
Application allow listing and deny listing	AV/antispware
Executable integrity checking	

Host Observables and Perspective (not Exhaustive)

From mounted file systems and any other storage:

- OS version, installed service pack(s), and patch level
- Installed applications
- Resident files, modification times, ownership, security permissions, contents, and summary data (size and cryptographic hash value)
- Author, date, header, hash, and other qualities of executables and libraries such as Portable Executable (PE) files, Dynamic Link Libraries (DLLs), ELF binaries, etc.
- File system “slack space” containing deleted files and recycle bin/trash contents
- Contents of the entire physical disk such as a bit-by-bit image
- OS and application logs
- OS and application configuration data (e.g., Windows registry hive contents)
- Browser history, cache, cookies, and settings

From system memory and processor(s):

- Application process identification number (PID), creation time, executable path, execution syntax with arguments, name, user whose privileges it is running under, parent (spawning) process identified, and cryptographic hash (user context), CPU time used, and priority
- Actions and behavior taken by running processes and threads, such as execution behavior and system calls
- RAM contents and memory map
- Clipboard contents
- Contents and disposition of CPU registers and cache
- Logged-in users or applications acting with privileges of a remote user such as with a database or custom application

Host Observables and Perspective (not Exhaustive)

From attached devices and system input/output (I/O):

- Network flow (sometimes known as “host flow”) data, possibly including enrichments that tie process name to the ports and connections it has open
- Content of network traffic
- User keystrokes
- Actions from other input devices such as mice, touch pads, or touch screens
- Screenshots
- Connected devices, potentially including details such as device type, driver info, serial number/ID, system resources, addressable storage or memory (if applicable), and insertion/remove events

Endpoint Detection and Response

Endpoint Detection and Response

Purpose-built, commercial host monitoring systems using a mix of signature and host-based techniques to detect and block attacks had been around for a while, new themes emerged or were emphasized:

- Leveraging more perspectives in the operating system to detect presence of the adversary, particularly adversaries who leave few traces on persistent storage
- Allowing the user to interactively collect host state and other details on demand, and to interact with that rich telemetry in a manner that goes beyond alert triage
- Stronger coverage across the cyber-attack life cycle, combined with an increased integration and focus on high-fidelity cyber threat intelligence

Since then, techniques consistent with EDR capabilities have become an indispensable tool for the SOC. EDR capabilities can be achieved by buying a single commercial product, by building a solution from disparate tools, or a combination thereof.

Alternatives to an EDR solution

It is possible to compose many of the same capabilities as an “all in one” EDR from disparate host telemetry scanning and capabilities. Sysmon, OS Query, and GRR provide hugely rich host SA. Even ordinary Windows Event Collection and Forwarding (WEC/WEF) and Linux auditd provide tremendous insight into host activity.

The advantages to building a custom capability is typically increased flexibility and lower initial acquisition cost. However, they also require an increased time investment to develop and deploy, and usually do not have the benefit of technical support. SOCs looking to take this approach should also observe the following considerations:

- A best-of-breed EDR will ship with a library of thousands of curated detections; it is virtually impossible for a single SOC to achieve this same level of detection coverage and sophistication from scratch.
- The EDR graphical user interface (GUI) is optimized for working with EDR data; building this using other available tools may not yield the same user experience.

Application Allowlist, Denylist and Integrity Checking

Often built into operating systems, application deny listing is a technique whereby an OS module or protection agent blocks unwanted processes running on the end host. Similarly, application allow listing policy uses a default deny approach. Sysadmins must define which programs and software publishers are authorized for execution; all others are blocked from running either by the OS or by the allow listing/deny listing client. **Gatekeeper in macOS, AppLocker in Windows and AppArmor in Linux** can be used to **limit which users use what programs, and with which permissions**. Apple has released Gatekeeper, an allow listing component to keep out unnotarized (vetted) applications and malware.

SOCs wishing to pursue application allow listing or deny-listing technologies should consider the **additional management overhead involved in tracking allowed or denied applications on the enterprise baseline**. To implement allow listing:

- all monitored hosts should adhere to a known OS
- application baseline (the SOC must continually maintain consistency with that baseline)

This can be problematic with a complex enterprise baseline or decentralized IT administration

Generally, application allow listing and deny listing are **most successful for high-risk users that have a finite software baseline and/or stick to software from a known set of publishers or app stores without much divergence**.

More traditionally, **Tripwire** is used on end hosts to detect changes to key configuration files and can alert on changes that may be an indicator of malware or a malicious user. Changes that are detected in monitored files and settings can be detected and reversed by the administrator. **Other tool permit now a file integrity checking control**.

Host-Based Firewalls & Antivirus and Antispyware

Traditional security devices still play a role in overall security and SOC success. Although firewalls are most widely recognized as appliances that filter traffic crossing between two or more network boundaries, host-based network traffic filtering capabilities can be found in virtually all popular varieties of UNIX, Linux, and Windows, and are integrated in some EDR products.

Antivirus was one of the earliest host-based defensive capabilities. It is a program that inspects file system and memory contents, leveraging a large signature pool and heuristics to find known malware or malware techniques. **Antispyware** capabilities are often included in most AV suites. They add to malware detection capabilities by examining Web browser specifics such as stored cookies, content, extensions, and stored cache.

A common criticism of AV tools is that their system resource utilization, RAM footprint, and regular disk scans outweigh their diminishing benefits. AV on non-Windows platforms such as Apple, Linux, and UNIX are regarded as unnecessary by some defenders, whereas on Windows, AV still provides some value, especially for malware detection resulting from Web surfing. However, AV indicated “cleaned” infections can be deceiving, sometimes leaving adversary tools and persistence on the system.

Today, it is most common for a SOC to leverage traditional AV as part of a larger EDR suite

DLP & UAM

Data Loss Prevention

For many constituencies, there is significant concern about the **exfiltration** of sensitive data from the enterprise. This can include anything from sending sensitive documents over personal email to downloading HR data to a thumb drive. One feature set of certain **endpoint products**, including purpose-built data loss prevention (DLP) solutions is to monitor, detect, or prevent loss of confidential or sensitive data. This can range from healthcare records to financial data, to PII.

No matter how implemented, **the host is often the only place** where the SOC can expect to clearly see this activity (e.g., through network traffic, clipboard, file copy, print activity and system call observables). Some DLP packages can also be used to block or limit user access to removable media, enhancing functionality already present in Windows domain GPOs.

Alternatively, some adversary engagement and deception products can leverage techniques like **honeytokens**, or **bogus records**, datasets, or **other data of no value**, are often set to entice intruders. **When altered or exfiltrated, alerts are sent to the SOC.**

User Activity Monitoring

In some enterprises, there is a significant concern over the actions of portions of the user populace. These constituencies must follow a policy of “trust but verify,” whereby users are given latitude to perform their job functions, but their actions are heavily monitored. These may include any constituency that handles large amounts of sensitive or high-value data, such as defense, intelligence, or finance.

In such cases, security, counterintelligence, or intellectual property loss prevention may require full scope user activity monitoring, primarily from monitoring on the host. Typically, these capabilities involve comprehensive capture of user activity on desktops, where users’ actions can be monitored in real time or replayed with screenshots and keystrokes. The efficacy, ethics, and legal issues surrounding use of such software are outside the scope of this presentation.

Host Sensor Placement

Although host-based sensing is both scalable and frequently used, not all SOC's are resourced to put an agent on every constituency host. Table provides some considerations and examples for where to prioritize host monitoring deployment.

Prioritized Placement	Example(s)
Host, service, application, or workload mission criticality	Key enterprise database servers, financial systems, manufacturing automation control, systems containing PII, systems under regulatory/compliance controls
Number and strength of trust relationships between that system and other hosts, especially hosts residing in other enclaves	<ul style="list-style-type: none">• Web servers directly exposed to Internet• Web services systems forming a business-to-business (B2B) relationship with a partner company• Remote access VPN or webmail servers
Number of, and privileges wielded by, users on that system, especially users residing in other enclaves	Web-enabled financial application server; call center ticketing system
Vulnerability and attack surface exposed by system(s) of concern	Any server that cannot be regularly patched for whatever reason (legacy, operational demands, fragility, etc.)
Stability, maturity, applicability of protection mechanism(s) to that platform	Commodity, non-embedded IT such as Windows, Linux, and macOS systems

Not all monitoring tools are applicable to all hosts. In some cases, the most important systems in the enterprise may not be well suited for a typical host sensor suite, such as legacy mainframe systems and embedded OT. The SOC may depend on other tools like configuration checkers, robust logging, and native OS host firewalling.

Network Monitoring – NIDS-NIPS

Although there is a strong move toward host-based monitoring, network-based monitoring is still used by many SOC's. Network-based monitoring technologies can sometimes be the most cost-efficient and simplest means by which SOC's can gain visibility and attack detection coverage for a given enclave or network, especially in cases where they have no other visibility.

- Attacks detected by NIDS, NIPS, such as exploits executed across the network (most notably remotely exploitable buffer overflows), no longer comprise the majority of initial attack vectors.
- Client-side attacks, such as phishing, have long become far more prevalent, giving way to the content detonation and analysis devices.
- Signature-based methods by themselves (e.g., AV and traditional NIDS) are no longer sufficient for finding attacks and defending a network.
- Many cloud-based services consumed by many enterprises do not support the deployment of traditional NIDS/NIPS due to their network topology.

Vendors such as Cisco and Palo Alto merged their firewall and NIDS/NIPS capabilities into single product suites years ago. It is increasingly difficult to find a firewall without an IDS/IPS feature set, and vice versa. The term “Network Detection and Response” or NDR is often used to refer to products with NIDS/NIPS functionality. Today, **the focus for network sensing** is often around:

- a) merged function network security devices, sometimes referred to as “NGFW”
- b) NetFlow and traffic metadata collection
- c) malware detonation
- d) some dedicated network sensing/analytic platforms

Net Flow

Whereas some sensors examine entire contents of network traffic, it can also be useful for the SOC to have a capability that succinctly summarizes all network traffic. One data source complementary to sensor alerts are NetFlow records (often referred to as flow records or flows). **Rather than recording or analyzing the entire contents of a conversation, each flow record contains a high-level summary of each network connection.**

While different NetFlow generation and manipulation tools are available, each flow record generally provides the following information:

- Start time and end time (or duration since start time)
- Source and destination IP
- Source and destination port
- Layer 4 protocol—TCP, UDP, or Internet Control Message Protocol (ICMP)
- Bytes sent and bytes received
- TCP flags set (if it is a TCP stream)

Whereas the contents of a network connection could be gigabits in size, a single flow record is less than a few kilobytes.

NetFlow Devices

Flow records can be generated by different devices, including:

- Routers and switches
- Some sensor products, in addition to normal stream of intrusion detection alerts
- Some EDR tools record not only flows seen by the local host, but also tie the flow to the OS process transmitting or receiving on the port in question (sometimes known as hostflow), enriching the contextual quality of the data at the potential expense of extremely high volume if widely deployed.
- Software packages purpose-built for flow generation, collection, and analysis, such as SiLK, Argus and Zeek (can generate functionally similar telemetry and much more)

Many SIEM tools and log management systems are more than adequate at consuming and querying flow data. SIEM tools are useful in analysis because they can process and alert on NetFlow records in real time

Traffic Metadata

- With all the data sources, and particularly combining host and network data, parsing can be unreliable and cumbersome when trying to manage full content analysis.
- Fortunately, network traffic metadata tools take NetFlow one step deeper into the TCP/IP stack, providing analysts with rich network-based situational awareness.
- Metadata is roughly as voluminous as NetFlow, in terms of the number of records generated on a busy network link, but it can serve as an enhanced source of potential intrusion tip-offs.

Collecting metadata in the right places on the network allows the SOC to be more selective in what is collected. Thereby, it presents less of a performance burden on both the SOC's collection systems and network services such as DNS servers or mail gateways. More bluntly, many DNS servers will crash with full DNS logging turned on, whereas a **traffic metadata sensor** is designed precisely to record every DNS request and reply seen on the wire at very high speeds.

Some tools such as Yet Another Flowmeter (YAF) and SiLK and Zeek provide robust metadata generation and analysis capabilities.

Zeek has a vibrant community and ecosystem of plugins and analytics

Full Session Capture PCAP and Analysis

When analyzing a serious incident such as one that requires **active response or legal action**, the SOC requires **concrete proof of what happened**. This confirmation comes from host data.

Having a complete record of network traffic can also be helpful, especially when host telemetry is not available or untrustworthy

Traffic capture is typically done on major perimeter connections, and in an ad hoc manner near systems that are **suspected of compromise**, such as with adversarial engagements and other incidents. While the SOC can filter out traffic that has no value of being recorded past the header (such as SSL/TLS sessions), or in extremely long-running flows (e.g., “elephant flows”), the SOC can still face scalability challenges in all but the smallest deployments.

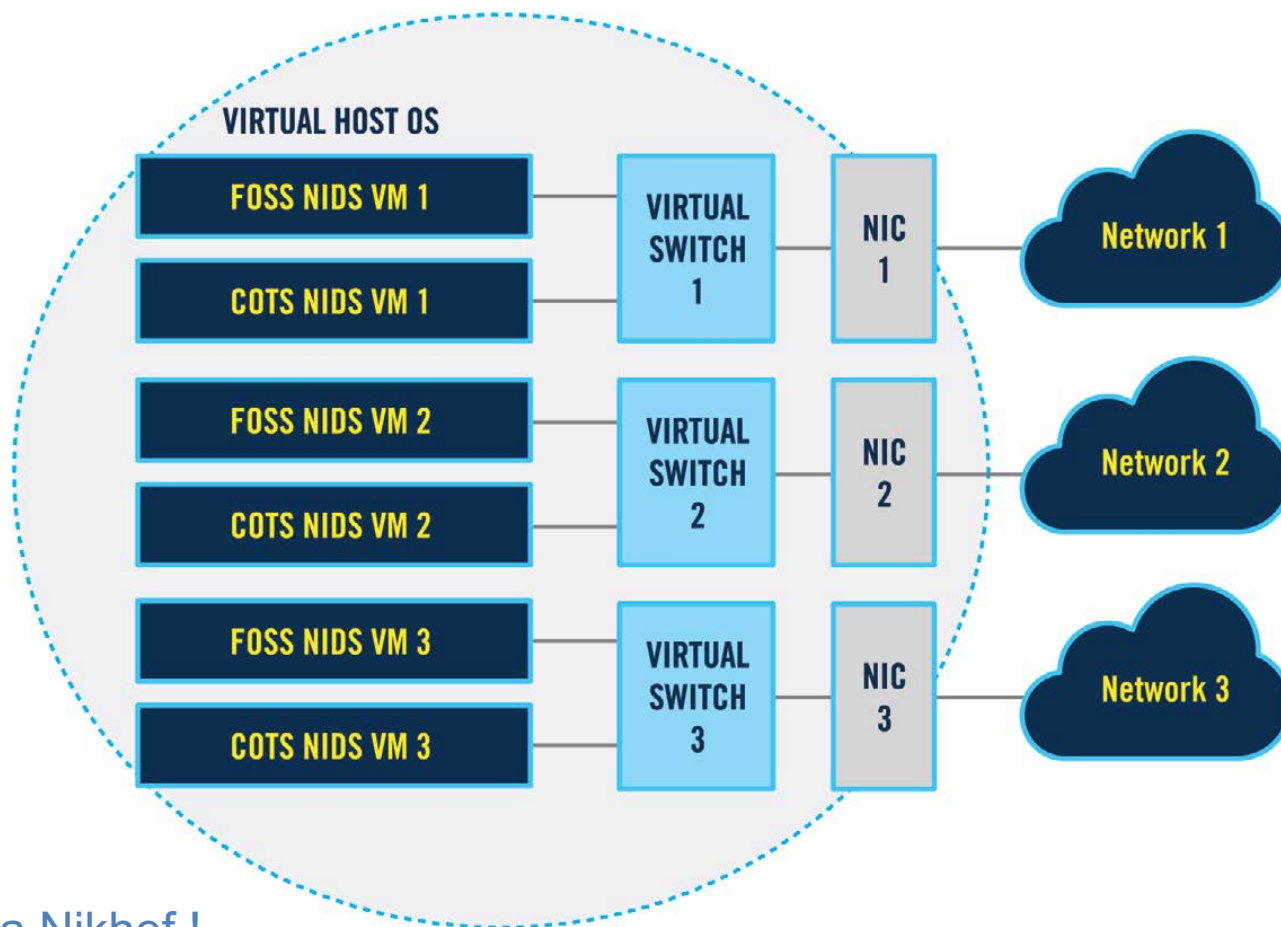
The biggest challenge with full-session capture is volume. Consider an office building that connects to the Internet through an ordinary 10gigabit/s Ethernet connection on its way to a VPN and ISP. At an average of 50 percent utilization, the SOC would collect this volume in a 24-hour period:

$10 \text{ Gbit/s} * 60 \text{ sec} * 60 \text{ min} * 24 \text{ hours} * .5 \text{ utilization} / 8 \text{ bits per byte} = 54 \text{ TB}$

Specific traffic collection and analysis tools include **RSA NetWitness**, **Arkime** (formerly Moloch) and **NTOP**

Building an Open-Source Network Monitoring Capability

- The SOC has different options for which platform may serve as a basis for network monitoring capabilities
- If the SOC needs collocated NIDS monitoring, NetFlow, or (and sometimes full PCAP) collection, these tasks may be accomplished at scale with FOSS tools such like Suricata, Zeek, and tcpdump, with scripting to glue them together. Some SOC's have bolted on additional functionality like file carving and file YARA scanning as well. However, as mentioned above, this can become complex.
- Zeek, Snort, and Suricata are regarded as de facto standards when it comes to performing custom network sensing. Some commercial vendors have integrated these technologies directly into their platforms and/or provided interoperable signature and scripting formats.



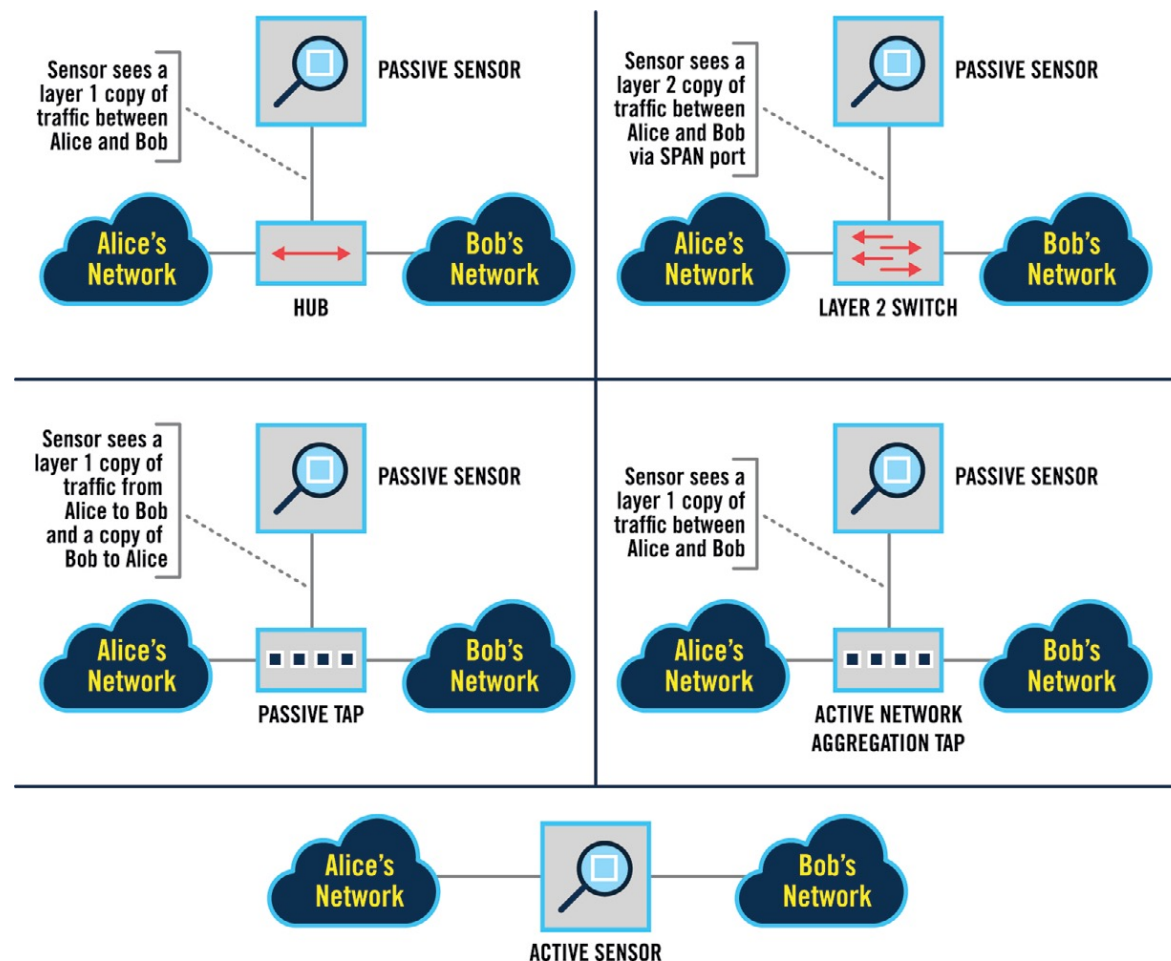
Questo se non erro è il progetto in Corso a Nikhef !

Directing Traffic to Network Sensors

At the top right, the hub is replaced with a layer 2 or layer 3 network switch. This switch is configured with a switched port analyzer (SPAN) to copy or “span” traffic from one or more source ports or virtual LANs (VLANs) to the port hosting a network sensor.

In the middle of the diagram, a network tap is used. A network tap is essentially a device inserted between two network nodes that makes a copy of all network traffic flowing between them.

Popular manufacturers of network taps include **Network Critical**, **Netscout** and **Gigamon**. Network taps are not generally subject to the same range of misconfigurations that switch SPANs are.



Directing Traffic to Network Sensors

Physically placing sensors within close proximity to their monitored network segment is almost always the cheapest option; as a result, effective remote management is essential.

All these traffic redirection options have implications for how to prevent the network sensor from compromise or discovery.

First, the monitoring port or ports should not have an IP address assigned to them. This will minimize the likelihood that it will talk back out on the network or bind services to the port

What	Pros	Cons
Hub	<ul style="list-style-type: none"> Inexpensive Easy to install Can attach as many monitoring devices as there are free ports 	<ul style="list-style-type: none"> Sensors will miss packets due to collisions. Almost never an option: modern networking is usually 1gigE and up, whereas hubs only work on 100mbit and below.
SPAN	<ul style="list-style-type: none"> Free to use if monitoring points already have managed switches in place, which is very likely. RX and TX are combined; one network cable off a SPAN port can plug right into a sensor. Straightforward for monitoring traffic from any device hanging off a switch (such as a firewall, WAN link, or cluster of servers). Can attach as many monitoring devices as there are free ports (and switch SPAN capacity). Can be used to monitor network core, such as spanning multiple ports off a core switch or router. 	<ul style="list-style-type: none"> An adversary with access to the enterprise network management platform can disable monitoring feeds to the sensor. Some older or cheaper switches support only one or two SPAN ports per switch, limiting options. When spanning traffic from multiple source ports, the destination SPAN port may become oversaturated if the source ports' traffic aggregate bandwidth exceeds the SPAN port's speed. Changes to VLAN or port configurations after initial SPAN configuration can partially or completely blind the network sensor without the SOC necessarily realizing it.
Tap (include both passive and active)	<ul style="list-style-type: none"> Invisible from a logical perspective. Only operates at the physical layer, meaning the adversary does not have an obvious target to exploit or circumvent. Should not alter packets in any way. Active network regen taps support multiple monitoring devices. Active aggregation taps with packet deduplication can reduce the total network sensor count and total sensor capacity requirement. 	<ul style="list-style-type: none"> An additional device (albeit usually well-built and simple) that can fail is introduced into critical network links. Only appropriate when observing conversation between two networked devices (as opposed to many with a network switch SPAN), as is often the case in perimeter network monitoring. Every monitoring point requires the purchase of a tap device. With a passive tap, RX and TX lines need to be recombined; some sensor technologies do have the internal logic to do so. Passive network taps only support one monitoring device.
What	Pros	Cons
In-line	<ul style="list-style-type: none"> Sensor can actively block traffic, depending on rule set. 	<ul style="list-style-type: none"> If sensor goes down, it may cut off communication unless resiliency features are built in (e.g., "fail open"). Some sensor technologies introduce packet latency or packet reordering, which in turn can sometimes degrade network quality of service or make the sensor detectable. More than one monitoring device means serial attachment of devices in-line, each being a separate point of failure.

SecWS23

Network Sensor Placement

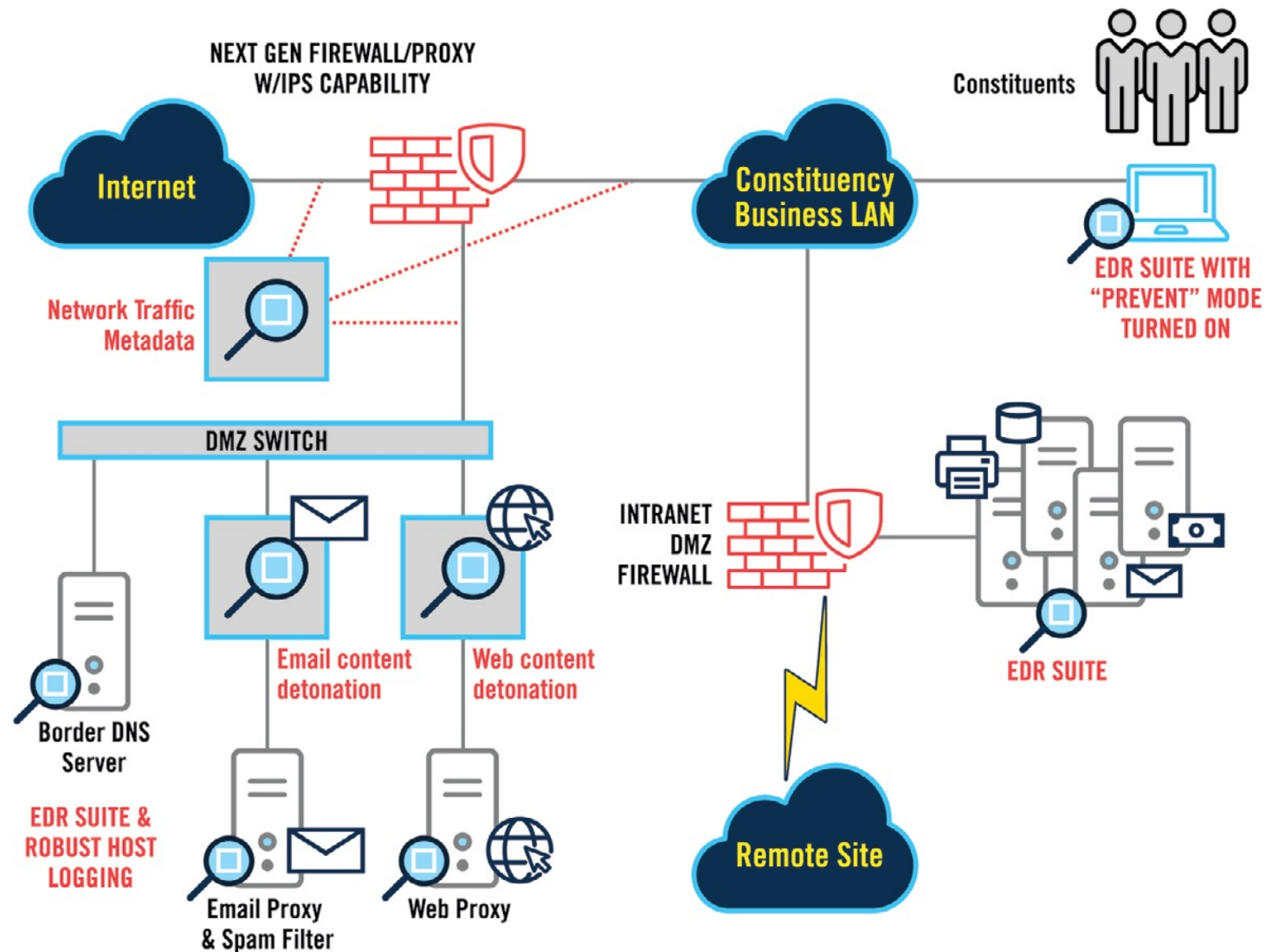
Goals	Placement Example(s)
Gain visibility into systems important to constituency mission.	<ul style="list-style-type: none"> Servers hosting custom mission applications and sensitive data placed behind sensor
Provide coverage for systems that are of especially high value to adversaries.	<ul style="list-style-type: none"> Systems behind sensor contain trade secrets, source code, or confidential records An Internet-facing email gateway serving a large user population
Achieve greatest “bang for the buck” by picking locations that host a large number of network connections (e.g., network “choke points”).	<ul style="list-style-type: none"> All network traffic between two major corporate regions transit sensor, covering 10,000 systems
Protect systems that sit on the trusted side of a controlled interface (e.g., a firewall).	<ul style="list-style-type: none"> Sensor is between university dorm networks and the university’s registrar’s office. Company A’s servers communicate with Company B’s servers across a private link
Goals	Placement Example(s)
Have complete insight into the traffic being observed (e.g., it is not encrypted and uses protocols the sensor understands).	<ul style="list-style-type: none"> On the unencrypted side of a VPN termination point or SSL accelerator On both sides of a NATing firewall or Web proxy
Leverage passive monitoring as a compensating control for systems that lack critical security features or have serious unmitigated vulnerabilities.	<ul style="list-style-type: none"> Legacy or proprietary ICS/SCADA or mainframe enclaves or network segments

There are variety of network monitoring technologies that can be placed throughout the environment, including:

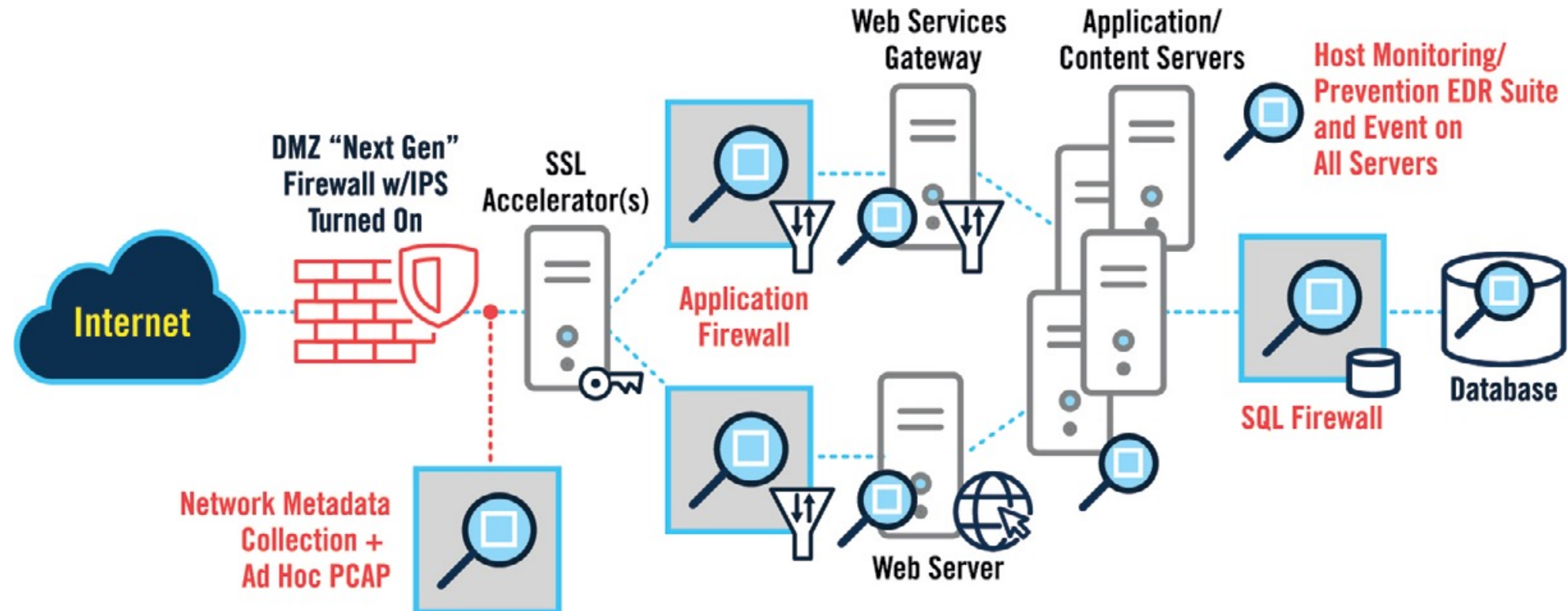
- Dedicated network sensors
- Combined security devices that feature IDS/IPS features such as next gen firewalls and all-in-one security perimeter protection
- NetFlow and/or traffic metadata record generation
- Sustained and ad hoc full PCAP collection

Even if a SOC completely eschews classic signature-based NIDS, it should consider other strategies like network traffic metadata collection. Regardless of the technology chosen, Table features some tips for sensor placement.

Example #1: On-Prem Enterprise Network



Example #2: On-Prem-Based or Cloud-Based DMZ



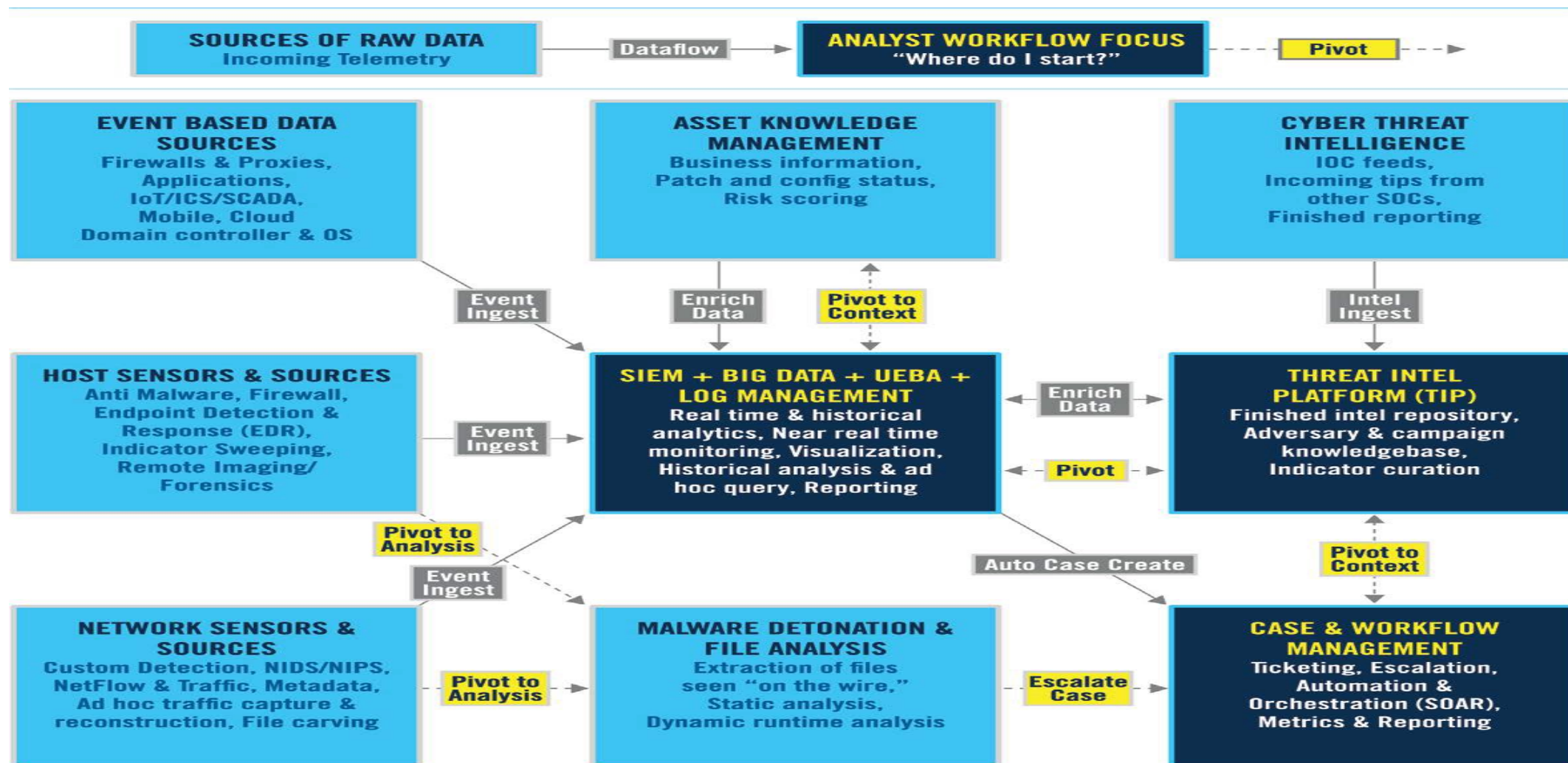
Leverage Tools to Support Analyst Workflow

- Previous strategies discussed the sources of data and threat intelligence the SOC has at its disposal, including sensing technologies and log feeds.

Each piece of data is valuable on its own, but its only when combined that the true power of the data becomes available.

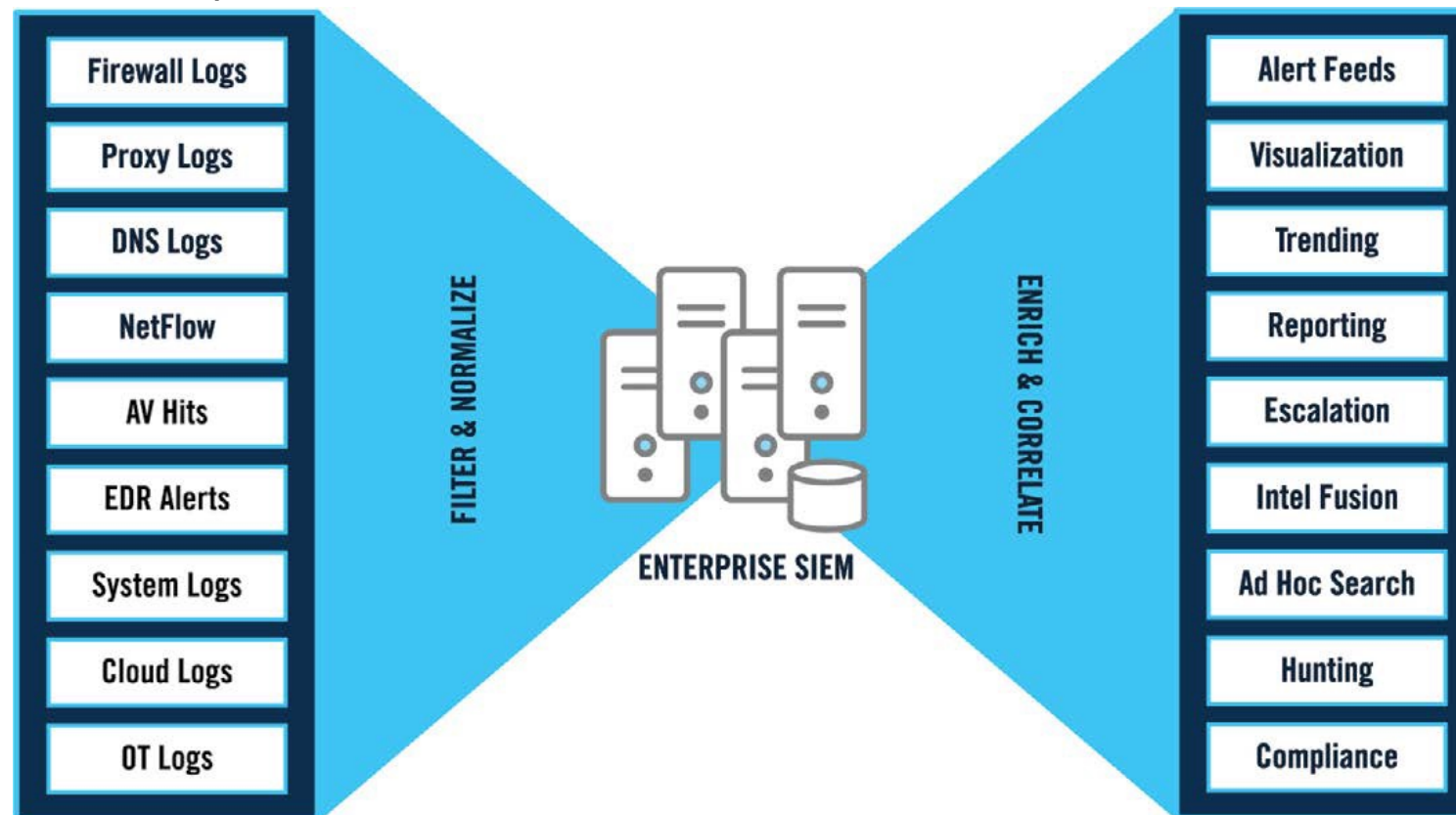
- To achieve this goal the SOC needs to bring all this data together into an architecture that can help turn the data into information, and information into knowledge. And this architecture must support the analyst workflow within the SOC. As with many aspects of the SOC there is not a one-size-fits-all answer about how to do this.
- Different SOC's will put different tools at the focal point for their workflow: **SIEM, SOAR, case management, EDR, threat intel management**, and so forth.
- Rather, reducing the number of panes of glass, and providing integration between them is the best strategy with an emphasis on automation and integration for repeated tasks, escalation, and incident handling.

Tool Integration Overview



Security Information and Event Management

- SIEMs promise the ability to maximize the value of the billions of events collected every day.
- **SIEMs can be very expensive both to acquire and to use;** like any other SOC technology, the value found from a tool is largely proportional to the effort put into that tool.



Security Information and Event Management

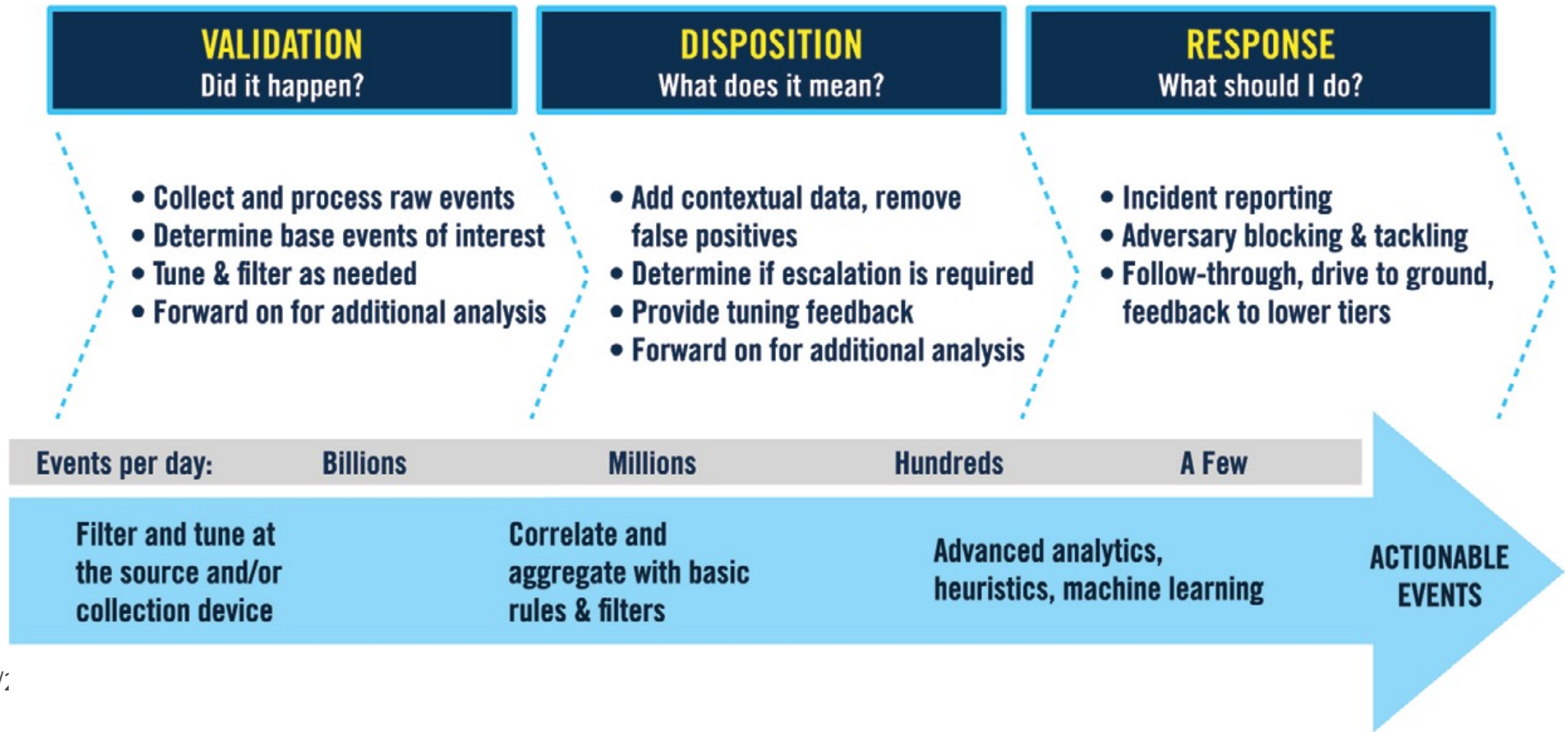
The purpose of SIEM is to enable the analyst to turn information collected by the SOC into knowledge that can be acted upon in a timely fashion. Modern best-of-breed SIEMs can support many compelling use cases:

- **APT detection:** Including piecing together disparate data indicating lateral movement, remote access, command and control, and data exfiltration
- **Incident analysis and log forensics:** Including retention and investigation of historical log data
- **Workflow and escalation:** Tracking an event and incident from cradle to grave, including ticketing/case management, prioritization, and resolution
- **CTI fusion:** Integration of tipsters and signatures from CTI feeds
- **Trending and threat hunting:** For analysis of long-term patterns and changes in system or network behavior
- **Perimeter network monitoring:** Classic monitoring of the constituency for malware and external threats
- **Insider threat and audit:** Data collection and correlation that allow for detection and monitoring for profiles of suspicious internal threat activity
- **Configuration monitoring:** Alerting on changes to the configuration of enterprise servers and systems, from password changes to critical Windows registry modifications
- **Cyber SA:** Enterprise-wide understanding of threat posture
- **Policy compliance:** Built-in and customizable content and reporting that satisfy elements of various regulatory compliance, such as PCI, SOX, and FISMA.

Security Information and Event Management

Figure follows the basic SOC workflow: alert enrichment, prioritization, triage, investigation, escalation, and response.

In this process, SIEM moves from automation on the left, through correlation and triage, to workflow support and enabling features such as event drill-down, case management, and event escalation on the right.



SIEM Architecture, Common Features, and Expectations

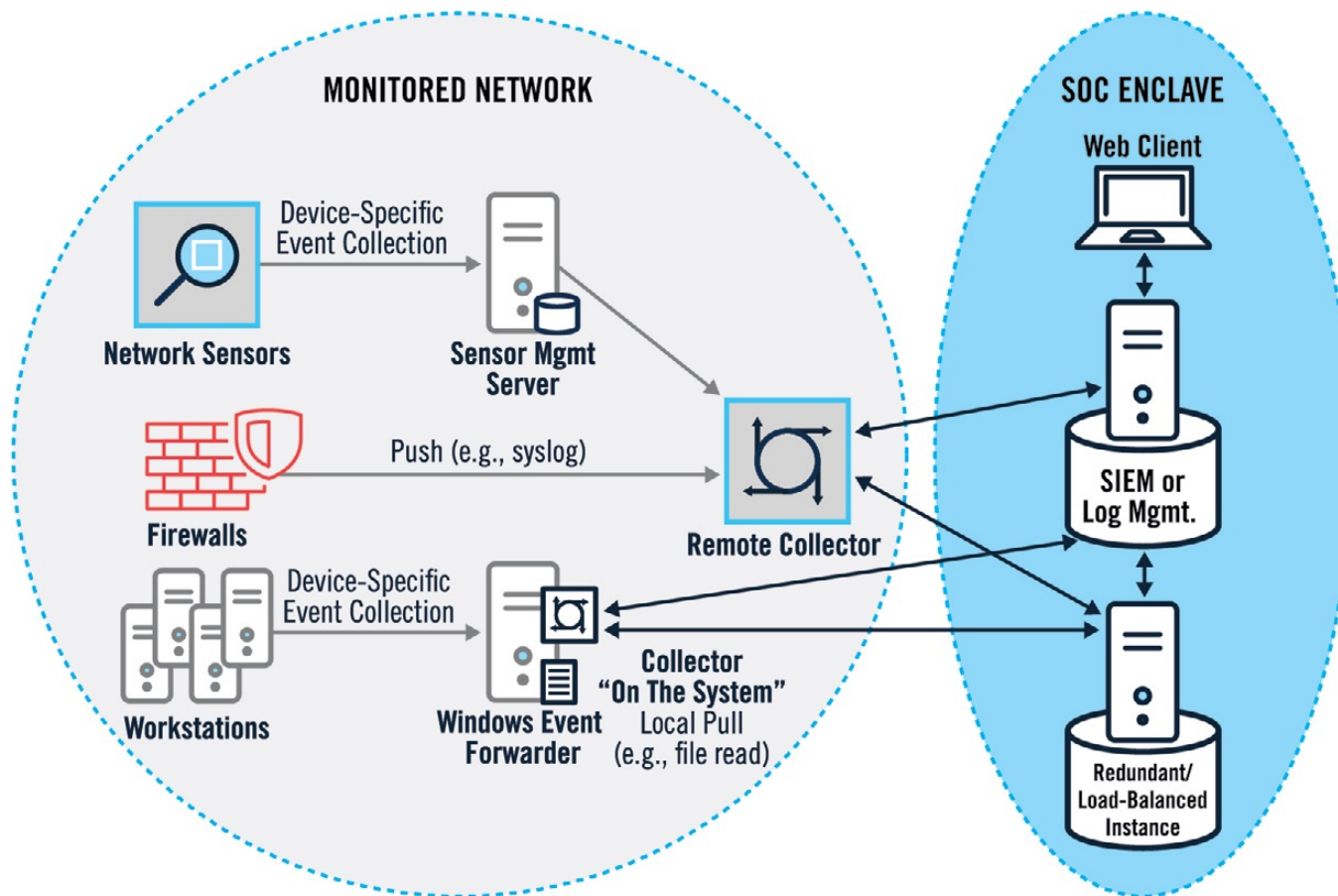
Each SIEM vendor brings its own approach to bear in providing its blend of functionality. With that said, there are some common functions and components in modern SIEMs.

SIEM Data Acquisition and Collection

The monitored host: Where it has direct access to logs such as through local APIs, or files accessible from a filesystem seen by the host.

Remotely: Where it either interrogates one or more devices for data (pull) or accepts data sent to it (push); the agent can gather this data through various native protocols such as syslog, RESTful APIs, and Java Database Connectivity (JDBC).

There is no SIEM architecture that is fully agentless, meaning there is always a piece of software that must ingest the data; what is in question is the location of that agent—on the host being monitored, running as software on a nearby system, running on an appliance, an API on the SIEM, or in the cloud as a SaaS capability; best-of-breed SIEMs should offer most or all these scenarios.

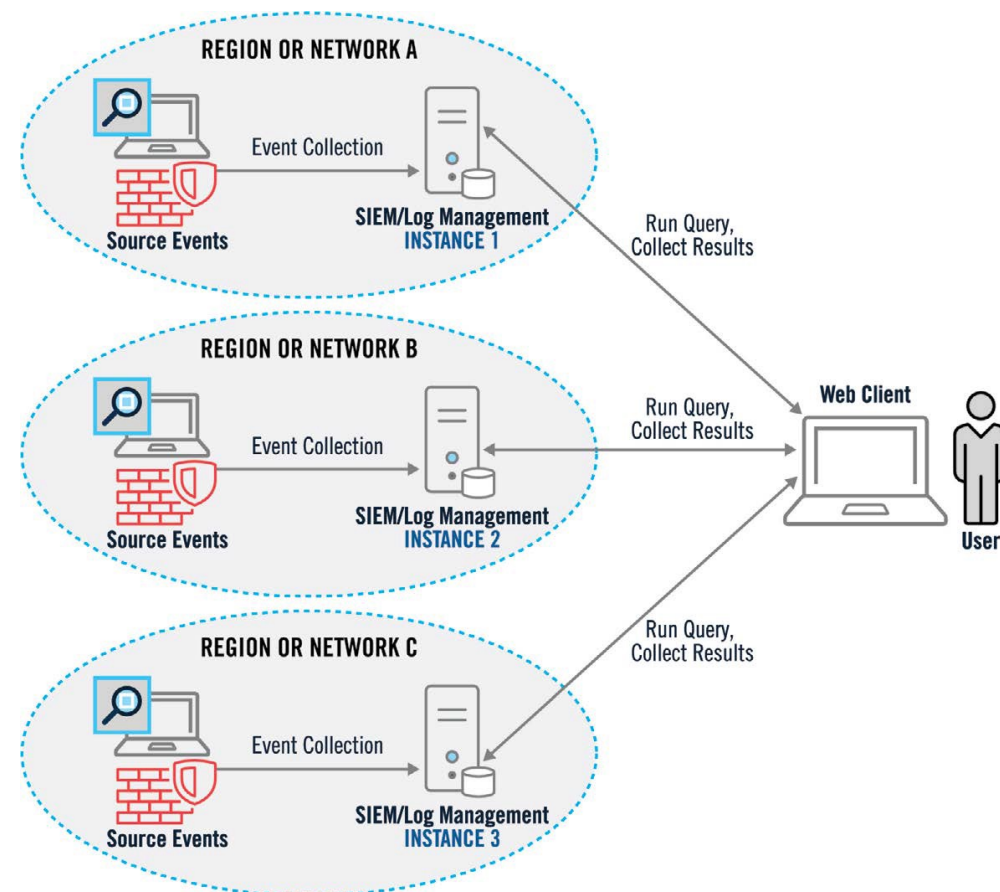


SIEM data normalization and persistence

In many SIEMs, data is collected at a central location. Data is typically stored in a backend that supports high-speed queries and condenses on-disk storage. Most SIEMs offer a distributed, horizontally-scalable architecture that uses NoSQL techniques such as MapReduce, document stores, Key Value Stores, or columnar stores to fragment or “shard” data across many nodes.

Using a combination of the above techniques, modern SIEMs can persist, index, and query data measured in the multi-petabyte range. In situations where a single SIEM exceeds roughly 20TB-100TB per day or 100,000-500,000 events per second, the SOC may wish to pursue “cluster of clusters” approaches whereby disparate SIEM cluster instances share persistence, query, and analytic load. **These techniques are often known as federated query**, [federated search, cross cluster join], or when geographically distributed, geo sharding.

Federated query is an extremely powerful technique whereby a single user, running a single query, can interrogate multiple disparate SIEM or log management systems in parallel, with the results collated in a manner that makes the experience seamless for the user



SIEM data analytics

The SIEM will generally support two or three approaches to analytics and detections:

A near-real-time alerting and correlation engine: Supports alerting on single event matches (known as atomic rules) and sets of events, potentially utilizing a state machine (e.g., “true” multi-event correlation)

An analytic engine that executes analytics against data persistent on disk: Sometimes referred to as “query on a timer” that executes on a schedule defined in each analytic

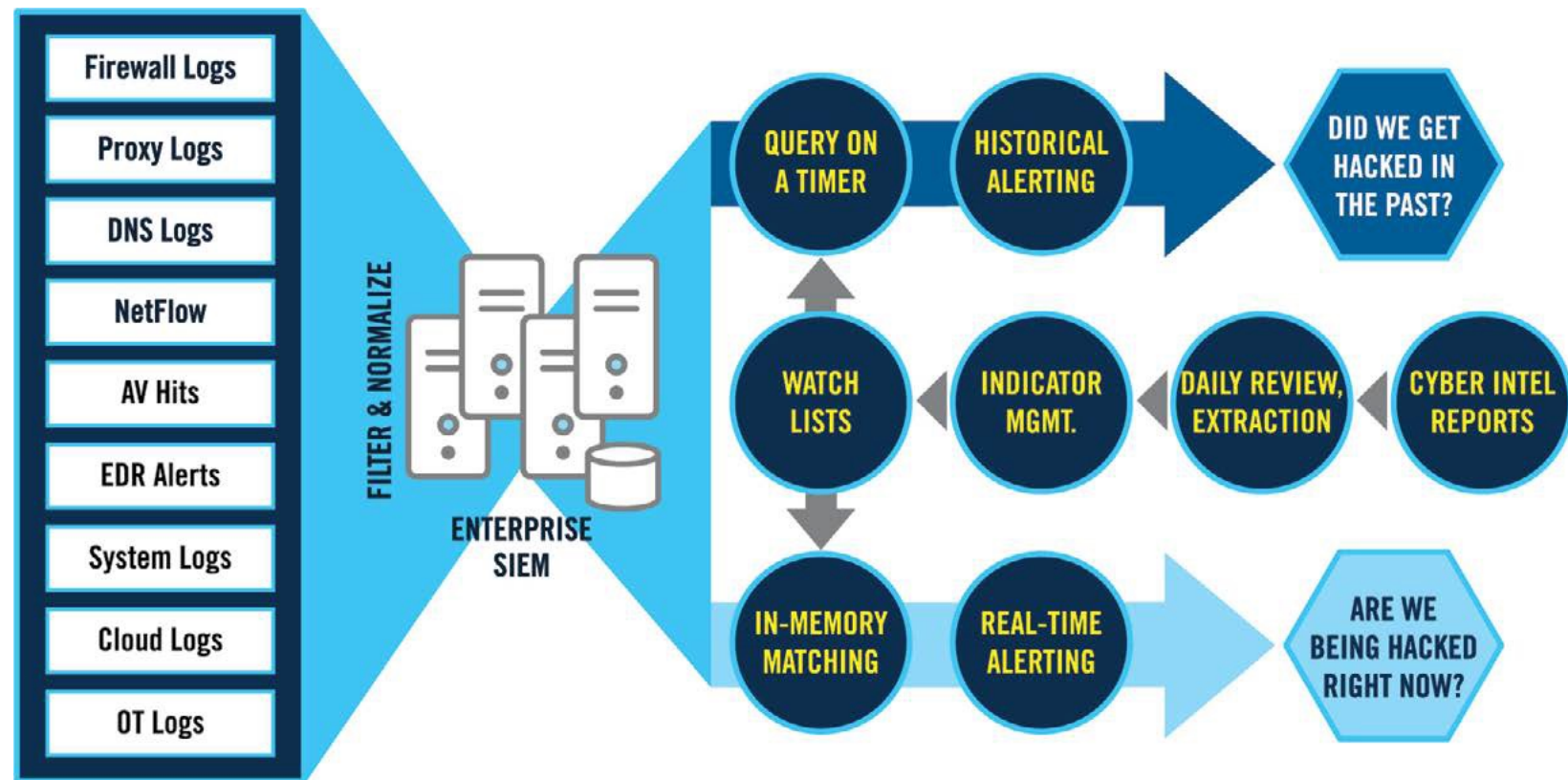
A machine learning (ML) engine: For more advanced SIEMs (and SOCs), the ML engine can run on data in-memory as it streams in and/or against data persisted on disk

The SIEM analytic engine is its most complex and defining feature in contrast to ordinary log management systems. It will ship with “stock” rules targeting various cyber defense, insider threat, compliance, and other use cases to detect complex behaviors or pick out potential incident tip-offs.

- Normalization, prioritization, and categorization that enable the SIEM to leverage various data feeds in a device-agnostic manner but is sometimes challenged due to the large diversity of data.
- Events can have their priority raised or lowered based on hits against correlation rules and enrichment such as comparison against vulnerability scan data and various ML techniques.
- Alerts fired by various analytics can trigger various other user-configurable actions such as creating a case within SIEM and attaching the event to it, running a script, or emailing to an analyst. This functionality may be further extended through a SOAR product

SIEM data analytics

- To illustrate both real-time and retrospective techniques brought to bear by many SIEMs, one may consider the case of IOC matching. IOC searches can be done both against data as it streams into the SIEM, as well as against historical value.
- Some SOCs do both, enabling both near-real-time alerting on IOCs, and retrospective matching on recently ingested IOCs matched against events ingested a week ago (for example).



Log Management

Collecting and querying events from a disparate set of systems or applications does not always necessitate the features and cost associated with a full-blown SIEM. Oftentimes a less-expensive log management system, which is usually simpler to set up and use, is a better choice.

Log management systems incorporate some of the aggregation, storage, and reporting capabilities found in SIEM, but with a comparatively smaller feature-set. Some SIEM and log management systems perform “dual duty” meaning they can serve both general IT use cases and the SOC. **Two very good examples of this are Elasticsearch and Splunk**

Some organizations have few resources and do not devote many (if any) full-time staff to alert triage and incident response. Discussed below in SIEM Alternatives, their needs are likely satisfied by log-management system in concert with an EDR product. Full-fledged SIEMs requires care and feeding that small SOC's, and security teams are historically challenged to provide, although cloud based SIEM “as a service” are changing this equation.

SIEM Alternatives

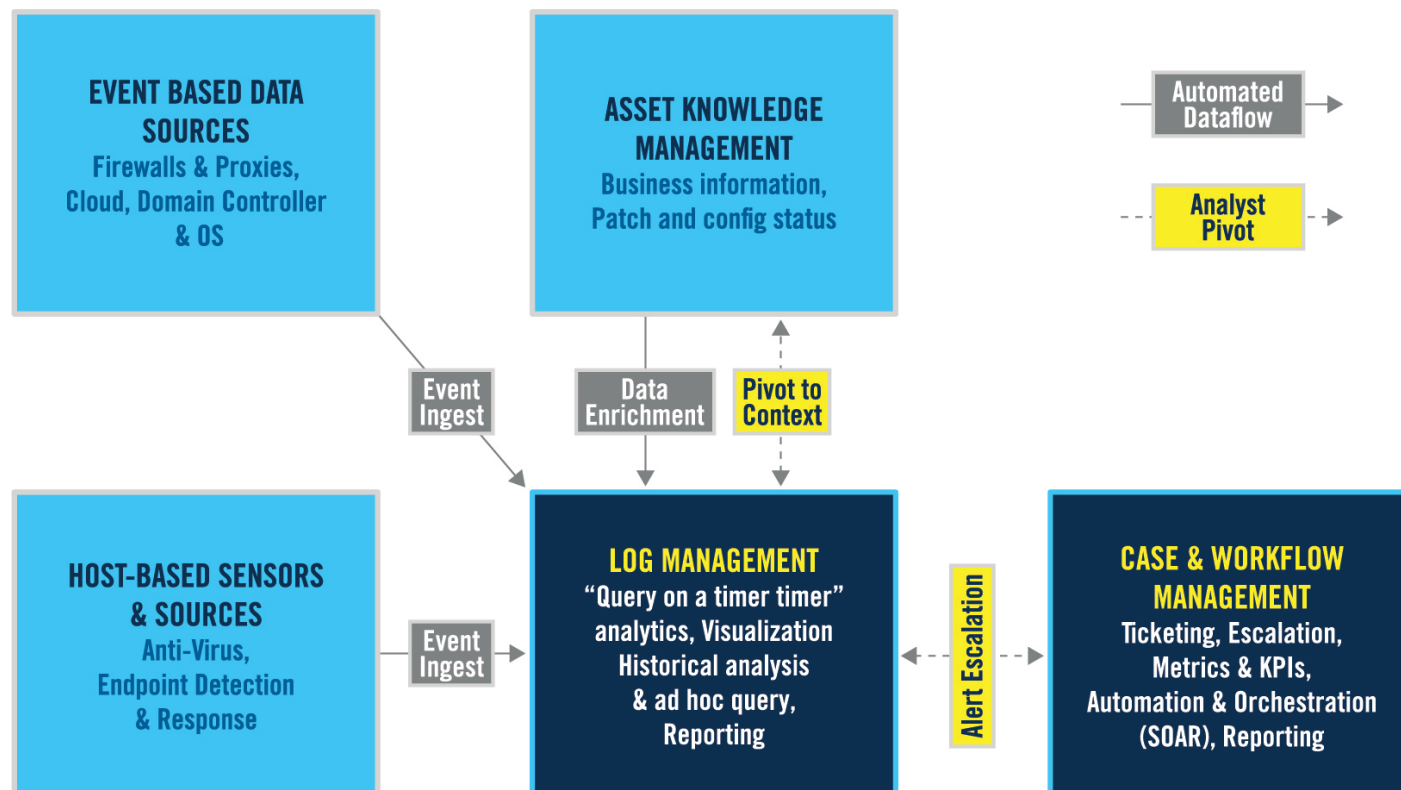
Small and New SOC: EDR Plus Log Management

Many small and young SOC do not have the resources or expertise to stand up a SIEM. Specifically:
Not enough resources to operate and maintain a SIEM.
Not enough data sources to justify running a SIEM.

They have an incumbent or shared log-management solution that gives them access to most of the log data they need and standing “queries on a timer” in the log-management solution fill the handful of detection requirements they have.

Based on their mix of desktop/laptop endpoints and cloud-based services, they choose to satisfy their most important monitoring and analytic use cases with a combination of EDR and log management.

This is a very pragmatic approach for monitoring a small enterprise. In combination with some investments in managed security services, this SOC has satisfied its needs on a very modest budget



Some very large, mature SOC's feel that they have "outgrown" SIEM in part or in totality. They have:
A large shop of over a dozen tool admins and engineers savvy in development and big data

Dozens of disparate data feed types, tens of thousands of nodes to monitor, and well over 10TB/day of data ingestion

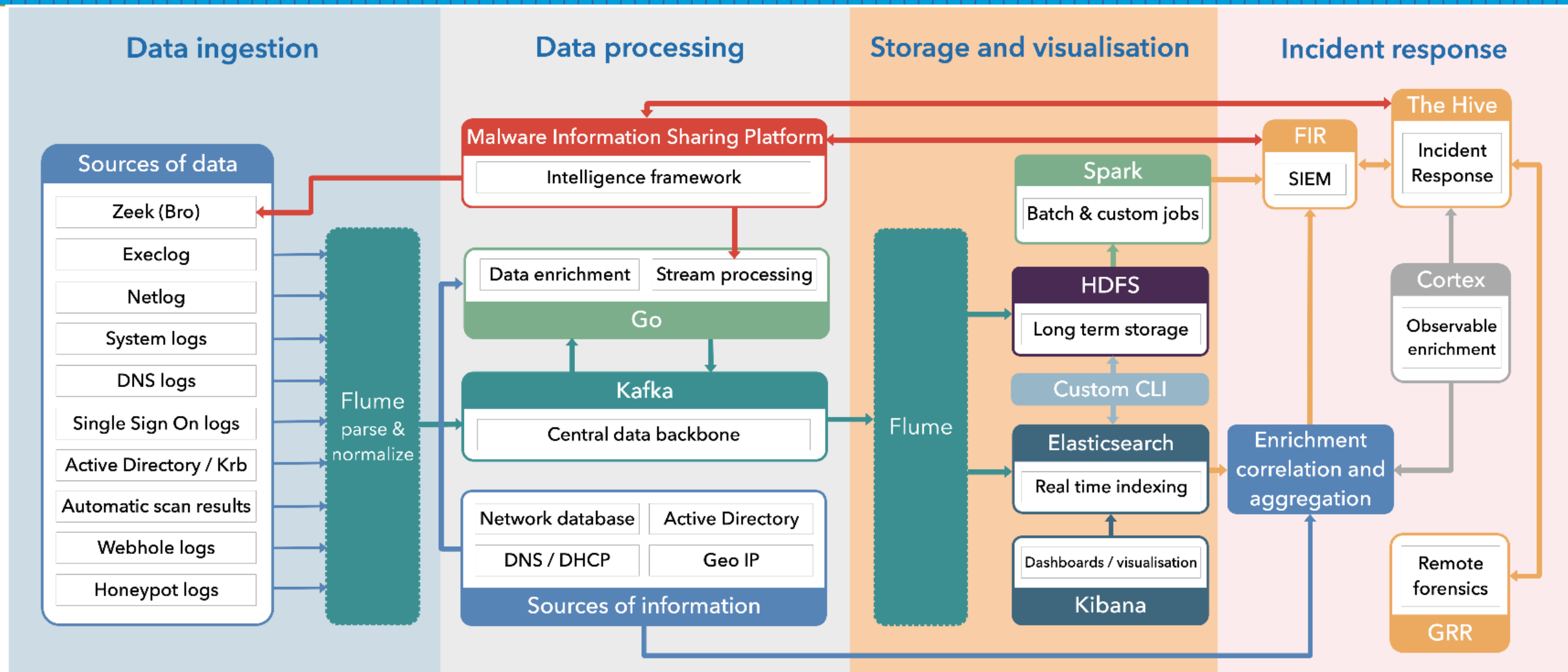
Complex analytic and detection requirements, with dedicated resources for daily detection authoring and tuning, including specialists in intel fusion, hunting, and maybe one or two data scientists

A large user base of SOC analysts and partner system/service owners that have been deputized by the SOC to participate in analytic creation

Experience with commercial SIEMs such that they understand its inner workings and requirements well, and have felt constrained by its limitations, or burdened by its cost model



Log Analysis Platform Reference Model



Security Automation, Orchestration, and Response

SOAR are a set of products and features that, as their name implies, enable the security operations user to quickly and efficiently design and leverage repeatable processes common to the SOC.

Leveraging SOAR, the SOC can:

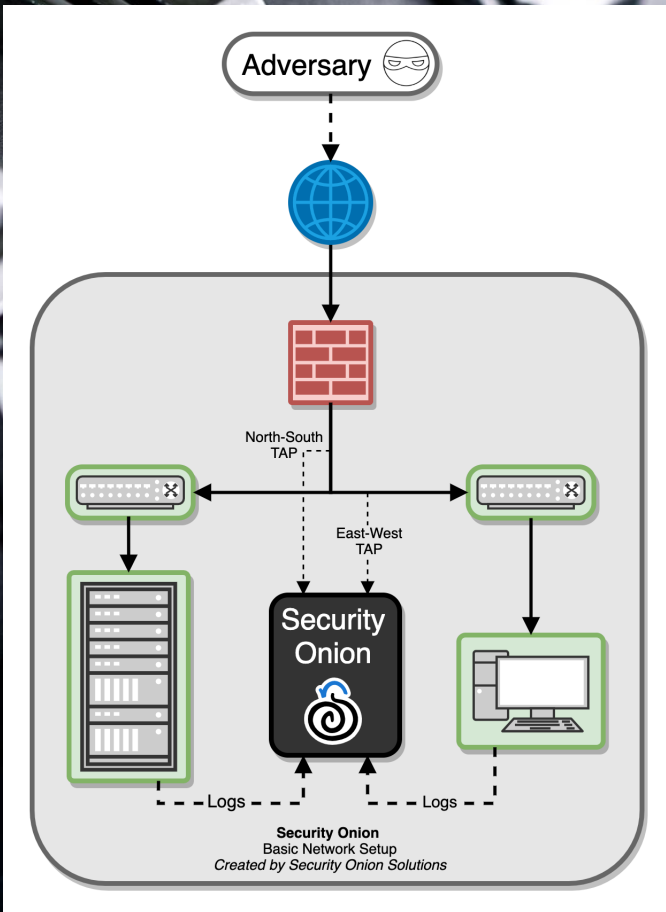
- Gather incidents from disparate systems, presenting a single pane of glass view for alert triage and alert management.
- Enrich and prioritize alerts, integrating threat intelligence and knowledge of entities involved in an alert.
- Execute automated queries or other information gathering activities when an alert fires, like sending a file to malware detonation chamber, gathering vulnerability scanner results, or looking up a user's HR data.
- Run a series of frequently used queries against a log repository.
- Perform routine constituent interactions, such as sending alert details to a constituent, asking for confirmation or repudiation, "was this expected" or "was this really you?"
- Automate response actions like terminating network connections or disabling user accounts

Strumenti x SOC

- Wazuh (Presentazione di Alessandro)
- Security Onion (qualche slide nel seguito)
- Microsoft Security (with Sentinel)
- Cisco SecureX (presentazione CCR mettere link)
- Splunk (qualcuno lo ha provato ?)

Security Onion

- **Network Security Monitoring**
- From a network visibility standpoint, Security Onion seamlessly weaves together intrusion detection, network metadata, full packet capture, file analysis, and intrusion detection honeypots.
- **Intrusion Detection**
- Security Onion generates NIDS (Network Intrusion Detection System) alerts by monitoring your network traffic and looking for specific fingerprints and identifiers that match known malicious, anomalous, or otherwise suspicious traffic. This is signature-based detection so you might say that it's similar to antivirus signatures for the network, but it's a bit deeper and more flexible than that. NIDS alerts are generated by [Suricata](#).



Security Onion

- **Network Metadata**

- Unlike signature-based intrusion detection that looks for specific needles in the haystack of data, network metadata provides you with logs of connections and standard protocols like DNS, HTTP, FTP, SMTP, SSH, and SSL. This provides a real depth and visibility into the context of data and events on your network. Security Onion provides network metadata using your choice of either [Zeek](#) or [Suricata](#).

- **Full Packet Capture**

- Full packet capture is like a video camera for your network, but better because not only can it tell us who came and went, but also exactly where they went and what they brought or took with them (exploit payloads, phishing emails, file exfiltration). It's a crime scene recorder that can tell us a lot about the victim and the white chalk outline of a compromised host on the ground. There is certainly valuable evidence to be found on the victim's body, but evidence at the host can be destroyed or manipulated; the camera doesn't lie, is hard to deceive, and can capture a bullet in transit. Full packet capture is recorded by [Stenographer](#).

Security Onion

- **File Analysis**
 - As [Zeek](#) and [Suricata](#) are monitoring your network traffic, they can extract files transferred across the network. [Strelka](#) can then analyze those files and provide additional metadata.
- **Intrusion Detection Honeypot (IDH)**
 - Security Onion includes an [Intrusion Detection Honeypot](#) node option. This allows you to build a node that mimics common services such as HTTP, FTP, and SSH. Any interaction with these fake services will automatically result in an alert.
- **Enterprise Security Monitoring**
 - In addition to network visibility, Security Onion provides endpoint visibility via agents like [Beats](#), [osquery](#), and [Wazuh](#).
 - For devices like firewalls and routers that don't support the installation of agents, Security Onion can consume standard [Syslog](#).

Security Onion

- **Security Onion Console (SOC)**
- [Security Onion Console \(SOC\)](#) is the first thing you see when you log into Security Onion. It includes our [Alerts](#) interface which allows you to see all of your NIDS alerts from [Suricata](#) and HIDS alerts from [Wazuh](#).

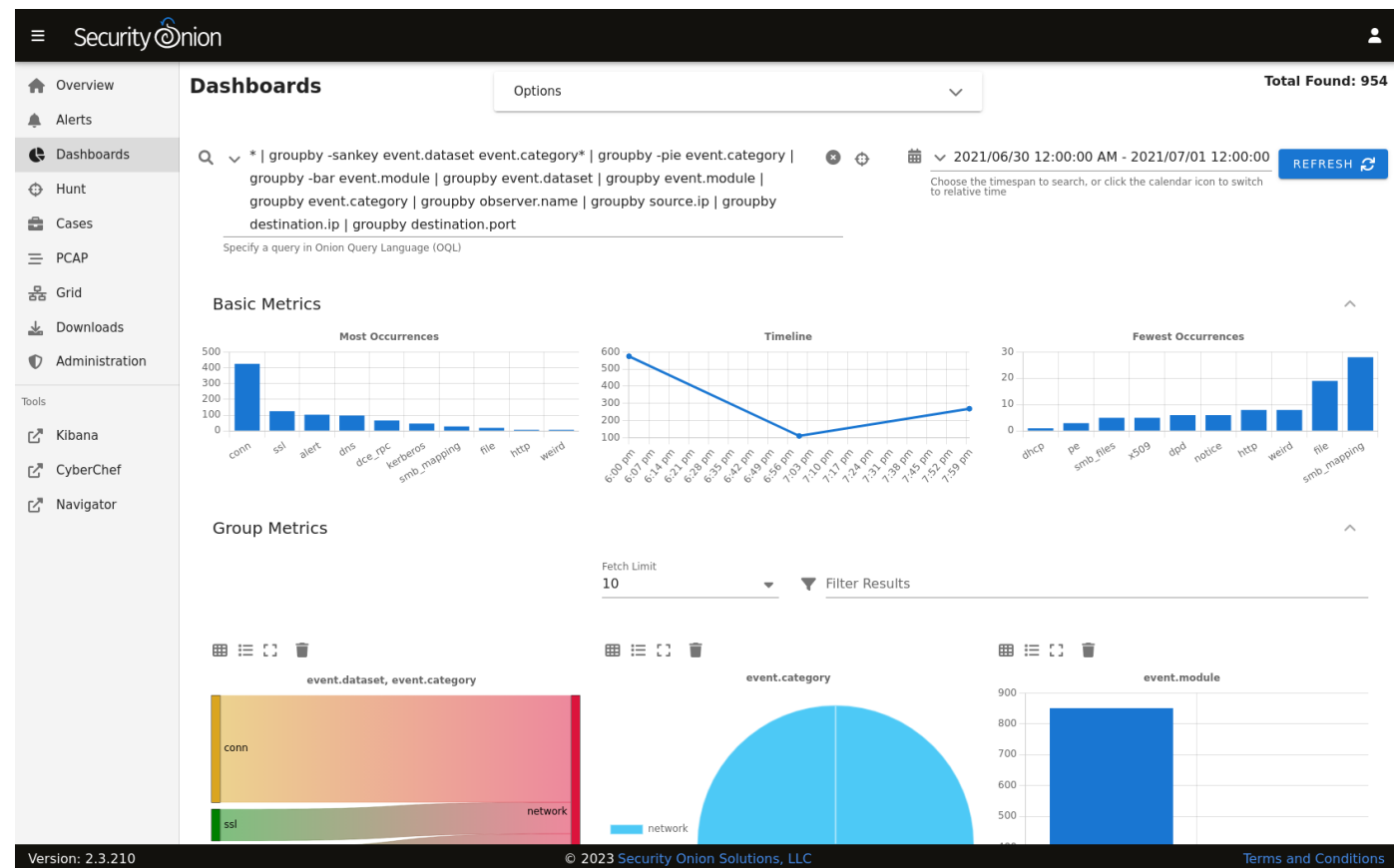
The screenshot displays the Security Onion Alerts interface. The left sidebar contains navigation links: Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration, and Tools (Kibana, CyberChef, Navigator). The main panel shows a list of alerts with the following columns: Count, rule.name, event.module, and event.severity_label. The alerts are sorted by Count in descending order.

Count	rule.name	event.module	event.severity_label
59	ET POLICY OpenSSL Demo CA - Internet Wldgits Pty (O)	suricata	low
4	ET MALWARE Trickbot Checkin Response	suricata	high
4	ET POLICY HTTP traffic on port 443 (POST)	suricata	medium
3	ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1	suricata	medium
3	ET MALWARE VNCStartServer BOT Variant CnC Beacon	suricata	high
3	ET MALWARE VNCStartServer USR Variant CnC Beacon	suricata	high
3	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
2	ET HUNTING curl User-Agent to Dotted Quad	suricata	medium
2	ET INFO Dotted Quad Host DLL Request	suricata	medium
2	ET MALWARE Win32/Trickbot Data Exfiltration M2	suricata	high
2	ET POLICY curl User-Agent Outbound	suricata	medium
1	ET DNS Query to a *.top domain - Likely Hostile	suricata	medium
1	ET EXPLOIT ETHERNALBLUE Probe Vulnerable System Response MS17-010	suricata	high
1	ET EXPLOIT Possible ETHERNALBLUE Probe MS17-010 (Generic Flags)	suricata	high
1	ET HUNTING Suspicious POST with Common Windows Process Names - Possible Process List Exfiltration	suricata	high
1	ET HUNTING Suspicious Windows Commands in POST Body (ipconfig)	suricata	medium
1	ET HUNTING Suspicious Windows Commands in POST Body (net config)	suricata	medium
1	ET HUNTING Suspicious Windows Commands in POST Body (net view)	suricata	medium
1	ET HUNTING Suspicious Windows Commands in POST Body (nltest)	suricata	medium

Version: 2.3.210 © 2023 Security Onion Solutions, LLC Terms and Conditions

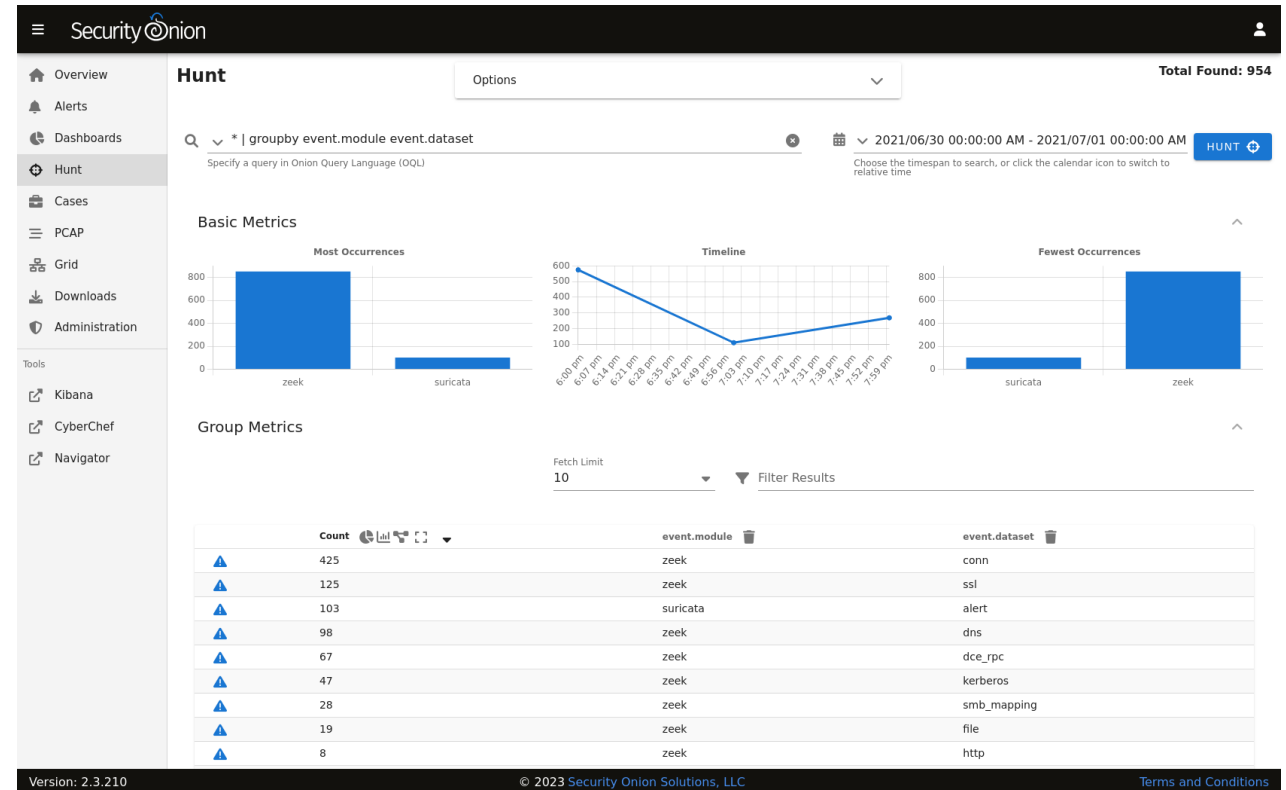
Security Onion

- [Security Onion Console \(SOC\)](#) also includes our [Dashboards](#) interface which gives you a nice overview of not only your NIDS/HIDS alerts but also network metadata logs from [Zeek](#) or [Suricata](#) and any other logs that you may be collecting.



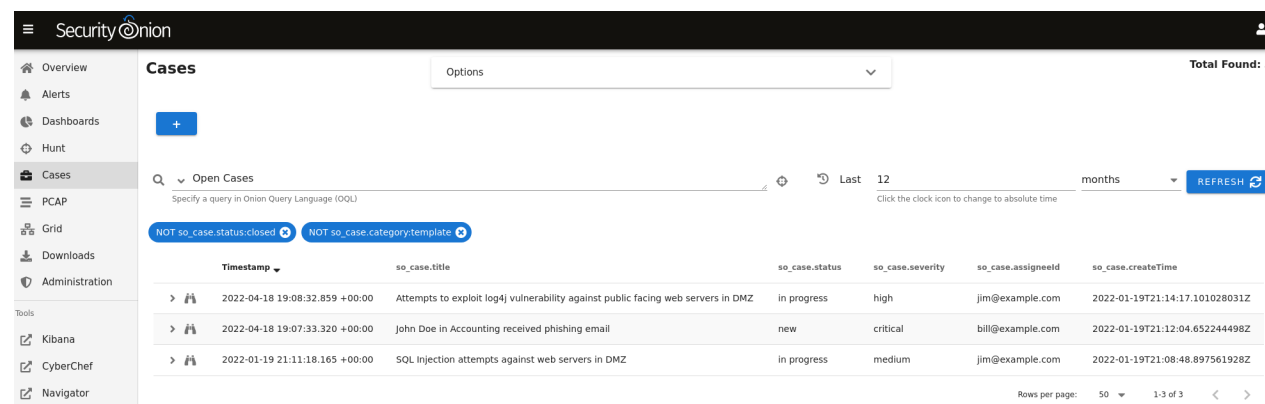
Security Onion

- Hunt is similar to Dashboards but its default queries are more focused on threat hunting.



Security Onion

- [Cases](#) is the case management interface. As you are working in [Alerts](#), [Dashboards](#), or [Hunt](#), you may find alerts or logs that are interesting enough to send to [Cases](#) and create a case. Other analysts can collaborate with you as you work to close that case



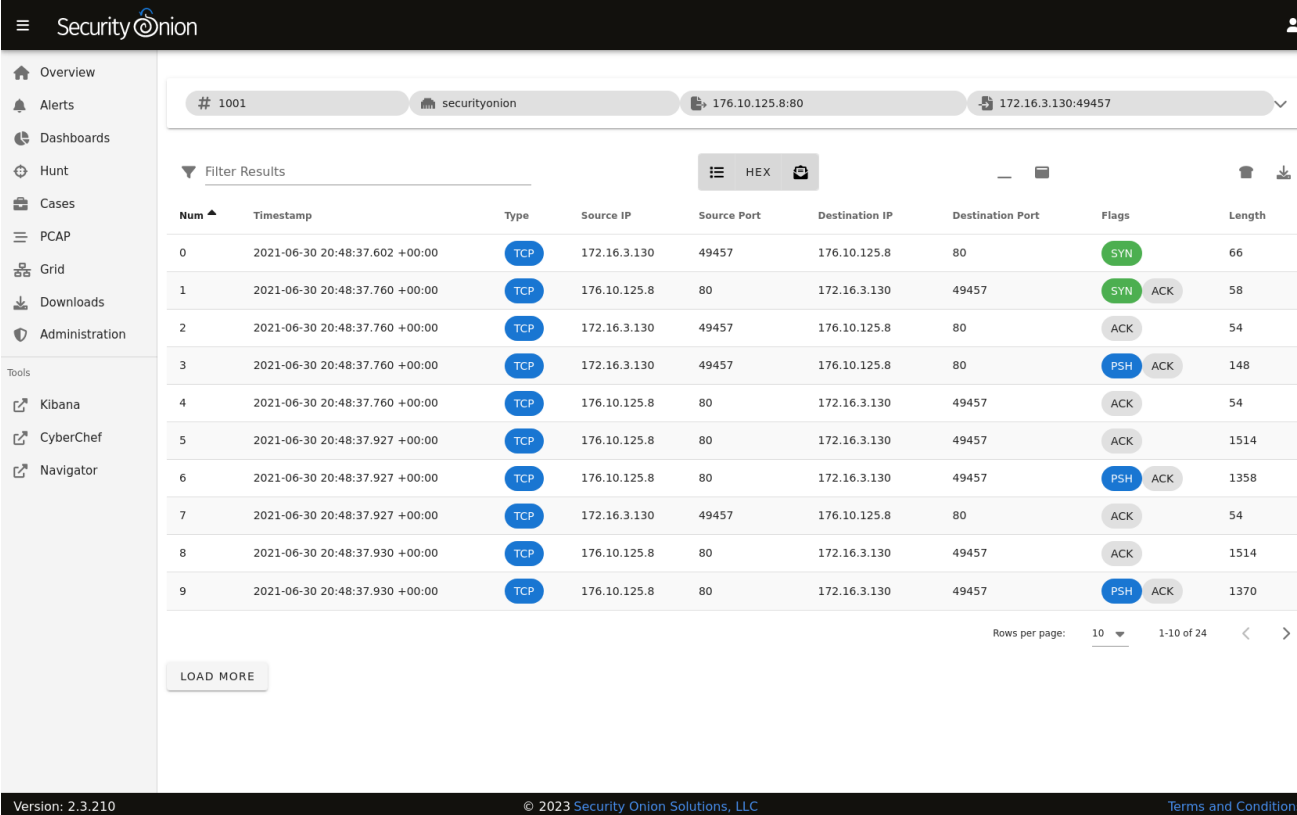
The screenshot shows the Security Onion web interface. On the left is a sidebar with navigation links: Overview, Alerts, Dashboards, Hunt, Cases (selected), PCAP, Grid, Downloads, and Administration. Below these are tool links for Kibana, CyberChef, and Navigator. The main panel is titled 'Cases' and features a search bar with 'Open Cases' selected, a query input field, and buttons for 'Last 12 months' and 'REFRESH'. Below the search bar are two filter buttons: 'NOT so_case.status=closed' and 'NOT so_case.category=template'. A table displays three case entries with columns for Timestamp, so_case.title, so_case.status, so_case.severity, so_case.assigneeid, and so_case.createTime.

Timestamp	so_case.title	so_case.status	so_case.severity	so_case.assigneeid	so_case.createTime
> 2022-04-18 19:08:32.859 +00:00	Attempts to exploit log4j vulnerability against public facing web servers in DMZ	in progress	high	jim@example.com	2022-01-19T21:14:17.101028031Z
> 2022-04-18 19:07:33.320 +00:00	John Doe in Accounting received phishing email	new	critical	bill@example.com	2022-01-19T21:12:04.652244498Z
> 2022-01-19 21:11:18.165 +00:00	SQL Injection attempts against web servers in DMZ	In progress	medium	jim@example.com	2022-01-19T21:08:48.897561928Z

Rows per page: 50 1-3 of 3

Security Onion

- [Security Onion Console \(SOC\)](#) also includes an interface for full packet capture ([PCAP](#)) retrieval.



The screenshot displays the Security Onion Console (SOC) interface. The top navigation bar includes a menu icon, the 'Security Onion' logo, and a user profile icon. The left sidebar contains a list of navigation items: Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration, and a Tools section with Kibana, CyberChef, and Navigator. The main content area shows a filter bar with '# 1001', 'securityonion', and IP addresses '176.10.125.8:80' and '172.16.3.130:49457'. Below the filter bar is a 'Filter Results' section with a 'HEX' button and a table of network packets. The table has columns for Num, Timestamp, Type, Source IP, Source Port, Destination IP, Destination Port, Flags, and Length. The packets are listed in a table with 10 rows. The bottom of the interface shows a 'LOAD MORE' button and a footer with version information, copyright, and terms and conditions.

Num	Timestamp	Type	Source IP	Source Port	Destination IP	Destination Port	Flags	Length
0	2021-06-30 20:48:37.602 +00:00	TCP	172.16.3.130	49457	176.10.125.8	80	SYN	66
1	2021-06-30 20:48:37.760 +00:00	TCP	176.10.125.8	80	172.16.3.130	49457	SYN ACK	58
2	2021-06-30 20:48:37.760 +00:00	TCP	172.16.3.130	49457	176.10.125.8	80	ACK	54
3	2021-06-30 20:48:37.760 +00:00	TCP	172.16.3.130	49457	176.10.125.8	80	PSH ACK	148
4	2021-06-30 20:48:37.760 +00:00	TCP	176.10.125.8	80	172.16.3.130	49457	ACK	54
5	2021-06-30 20:48:37.927 +00:00	TCP	176.10.125.8	80	172.16.3.130	49457	ACK	1514
6	2021-06-30 20:48:37.927 +00:00	TCP	176.10.125.8	80	172.16.3.130	49457	PSH ACK	1358
7	2021-06-30 20:48:37.927 +00:00	TCP	172.16.3.130	49457	176.10.125.8	80	ACK	54
8	2021-06-30 20:48:37.930 +00:00	TCP	176.10.125.8	80	172.16.3.130	49457	ACK	1514
9	2021-06-30 20:48:37.930 +00:00	TCP	176.10.125.8	80	172.16.3.130	49457	PSH ACK	1370

Rows per page: 10 1-10 of 24

Version: 2.3.210 © 2023 Security Onion Solutions, LLC Terms and Conditions

Security Onion

- **CyberChef**
- [CyberChef](#) allows you to decode, decompress, and analyze artifacts. [Alerts](#), [Dashboards](#), [Hunt](#), and [PCAP](#) all allow you to quickly and easily send data to [CyberChef](#) for further analysis.

The screenshot displays the CyberChef web interface (Version 9.55.0, Last build: 2 months ago). The interface is divided into three main sections: Operations, Recipe, and Input/Output.

Operations: A sidebar on the left lists various operations including Search..., Favourites, To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic, Data format, Encryption / Encoding, Public Key, Arithmetic / Logic, Networking, Language, Utils, Date / Time, Extractors, Compression, and Hashing.

Recipe: The central area shows a sequence of operations:

- From Hexdump:** Converts hex data to a string.
- Strip HTTP headers:** Removes HTTP headers from the string.
- Strings:** Extracts strings from the remaining data. Options include Encoding (Single byte), Minimum length (9), and Match (Alphanumeric).

 At the bottom of the recipe, there are checkboxes for "Display total", "Sort", and "Unique".

Input: The top right section shows the raw hex input data, which is a hex dump of an HTTP GET request. Metadata includes length: 61132 and lines: 828.

Output: The bottom right section shows the result of the recipe, which is the decoded text of the HTTP request. Metadata includes time: 7ms, length: 99, and lines: 5. The output text includes headers like "GET /105.dll HTTP/1.1" and "Keep-Alive: 60" and a body containing "This is a Windows NT windowed dynamic link library".

At the bottom of the interface, there is a "BAKE!" button and an "Auto Bake" checkbox.

Security Onion

- Playbook allows you to create a Detection Playbook, which itself consists of individual plays. These plays are fully self-contained and describe the different aspects around the particular detection strategy.

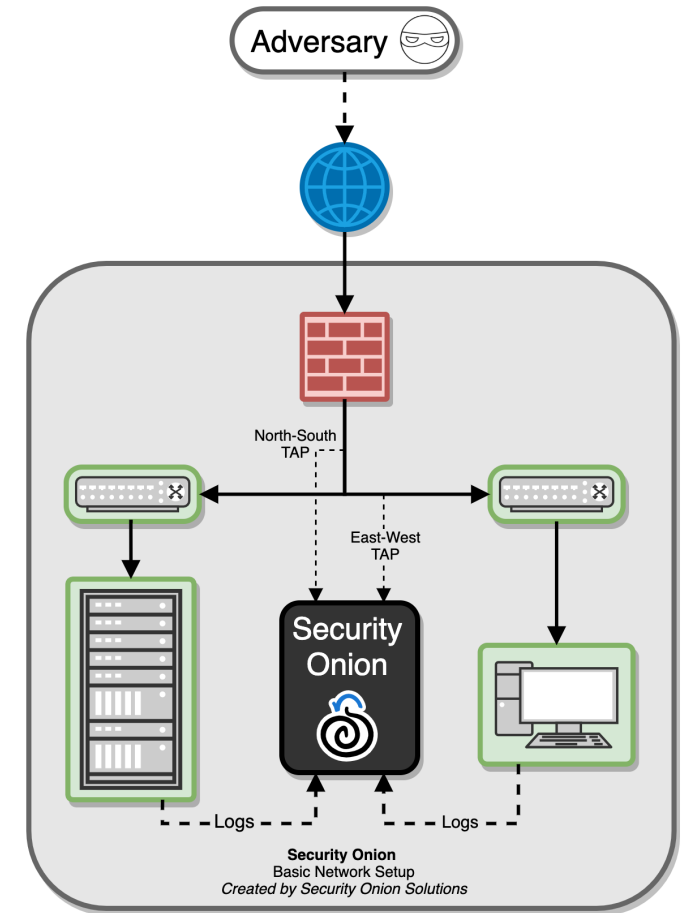
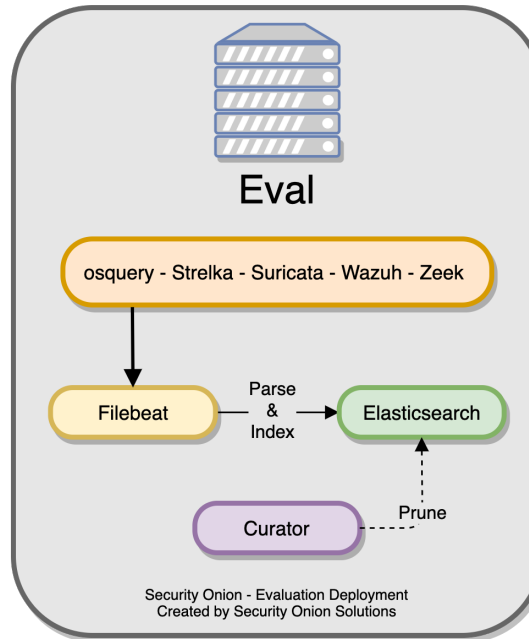
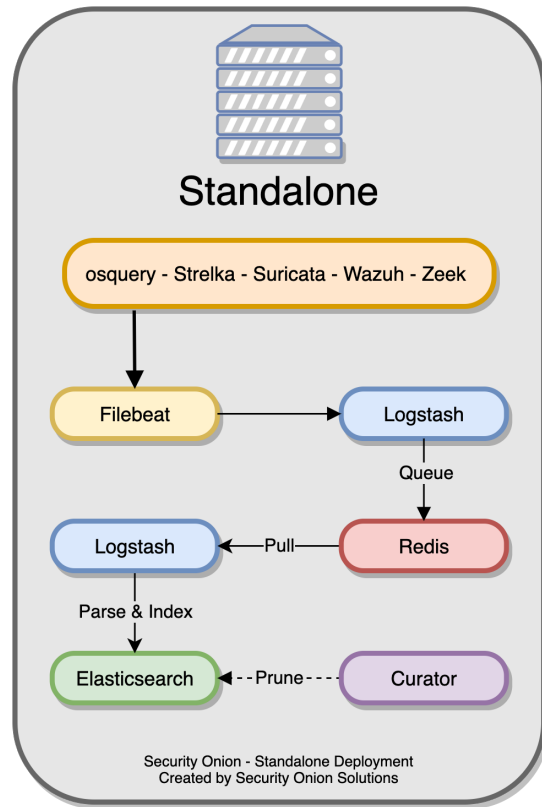
The screenshot shows the 'DETECTION PLAYBOOKS' interface in Security Onion. The top navigation bar includes 'Home', 'Activity', 'Playbook', and 'Sigma Editor'. The 'Playbook' tab is active. Below the navigation bar, there's a 'Playbook' section with filters (Status: open, Add filter) and a table of plays. The table has columns for Status, Level, Playbook, Product, Title, and Updated. The table lists 25 plays, mostly in 'Draft' status with 'medium' or 'high' levels. The right sidebar shows 'Custom queries' with links to 'All Plays', 'Disabled Plays', 'Draft Plays', 'Playbook - Community Sigma', and 'Playbook - Internal'. At the bottom, there's a pagination bar showing '1' of 13 items and a footer with 'Also available in: Atom | CSV | PDF'.

	Status	Level	Playbook	Product	Title	Updated
623	Draft	medium	community	windows	Harvesting of Wifi Credentials Using netsh.exe	05/13/2020 02:07 PM
622	Draft	medium	community	windows	Advanced IP Scanner	05/13/2020 02:07 PM
621	Draft	high	imported	windows	Whoami Execution	05/13/2020 02:05 PM
620	Draft	medium	imported	osquery	New Sensitive Shared Resource	05/13/2020 01:30 PM
618	Inactive	medium	community	windows	XSL Script Processing	05/03/2020 10:00 AM
617	Draft	high	community	windows	Wreset UAC Bypass	05/01/2020 08:58 PM
616	Draft	high	community	windows	Microsoft Workflow Compiler	05/01/2020 08:57 PM
615	Draft	critical	community	windows	Wmiprvse Spawning Process	05/01/2020 08:57 PM
614	Draft	high	community	windows	WMI Spawning Windows PowerShell	05/01/2020 08:57 PM
613	Draft	high	community	windows	WMI Persistence - Script Event Consumer	05/01/2020 08:57 PM
612	Draft	critical	community	windows	WMI Backdoor Exchange Transport Agent	05/01/2020 08:57 PM
611	Draft	high	community	windows	Windows 10 Scheduled Task SandboxEscaper 0-day	05/01/2020 08:57 PM
610	Draft	high	community	windows	Run Whoami as SYSTEM	05/01/2020 08:57 PM
609	Draft	high	community	windows	Shells Spawned by Web Servers	05/01/2020 08:57 PM
608	Draft	high	community	windows	Webshell Detection With Command Line Keywords	05/01/2020 08:57 PM
607	Draft	medium	community	windows	Java Running with Remote Debugging	05/01/2020 08:57 PM
606	Draft	high	community	windows	Possible Privilege Escalation via Weak Service Permissions	05/01/2020 08:57 PM
605	Draft	high	community	windows	Bypass UAC via WReset.exe	05/01/2020 08:57 PM
604	Draft	high	community	windows	Bypass UAC via Fodhelper.exe	05/01/2020 08:57 PM
603	Draft	high	community	windows	Bypass UAC via CMSTP	05/01/2020 08:57 PM
602	Draft	medium	community	windows	Domain Trust Discovery	05/01/2020 08:57 PM
601	Draft	high	community	windows	Terminal Service Process Spawn	05/01/2020 08:57 PM
600	Draft	high	community	windows	Tasks Folder Evasion	05/01/2020 08:57 PM
599	Draft	medium	community	windows	Tap Installer Execution	05/01/2020 08:57 PM
598	Draft	high	community	windows	System File Execution Location Anomaly	05/01/2020 08:57 PM

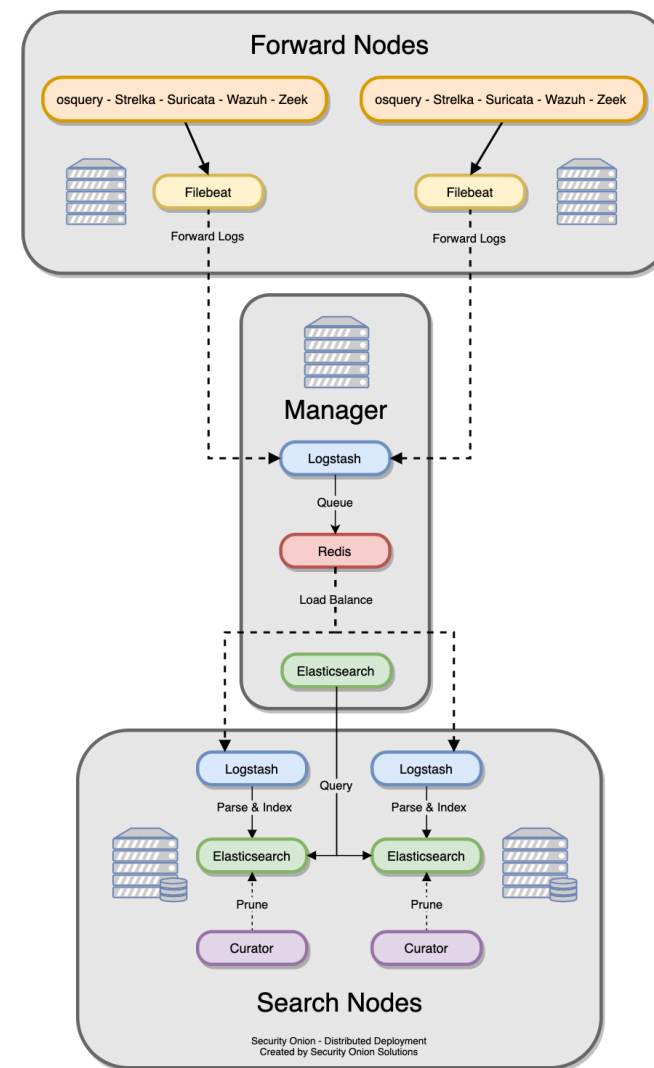
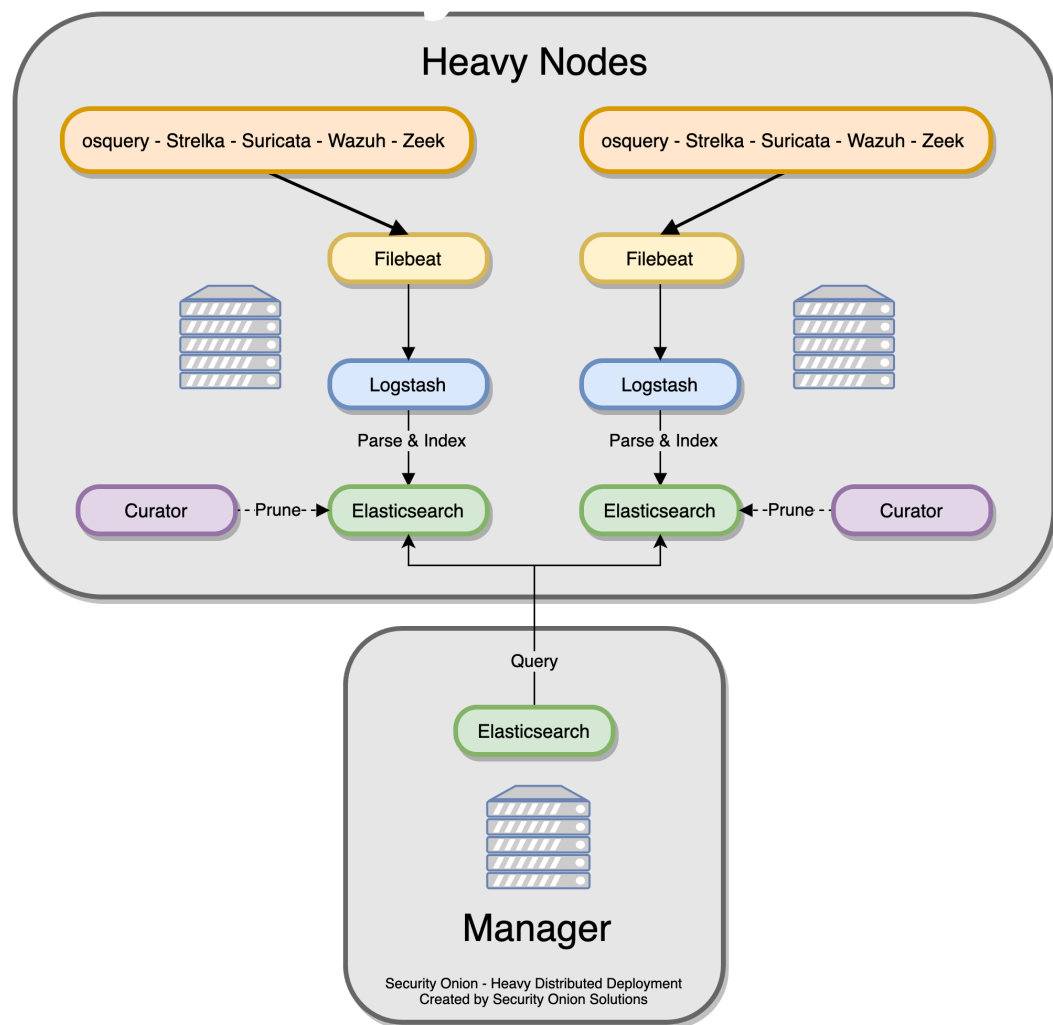
Security Onion

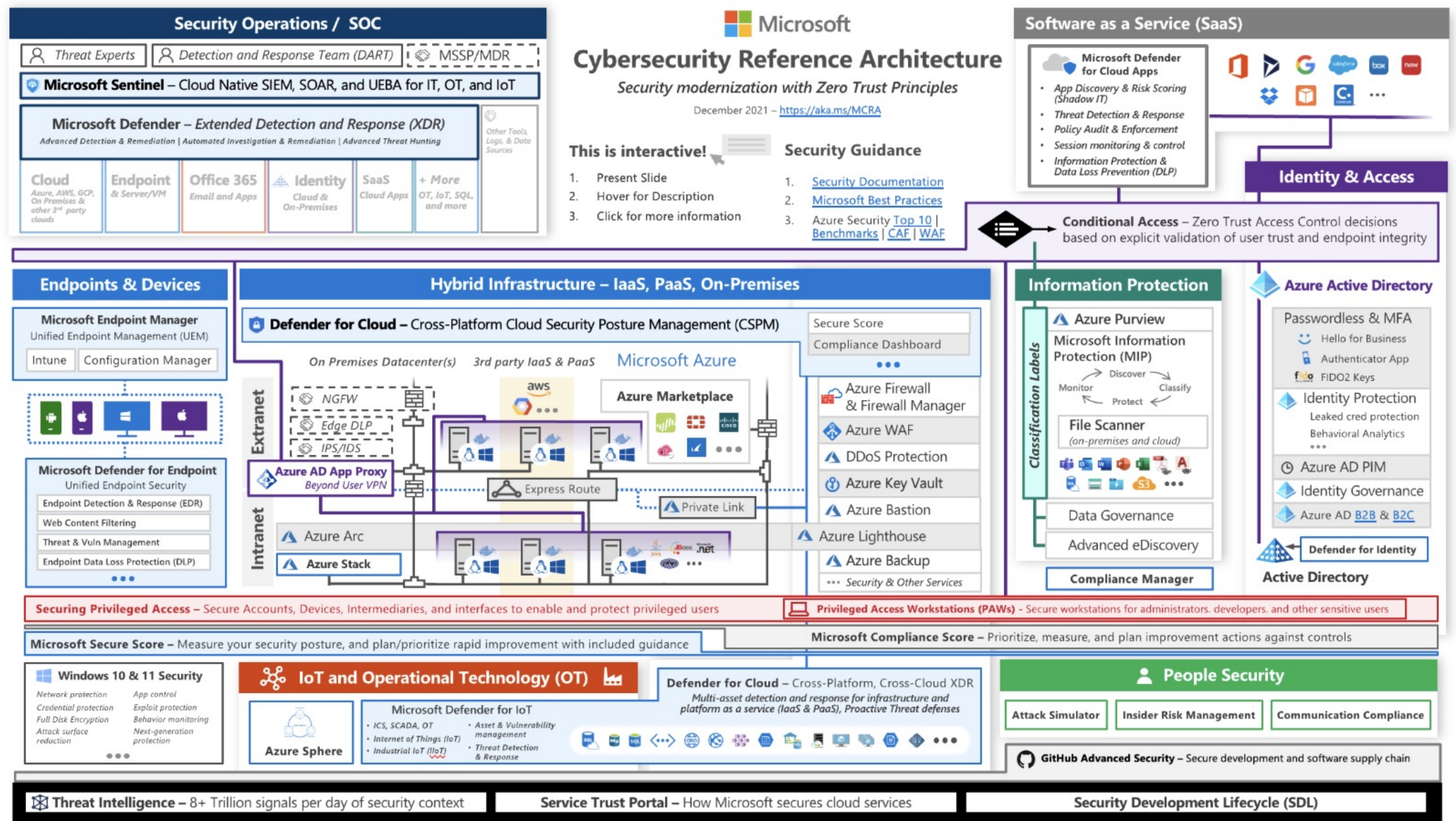
- All of these analysis tools work together to provide efficient and comprehensive analysis capabilities. For example, herès one potential workflow:
- Go to the [Alerts](#) page and review any unacknowledged alerts.
- Review [Dashboards](#) for anything that looks suspicious.
- Once you've found something that you want to investigate, you might want to pivot to [Hunt](#) to expand your search and look for additional logs relating to the source and destination IP addresses.
- If any of those alerts or logs look interesting, you might want to pivot to [PCAP](#) to review the full packet capture for the entire stream.
- Depending on what you see in the stream, you might want to send it to [CyberChef](#) for further analysis and decoding.
- Escalate alerts and logs to [Cases](#) and document any observables. Pivot to [Hunt](#) to cast a wider net for those observables.
- Develop a play in [Playbook](#) that will automatically alert on observables moving forward and update your coverage in [ATT&CK Navigator](#).
- Finally, return to [Cases](#) and document the entire investigation and close the case.

Security Onion



Security Onion





R&D: infrastruttura, piano attività

- Scelta del modello (distribuito,centralizzato,federato)
- Scelta delle sonde (Log, Host, Rete, FW, App)
- Scelta degli strumenti (SIEM,SOAR)
- Implementazione prototipo piattaforma (😊)

R&D: infrastruttura, piano attività EDR

- Dispiegamento piattaforma EDR (Microsoft Security)
- Configurazioni console multisito
- Onboarding endpoint
- Integrazione con MISP
- Integrazione con CSIRT Tool
- Policy e Formazione

THE END



Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

Fonti (la prima soprattutto)

- <https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf>
- <https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf>
- <https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework>
- <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc>
- https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf
- https://english.ncsc.nl/binaries/ncsc-en/documenten/factsheets/2019/juni/01/factsheet-building-a-soc-start-small/Factsheet_Building_a_SOC_start_small.pdf