

## Strategic Efficiency Consortium Industrial Security Intelligence Data Platform Services

### CAPABILITY LIST (Extract)

Security Intelligence Data + Security Threat Intelligence Data + Industrial Security Intelligence News Data + Security Threat Intelligence Data Feeds + Intelligence News Data Services

#### Security Intelligence Data Features

- Industrial Security Intelligence Data Services
- Industrial Security Intelligence News Data Services
- Strategic Competitive Industrial Security Intelligence News Data Services
- Security Threat Intelligence Data related to Business Risk Intelligence
- Primary Security Threat Intelligence Data Feeds
- Foundation Open Source Intelligence OSINT Data Service

#### Security Intelligence Data Service Platform

##### Collaborative Security Intelligence Ecosystem

11 Partners | 5 Technical Research Work Groups | 2 Research and Development Initiatives | Canada + USA Market Focus | +3 million data sources | +500k data updates processed daily | +900 Content Channels in Development

#### Security Intelligence Data Service Platform

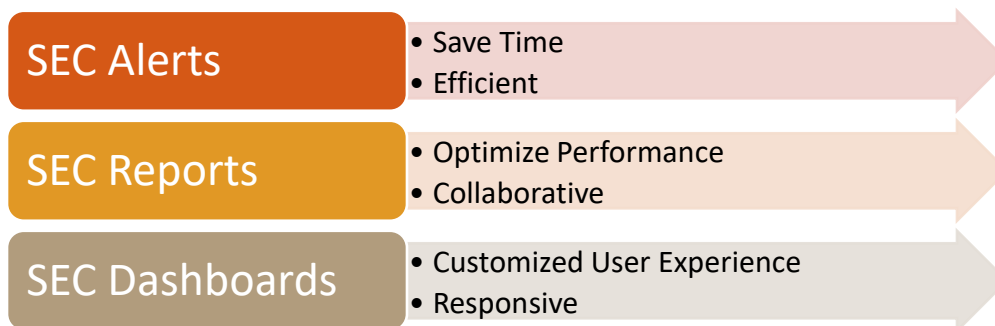
Innovative | Unique | Efficient

#### All in One Security Intelligence Data Solution

Alerts | Reports | Dashboards

#### User Client Driven Security Intelligence Data

Available | Reactive | Responsive | Collaborative



## **Comprehensive Scalable Monitoring Security Intelligence Data Platform**

Optimize Performance | Save Time

- This platform has completed version 2.25; completed upgrades and revisions developing and migrating to Intelligence version 4.95 and planned upgrades and revisions into Learning version 9.45. We currently manage +3 million data sources and process +500k daily data updates; data sources are planned for expansion to +75 million data sources.

## **Accessible Ergonomic Security Intelligence Data Platform**

Optimal | Customized User Experience | Responsiveness

- Continuous data information monitoring and detection using over 3 million data sources and processing over 500k daily data updates
- Fully comprehensive and scalable monitoring platform to meet specific security intelligence data demands.
- User support from our team of experts; made up of research and security industry experts with complementary skills, with the common goal of enhancing your Security Intelligence performance.
- A community of users and partners.

## **Foundation Open Source Intelligence OSINT Service designed to complement:**

- Security Information and Event Management SIEM or Security Information Management SIM
- Cyber Threat Intelligence CIT Design

Open Source Intelligence OSINT structured to raise client awareness.

Our data management process includes four key critical elements:

- Research and Discovery – building, expanding and uncovering data sources each day driven to deepen expertise, solution, problem and archival knowledge.
- Content Selectivity – all content is hand selected by our intelligence editors, there is careful discrimination between good and bad sources, relevant sources selection and categorization is a critical part of the unique value of the process.
- Content Structure and Refining –important refining, categorization and guidance of data into client specific focused channels, headlines, search reports and reports.
- Content Delivery – timeliness, ease of access, readability, flexibility, time efficient, easily understandable, client friendly delivery formats: high standard Content and high standard Format.

## **Content Context:** Our service is designed upon contextual intelligence data versus volume data:

- identification, collection, and enrichment of relevant data and information
- facilitate client output of analysis based on identification, collection, and enrichment of relevant data and information.
- our service provides the relevant raw data and information needed and processed by client users
- focus on relevant data directly attributable and contributable to business goals
- focus on relevant data that; organically feeds and builds a threat intelligence and defensive architecture program designed to reduce operational risk focused on specific aspects of security that are clearly linked to the markers used to measure the client's unique cyber risks

## **Content Workflow:** Threat Intelligence Data Feeds: Threat Intelligence Platform Features:

- analyzes over 3,00,000 web sources and automatically extracts emerging trends and indicators which are then presented as segmented headlines, subjects, channels, searches, reports.
- combines thousands of feeds into a single location.
- receives alerts in real time.
- normalizes feed data into user based-driven categories and evolved based on user driven threat context
- data feeds that are relevant, fully contextualized, and actionable
- tools for client to produce their own strategic intelligence feeds and categories
- customizable Security Threat Intelligence Data Feeds
- scheduling; Data feeds set up with delivery mechanism for specific types of data at pre-determined intervals.
- single, at-a-glance communication messages
- Industrial Information Security Headlines formats
- Top Trending Industrial Information Security News Stories formats
- External Threat Intelligence Data subscriptions; intelligence that an organization acquires from outside itself

## **Content Delivery:** Threat Intelligence Data Feeds: Threat Intelligence Platform Formats: Data feed sources can be further separated into subgroups and delivered in the following ways:

- Emails delivered at an interval, such as hourly, daily or weekly
- Subscriptions that provide lists of indicators, also delivered at intervals in various formats, such as JSON or CSV
- Scripts that utilize APIs to extract information from a data source, such as a database or website
- Reports and White Papers
- Attacker and attack tactics, techniques and procedures Reports
- Data Feeds formats widely used by information security organizations

### SEC Content Research and Discovery

- building, expanding and uncovering data sources each day driven to deepen expertise, solution, problem and archival knowledge

### SEC Content Selectivity

- all content is hand selected by our intelligence editors, relevant sources selection and categorization is a critical part of the unique value

### SEC Content Structure and Refining

- important refining, categorization and guidance of data into client specific focused channels, headlines, search reports and reports

### SEC Content Delivery

- timeliness, ease of access, readability, flexibility, time efficient, easily understandable, client friendly delivery formats: high standard content and high standard format

### SEC Content Context

- contextual intelligence data versus volume data

## Strategic Efficiency Consortium Industrial Security Intelligence Data Platform Services

### CAPABILITY LIST (Extract)

#### Security Intelligence Data + Security Threat Intelligence Data + Industrial Security Intelligence News Data + Security Threat Intelligence Data Feeds + Intelligence News Data Services

#### Security Intelligence Data Service Platform - Client Aims-Objectives-Deliverables

Security Threat Intelligence data must improve business risk profiles and our client's ability to manage risk -- not just in cybersecurity operations, but as the overlap between the cyber and physical threat landscapes expands, our threat intelligence must also overlap across client's physical security and supply chain risk, among others -- our threat intelligence data must enable client to make better business decisions.

Security Threat Intelligence Data is a first step that helps prioritize security actions, facilitate better client understanding of short and medium trends and solutions, and broaden client perspective to frame or snapshot industrial security markets.

We have designed and built this service to deliver well defined deliverables into critical intelligence demands of our client. These critical intelligence demands are across Technology Information Data Positioning Planning and Execution.

#### Client Intelligence Technology Information Data

- client understanding of Intelligence Technology and Intelligence Information and Intelligence Data
- client leverage of technology to process information relating to aspects of their operational environments
- client use of information to contribute to their decision-making process; provide reasoned insight into future environments; increase information utility

#### Client Intelligence Positioning

- client capability in anticipation and prediction of future environments and better defining differences in available courses of action
- client depth of quantitative analysis and qualitative judgment and competing interpretation
- client continuous examination of their intelligence needs
- client definitions of goals, frameworks, quantifiable outputs and objectives
- client focus on actionable intelligence creation

#### Client Intelligence Planning Execution

- client types of intelligence -- Warning; Current; General; Target; Scientific Technical; Counterintelligence; Estimative; Identity
- client levels of intelligence -- Strategic; Operational; Tactical
- client principles of intelligence -- Perspective; Synchronization; Integrity; Effort Singularity; Prioritization; Excellence; Prediction; Agility; Collaboration; Fusion

## Client Data Usage and Application

The aim of our service is to make sure our client is always as informed as possible:

- Our data service is designed to address key aspects and demands of Industrial Business Risk Intelligence IBRI, Industrial Business Risk Intelligence broadens the requirements and scope of cyber intelligence beyond threat detection to provide relevant context to business units not traditionally afforded the benefits of intelligence.
- Our security threat data intelligence is about improving business decisions, and clients building their frameworks around that objective
- Our security threat intelligence data service has the stated purpose to inform action.
- Our intelligence data service is focused on designing, creating, integrating and calibrating tools capable of performing vital intelligence functions

Our data is designed to multi-dimensionally increase client:

- market understanding
- sector understanding
- competitor understanding
- technology understanding
- security solution understanding
- threat problems
- threat solutions

Client users and analysts use our data feeds to:

- identify trends;
- educate employees and customers;
- study attacker tactics,
- learn tactics, techniques and procedures TTP;
- create defensive architecture recommendations

Clients focuses on:

- developing or procuring the systems needed to automate the identification, collection, and enrichment of threat data and information.
- creating and maintaining tools needed to produce operational threat intelligence.
- their attentions on the production of highly targeted and valuable strategic intelligence.

Data is client organization relevant and focused, sharing threat intelligence within client's organization:

- helps spread awareness of security issues among non-technical audiences.
- greatly improves ability to implement proactive and cohesive security and defense mechanisms,
- makes use of the collective knowledge and experience of your various technical and non-technical teams

## From Client Data Consumption > to Client Action

The value of this service is best realized only when the client implements the data knowledge provided into action; its tools, including firewalls, SIEM systems, endpoint agents and network-based security technologies. The service must be consumed and acted upon by the receiving organization to extract its value.

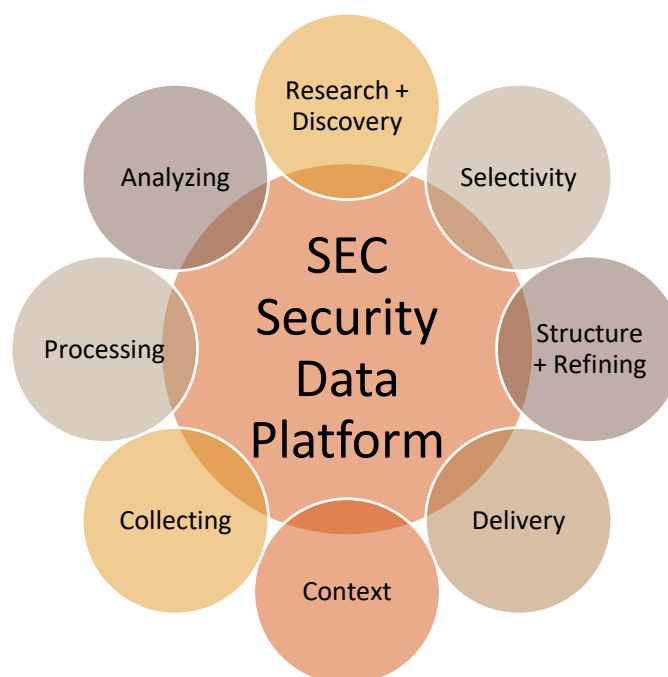
We work together to enhance client team's current cyber intelligence collection and processing capabilities, focus data and data segmentation towards information needs that are mission critical to the organization, and facilitate these needs into structured, client driven, user evolved intelligence requirements.

## Client Driven Security Threat Intelligence Data Services

After much consultation, evaluation and measurement of clients' demand and approach to Threat Intelligence, we have specifically designed and built this Security Threat Intelligence Data Service to deliver well-defined deliverables into the initial critical intelligence demands of our client; deliverables that can benchmark, define, grow and evolve successful client adaptability to the everchanging demands of Competitive Security Threat Intelligence.

Although we have developed a data and information platform comprising +500 channels of data to immediately address short and medium-term Security Threat Intelligence demands, this platform content is also designed to deliver medium and long term; a deeper, strategic and actionable change in the client to increase capability and competence in:

- client understanding of Intelligence Technology and Intelligence Information and Intelligence Data
- client leverage of technology to process information relating to aspects of their operational environments
- client usage of information to contribute to their decision-making process; and usage of information to provide reasoned insight into future environments;
- client improvements in information utilization
- client capability in anticipation and prediction of future environments and better defining differences in available courses of action
- client depth of quantitative analysis and qualitative judgment and competing interpretation
- client continuous examination of their intelligence needs
- client definitions of goals, frameworks, quantifiable outputs and objectives
- client focus on actionable intelligence creation
- enhancing client types of intelligence – Warning; Current; General; Target; Scientific Technical; Counterintelligence; Estimative; Identity
- growing client levels of intelligence – Strategic; Operational; Tactical
- developing client principles of intelligence – Perspective; Synchronization; Integrity; Effort Singularity; Prioritization; Excellence; Prediction; Agility; Collaboration; Fusion



## Strategic Efficiency Consortium Industrial Security Intelligence Data Platform Services

### CAPABILITY LIST (Extract)

#### Security Intelligence Data + Security Threat Intelligence Data + Industrial Security Intelligence News Data + Security Threat Intelligence Data Feeds + Intelligence News Data Services

#### Security Intelligence Thinking Definition Terms Concepts Details

*What Is Security Threat Intelligence? Security Threat Intelligence: What It Is, and How to Use It Effectively?*  
*Security Threat Intelligence is the process of acquiring, via multiple sources, knowledge about threats to an environment: “evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard....”*

#### Intelligence: Technology Information and Data

- Technology enables access to, in near-real-time, very large amounts of information relating to aspects of the operational environment (OE)
- Information is of greatest value when it contributes to the decision-making process by providing reasoned insight into future conditions or situations.
- Raw data by itself has relatively limited utility. However, when data is collected and processed into an intelligible form, it becomes information and gains greater utility.

#### Intelligence

- Ultimately, intelligence has critical features that distinguish it from information.
- Intelligence allows anticipation or prediction of future situations and circumstances, and it informs decisions by illuminating the differences in available courses of action (COAs).
- Intelligence is not an exact science; intelligence analysts will have some uncertainty as they assess the OE.
- Intelligence, as the synthesis of quantitative analysis and qualitative judgment is subject to competing interpretation.
- Intelligence includes the organizations, capabilities, and processes involved in the collection, processing, exploitation, analysis, and dissemination of information or finished intelligence. Intelligence, however, is not an end in itself. To increase the operational relevance of intelligence, intelligence planners and managers should anticipate consumer needs. Thus, an examination of whether intelligence is effective or influential not only depends on the intelligence organizations, processes, and products, but must also examine users’ intelligence needs.
- Intelligence products provide users with the information that has been collected and analyzed based on their requirements. It is important to remember that because the OE is dynamic, intelligence is a continuous activity.

## Intelligence - Goals Before Data

- What systems, data, and other digital assets must be protected?
- How do you anticipate threat intelligence will help protect those assets?
- With which specific tactics are you expecting intelligence to help?

## Intelligence - Framework Tools

- Collecting: Ingesting threat data from the right sources.
- Processing: Turning the data into useful information.
- Analyzing: Turning the information into actionable intelligence.

## Intelligence - Defined

- Threat intelligence is the output of analysis based on identification, collection, and enrichment of relevant data and information.
- Always keep quantifiable business objectives in mind and avoid producing intelligence “just in case.”
- Threat intelligence falls into two categories. Operational intelligence is produced by computers, whereas strategic intelligence is produced by human analysts.
- The two types of threat intelligence are heavily interdependent, and both rely on a skilled and experienced human analyst to develop and maintain them.

## Intelligence Planning

Intelligence Planning (IP) occurs continuously while intelligence collection and production plans are updated as a result of previous requirements being satisfied and new requirements being identified.

A conceptual model of the intelligence process

### Planning and Direction.

Definition: Planning and Direction. In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, issuance of orders and requests to information collection agencies.

IP and direction are best understood as the development of intelligence plans and the continuous management of their execution.

Planning and direction activities include, but are not limited to:

- the identification and prioritization of intelligence requirements;
- the development of concepts of intelligence operations and architectures required to support the action or task;
- tasking subordinate intelligence elements for the collection of information or the production of finished intelligence;
- submitting requests for additional capabilities to higher review;
- and submitting requests for collection, exploitation, or all-source production support to external, supporting intelligence entities.

SEC Intelligence

Strategic

Operational

Tactical



## Intelligence Requirements and Information Requirements Planning

### Categories of Intelligence Products:

Warning; Current; General; Target; Scientific Technical; Counterintelligence; Estimative; Identity

- Warning intelligence
- Current intelligence
- General intelligence
- Target intelligence
- Scientific and technical intelligence
- Counterintelligence
- Estimative intelligence
- Identity intelligence

## Intelligence Requirements and Information Requirements Planning

### Levels of Intelligence: Strategic; Operational; Tactical

#### Strategic - Senior Leaders; Managers

- Assist in developing strategy and policy.
- Monitor the international or global situation.
- Assist in developing plans.
- Assist in determining major systems and structure requirements.
- Support the conduct of strategic operations.

#### Operational - Senior Leaders; Managers

- Focus on capabilities and intentions of threats and vulnerabilities
- Analyze the operational environment.
- Identify adversary centers of gravity and critical vulnerabilities.
- Monitor events in the areas of interest.

#### Tactical - Managers

- Support the planning and conduct of joint campaigns or efforts.
- Support planning and the execution of attacks, defense, engagements, and other joint force activities.
- Provide information on imminent threats and changes in the operational environment.
- Provide obstacle intelligence.

## Intelligence Requirements and Information Requirements Planning

### Principles of Joint Intelligence: Perspective; Synchronization; Integrity; Effort Singularity; Prioritization; Excellence; Prediction; Agility; Collaboration; Fusion

- Perspective (Think like the adversary.)
- Synchronization (Synchronize intelligence with plans and operations.)
- Integrity (Remain intellectually honest.)
- Unity of Effort (Cooperate to achieve a common end state.)
- Prioritization (Prioritize requirements based on authoritative guidance.)
- Excellence (Strive to achieve the highest standards of quality.)
- Prediction (Accept the risk of predicting adversary intentions.)
- Agility (Remain flexible and adapt to changing situations.)
- Collaboration (Leverage expertise of diverse analytic resources.)
- Fusion (Exploit all sources of information and intelligence.)

## Intelligence Requirements and Information Requirements Planning

Attributes of Intelligence Excellence: Anticipatory; Timely; Accurate; Usable; Complete; Relevant; Objective; Available

- Anticipatory
- Timely
- Accurate
- Usable
- Complete
- Relevant
- Objective
- Available

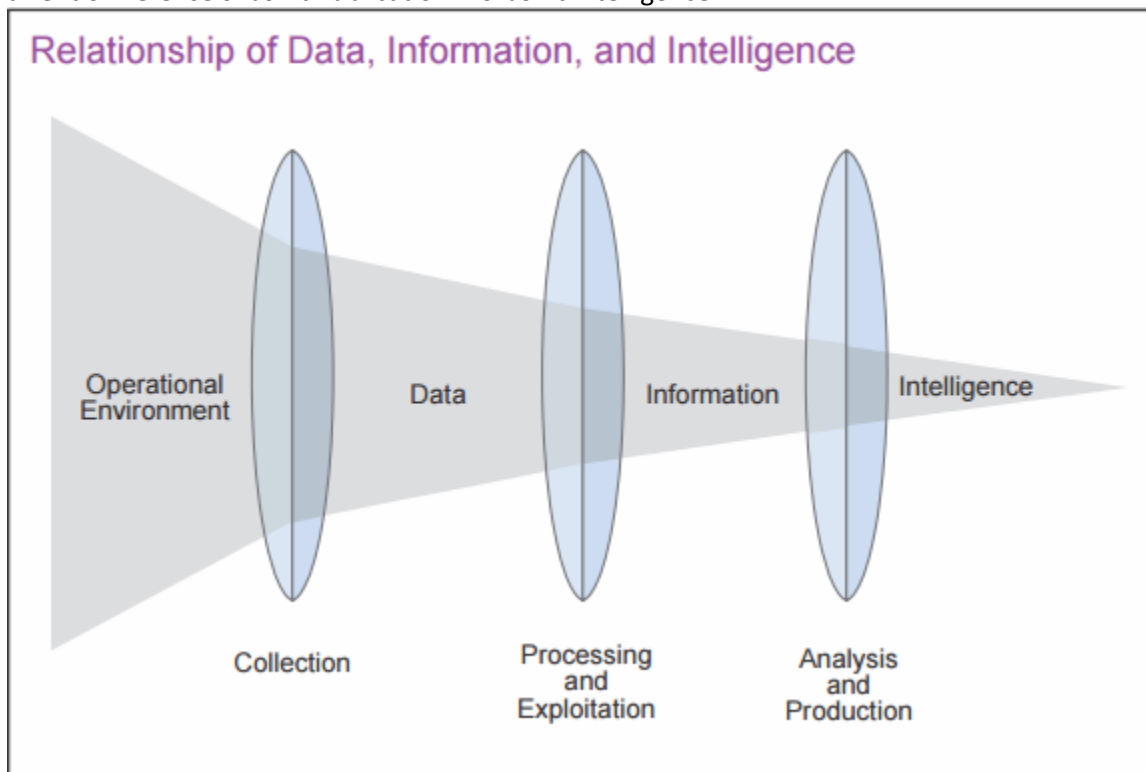
## Intelligence Requirements and Information Requirements Planning

Principles for Interorganizational Intelligence Collaboration:

- Establish strong relationship networks.
- Build mutual trust and respect for colleagues.
- Share a common vision.
- Minimize territorial issues.
- Establish continuous communication.
- Eliminate impediments.

## Intelligence: Relationship of Data Information and Intelligence

U.S. Department of Defense's "Joint Publication 2-0: Joint Intelligence"



"Tell me what you know...tell me what you don't know...tell me what you think—always distinguish which is which."

General Colin Powell, US Army

Guidance to Joint Staff J-2 on 13 November 1992 / Chairman of the Joint Chiefs of Staff, 1989-1993

Strategic Efficiency Consortium | [www.strategiefficiency.org](http://www.strategiefficiency.org)

▪ Security ▪ Operational Efficiency ▪ Infrastructure ▪ Advisory ▪

## Strategic Efficiency Consortium+ Industrial Security Intelligence Data Platform Services

### CAPABILITY LIST (Extract)

**Security Intelligence Data + Security Threat Intelligence Data + Industrial Security Intelligence News Data + Security Threat Intelligence Data Feeds + Intelligence News Data Services**

#### Security Intelligence Data

About Strategic Efficiency Consortium Security Intelligence Platform

**Inform | Measure | Define | Analyze**

Turning Data into Actionable Insights and Strategies



#### Strategic Efficiency Consortium Security Intelligence Data Service

This platform is working to develop a broader view and context of Security Intelligence. Our Security Intelligence Platform Service focus is on global and market depth, real-time updates on alerts, malware notices, security news and general cyber-security awareness. The objective behind the Security Intelligence Service is to provide user the ability to become aware, recognize and act upon indicators of attack and compromise scenarios in a timely manner that better protect against zero-day threats, advanced persistent threats, and exploits. By offering comprehensive Security Intelligence/Threat Intelligence capabilities to a user's software, hardware and policy defense strategy, it will enhance the user's ability (or in some user environments – create the ability) to search for advanced attacks, profile atypical malware and, detect adversaries.

#### Strategic Efficiency Consortium Security Intelligence Data Service

Security Intelligence Platform Content is designed to focus on key demand types of intelligence including: Business Intelligence: Commercial Intelligence: Market Intelligence: Competitive Intelligence: Strategic Intelligence.

Security Intelligence Platform continuously adapts Intelligence Content Design to facilitate and enable; building, strengthening and enhancing of Knowledge Disruption + Competitive Advantage + Strategic Decision Making.

Intelligence is user-defined as a set of internal activities to help understand and influence user's corporate strategy, deals, competitors, markets, and customers. User Intelligence is real-time collection, normalization, and analysis of the data generated by user, applications and infrastructure to impact the position, advantage and risk posture of the user enterprise, therefore we maintain strong focus on the critical goal of Intelligence to provide actionable, strategic, comprehensive insight to reduce user's risk and operational effort.



## Strategic Efficiency Consortium Client-User Driven Security Intelligence Data Service



After much consultation, evaluation and measurement of users' demand and approach to Intelligence, we have specifically designed and built this Security Intelligence Data Service to deliver well-defined deliverables into the initial critical intelligence demands of our user; deliverables that can benchmark, define, grow and evolve successful user adaptability to the ever-changing demands of Competitive Security Intelligence.

Although we have developed a data and information platform comprising over 500 channels of data to immediately address short and medium-term Security Intelligence demands, this platform content is also designed to deliver medium and long term; a deeper, strategic and actionable change in the user to increase capability and competence in:

- user understanding of Security Intelligence Technology and Security Intelligence Information and Security Intelligence Data
- user leverage of technology to process information relating to aspects of their operational environments
- user usage of information to contribute to their decision-making process; and usage of information to provide reasoned insight into future environments;
- user improvements in information utilization
- user capability in anticipation and prediction of future environments and better defining differences in available courses of action
- user depth of quantitative analysis and qualitative judgment and competing interpretation
- user continuous examination of their intelligence needs
- user definitions of goals, frameworks, quantifiable outputs and objectives
- user focus on actionable intelligence creation
- enhancing user types of intelligence – Warning; Current; General; Target; Scientific Technical; Counterintelligence; Estimative; Identity
- growing user levels of intelligence – Strategic; Operational; Tactical
- developing user principles of intelligence – Perspective; Synchronization; Integrity; Effort Singularity; Prioritization; Excellence; Prediction; Agility; Collaboration; Fusion

This platform has completed version 2.25; completed upgrades and revisions developing and migrating to Intelligence version 4.95 and planned upgrades and revisions into Learning version 9.45. We currently manage +3 million data sources and process +500k daily data updates; data sources are planned for expansion to +75 million data sources. Continued partner and client user collaboration is strongly encouraged, facilitated, structured and recommended throughout these development phases.

We currently manage +3 million data sources and process +500k daily data updates; data sources are planned for expansion to +75 million data sources. Continued partner and client user collaboration is strongly encouraged, facilitated, structured and recommended throughout the content expansions.

## Strategic Efficiency Consortium Security Intelligence Platform Project Partners

This project, platform and service was envisioned and originated by our Foundation Partner; Security Efficiency Consortium and their Security Work Group.

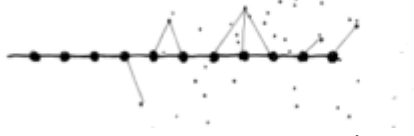
Project was further developed and focus expanded into the Industrial Control Systems Market by the MG Strategy+ and their Industrial Control Systems Group.

Platform is executed and managed by our Foundation Partners in Digital Management and Intelligence Content Management.

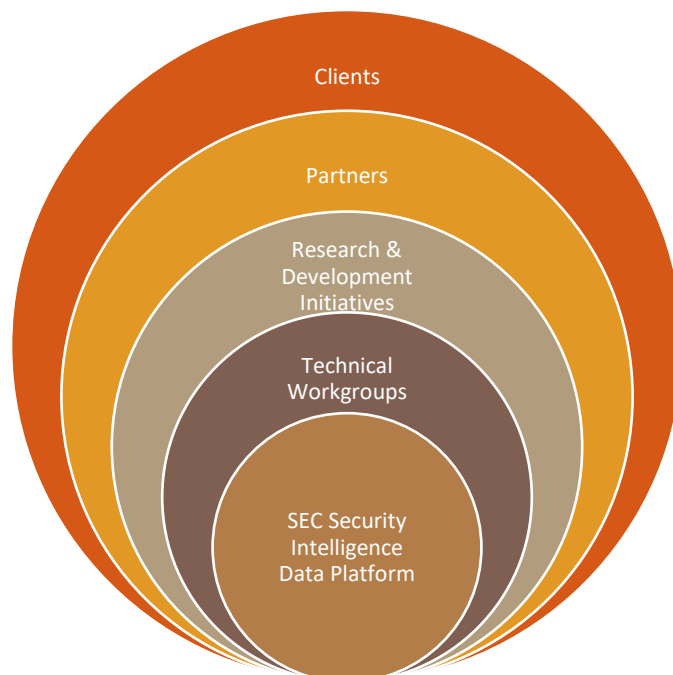
## SEC Security Intelligence Platform – User Community; a community of users, workgroups and partners;

### Aims and Objectives

### Intelligence Content < | > Content Intelligence



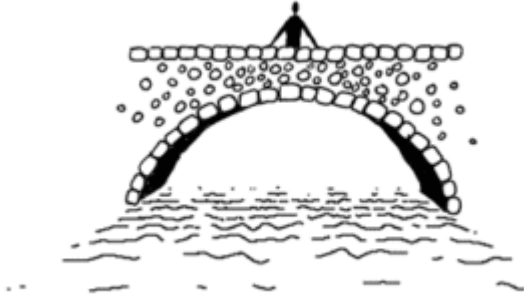
- User Community – This platform and service was envisioned and initiated by and continues development through our User Community comprising our users, workgroups and partners. Workflow and Software is developed in close collaboration with our user community. Our User community is founded on, and driven by, our Research, Analysis and Technical Consulting Workgroups. Users receive support from our workgroup teams of experts and dedicated analysts.
- User-driven collaboration designs and evolves the; accessibility, optimal user experience, responsiveness and ergonomics of the platform and service. This Security Intelligence Platform evolves, based on, and thanks to, the participation of our user community.
- Users are not focused on technology; but are more concerned with specific solutions to specific problems – this is a solution platform and service. We can neither predict nor foresee the uses of our data; therefore, our User Collaboration and our User Personalization are the keys to our data science, our platform, our solution.



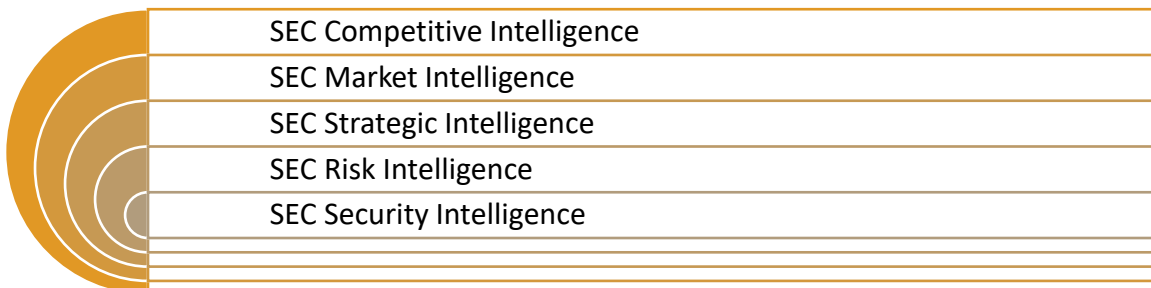
# Strategic Efficiency Consortium

**SEC**

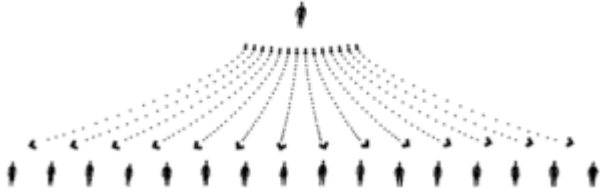
Strategic Efficiency Consortium Security Intelligence Platform – Interface: Functionality: Aims and Objectives  
Inform | Measure | Define | Analyze



- Intuitive and collaborative monitoring platform for competitive strategic security intelligence.
- Platform scalable to address all key intelligence deliverables: Competitive Intelligence, Market Intelligence, Strategic Intelligence, Risk Intelligence; Intelligence, Analysis, Insights.
- Platform built to facilitate flexible data management structures
- Platform to provide structure and meaning to large volumes of unstructured content.
- Platform to retrieve relevant information quickly, based on time saving, simplified configurations.
- Platform monitoring through clear, well-designed interfaces.
- Platform aggregation of content from various sources, and delivery of it in a relevant format.
- Information access platform that provides a single point of access to information from multiple sources.
- Platform to enables users to find and use the information they often already have but are in no position to utilize efficiently due to the sheer quantity and lack of structure.
- Platform built to facilitate shift in focus from internal to external data; external Data is increasingly becoming one of the richest sources for insight.
- Platform to unify internal and external sources into one role-based portal, so that knowledge users can do their jobs without having to move from one information source or application to another.
- Platform built on Unique Content Classification Systems: Automatic and Manual Classification: Content Aggregation and Content Management
- Qualified content sources are expanded continuously and constantly developed, screened, added, updated and integrated by our researchers
- Search-based software application designed to make knowledge workers more productive.
- Search Find – Full Text Search, Field Search, Intelligent Search, Navigate by Topics
- Professional Level SaaS Model
- Responsive, Standardized and Seamless User Experience
- Personalized Alerts, Bookmarks, Data
- Functionality based on single users and/or teams of users



## Strategic Efficiency Consortium Security Intelligence Platform – Content: Functionality: Design and Objectives Anticipate | Protect | Analyze



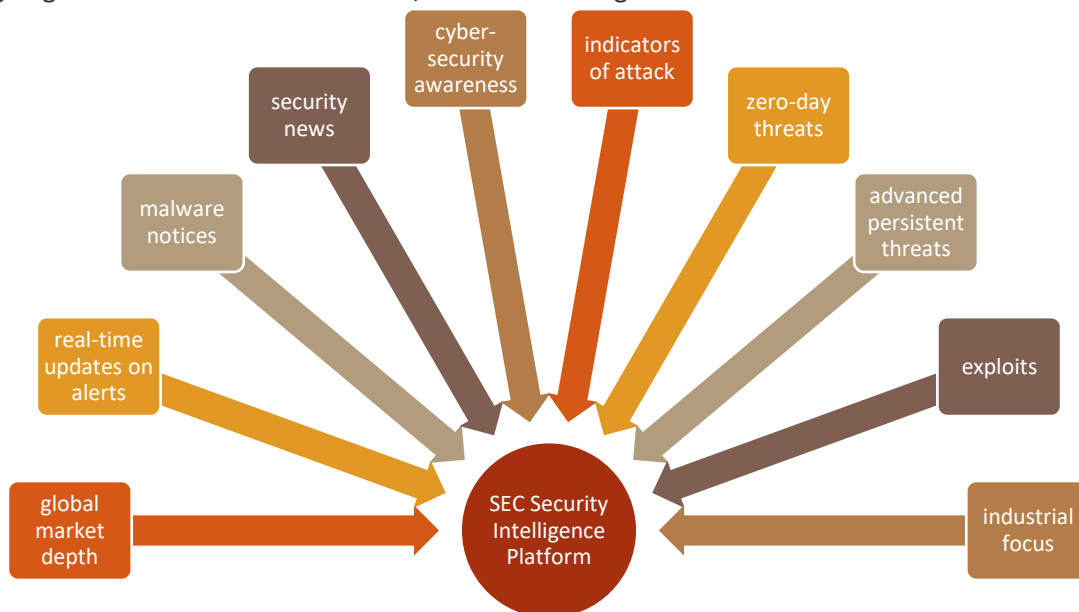
- Content is designed to make our knowledge users more productive, and facilitate and improve user:
- Monitoring – to better anticipate risk and innovate solutions
- Positioning – based on competitive strategic security intelligence
- Detection Perspective – based on information monitoring
- Trend Analysis – content is always working towards a clearer, more updated view of trends.
- Action – Transforming information and knowledge to actionable data.
- Time Utilization – Users now focus time on analyzing the content and gaining insights rather than searching for it. Competitiveness – Detection of risks and opportunities in your environment, to accelerate user competitiveness

Content is designed to drive clients towards:

- more data assisted decision making
- more utilization of external 3rd party objective data into/added to decision making
- more anticipatory / real-time decision-making vs after the fact decision making
- looking beyond their internal reporting data and systems to become more current and competitive
- leveraging data to better anticipate environment changes and to identify new opportunities

Content development and design is continuous and is differentiated by our unique:

- Designed Intelligence Content Ecosystems
- Designed Learning Content to continuously reduce Time to Knowledge
- Designing, remodeling, optimizing and implementing of Intelligence Processes and Efficiencies.
- Designing of end to end continuous and/or ad-hoc Intelligence Workflows and Processes.



## Strategic Efficiency Consortium Industrial Security Intelligence Data Platform Services

### CAPABILITY LIST (Extract)

#### **Security Intelligence Data + Security Threat Intelligence Data + Industrial Security Intelligence News Data + Security Threat Intelligence Data Feeds + Intelligence News Data Services**

SEC Security Intelligence Thinking

#### **Client Critical Security Threat Intelligence Need**

The critical need for an evidence based, automated, holistic approach of the security threat landscape. These are challenging times for security managers, with corporate boards demanding awareness of cyber risks, faster processing of progressively complex data and efficient managed services for an increasing number of intelligent devices than ever before.

Ultimately security teams are in a better position of strength to defend their organizations against threats if they know what is coming in their direction; tools and staff are vital but should be augmented with intelligence. Threat Intelligence is no longer for the large, well-funded organizations, but is required to be an overall component of mitigation strategies for all businesses that operate within this evolving technological environment; the economies of scale and adaptability of solutions now allows small businesses to be able to access credible security threat intelligence sources that can be based on an organizations profile and supply chain.

Critical data that used to be in a secured datacenter now moves across an increasingly complex ecosystem of networked environments, including IIoT, IoT, cloud servers, virtualized environments and mobile devices. The rate of change in some enterprise environments is so rapid that many organizations are struggling to keep pace with the evolving nature of cyber threats or being able to ascertain knowledge of what arises daily.

To build an effective cyber security strategy, awareness of specific cyber threats needs to occur as well as an analysis of how those threats affects the organization. Security Threat Intelligence provides context, indicators, increased awareness and actionable responses about current or emerging threats that aid in decision making at an operational, tactical or strategic level. Cyber adversaries are increasingly using sophisticated tools, techniques and procedures that are evading stand-alone security solutions with multiyear campaigns that target valuable and sensitive information. Organizations need an evidence based, holistic view of the threat landscape with a proactive security posture to defend organizations from a wide array of threat – A Security Threat Intelligence led cyber security program.

The goals behind Security Threat Intelligence Services are to provide organizations the ability to become aware, recognize and act upon indicators of attack and compromise scenarios in a timely manner that better protect against zero-day threats, advanced persistent threats and exploits. With security teams across the world being challenged to discover, analyze and interpret the vast number of daily events to discover attacks, there are efforts led through Security Consortiums that are automatically detecting, contextualizing, prioritizing, performing forensic analysis, automating compliance and responding to incidents that will move us beyond Security Information Management to Security Threat Intelligence.



SEC Security Intelligence Thinking

## **Client Critical Security Threat Intelligence Need (continued)**

Facility owners more and more, are defining within their overall strategy what they expect to achieve from Security Threat Intelligence; including the types of alerts needed, vendor news, how intelligence is collected, reported and communicated to relevant stakeholders, analysis process and how threat intelligence would be used. Only adding new and “innovative” products to the environment that requires integration and implementation of additional policies that needs to be managed by an overburdened staff is not the response required; but rather a Security Threat Intelligence Platform that better prepares their defense of the organization. By combining Security Threat Intelligence capabilities to an organizations’ software, hardware and policy defense strategy; it enhances staff’s ability to search for advanced attacks, profile atypical malware and detect adversaries.

***Typical internal threat intelligence teams are hardly common as they have been deployed and structured in a way that is costly, hands on and mis-aligned to the organizations security posture.***

Leveraging your tools and data in an effective manner is key to achieve your desired security posture.

As we exist in a global environment where attacks are generated at a machine level, Customers must ensure that the identification, sharing, comprehension and application of threat intelligence is as automated as much as possible. An automated platform allows for ease of access to the intelligence and the ability to contextualize and prioritize attacks for immediate mitigation strategies. Effective intelligence assess intelligence from various sources and source types to create a better threat and risk image for an organization. The value to end customers is not the quantity of the various intelligence feeds, but the applicability of those feeds to their entire environment. The ability to customize dashboards and filters to continuously illustrate threats allows security teams to focus on threats that impacts the organization. The threat intelligence market offers different types of information feeds that are not necessarily aligned to any industry or large manufacturer installed base. Though intelligence platforms must be recognized as a critical component to cyber-security, organizations must define their high-level requirements, functional requirements and visibility requirements.

***Through Continuous Security Threat Intelligence collection, analysis and optimization, organizations can increase their protective measures and strengthen their security tools.***

## Strategic Efficiency Consortium Industrial Security Intelligence Data Platform Services

### CAPABILITY LIST (Extract)

#### Security Intelligence Data + Security Threat Intelligence Data + Industrial Security Intelligence News Data + Security Threat Intelligence Data Feeds + Intelligence News Data Services

Security Intelligence Thinking

#### **Threat Intelligence, Information, Data: Critical Differences**

There is a difference between threat data, information, and intelligence; understanding the difference is essential to getting the most out of your threat intelligence platform. The progress from data to information to intelligence, reduces the volume of outputs while the value of those outputs simultaneously increases.

Threat intelligence platforms produce data and information, which human analysts must then use to produce actionable threat intelligence. A computer can never produce threat intelligence, but humans are unsuited to the task of collecting and processing huge volumes of threat data.

Action must always be the end goal. Threat intelligence is useless unless it can be used to improve action, in this case; cyber security action.

Most organizations assume that if they buy a threat intelligence platform it will do everything for them - that isn't the case – there are critical differences between threat data, information, and intelligence, and skilled analysts define the transition from one to the next.

The main differences between data, information, and intelligence come in two forms: volume, and usability.

Data is typically available in huge volumes and describes individual and unarguable facts. Details of individual connection requests are an excellent example of data, because they're simple statements of fact and aren't open to discussion.

Information is produced when a series of raw data points are combined to answer a simple question; although this is a far more useful output than the raw data, it still doesn't directly inform a specific action.

Intelligence takes this process a stage further by interrogating data and information to tell a story (a forecast, for example) that can be used to inform decision making. Crucially, intelligence never answers a simple question, rather it paints a picture that can be used to help people answer much more complicated questions. Intelligence may not directly answer a specific question, but it does aid in the decision-making process.









Threat Intelligence Platforms don't actually produce Threat Intelligence: To produce a small but steady stream of actionable threat intelligence, massive quantities of data are required. Simple threat intelligence platforms are able to consume and organize threat data on a large scale, which makes the job of your analysts far easier, and their outputs more useful.









Security Intelligence Thinking

## **Threat Intelligence, Information, Data: Critical Differences (continued)**

An important function of threat intelligence products is to organize threats according to their potential to damage an organization. This is where the very best providers differentiate themselves from the rest of the pack: They're able to prioritize threats automatically, so human analysts can focus their efforts on the most important threat data or information first. Because of the big data issues described above, having a tool that can prioritize threats is essential. If your analysts are digging through every single threat manually, you'll find that many urgent threats aren't identified until after the fact. The process of combining and organizing threat data into threat information is fundamental to the prioritization process.

When it comes to threat intelligence, action is the only thing that really counts. There's absolutely no value in possessing threat data, information, or intelligence unless you use it to improve your security program or defend against an incoming attack.

<b>Strategic Efficiency Consortium</b> <b>Industrial Security Intelligence Data Platform Services</b>		
<b><u>SEC Industrial Security Intelligence Data Platform Work Flow</u></b>		
This Platform typical workflow usage is below, each key area of the platform is highlighted below, clients are encouraged to setup the My Email Alert Dashboard and My Cyber Vendors and My Cyber Inventory		
	<b>Cybersecurity Data Dashboard</b> Cybersecurity Data Dashboard: Channels 1-39: Channels Related to Cyber Security: IT Security: ICS Security: Information Security → Review main Cybersecurity channels here for fast current snapshot of cybersecurity and information security activity.	<a href="#">CyberSecurity Data Dashboard</a>
	<b>CERT Data Dashboard</b> CERT Data Dashboard: Channels 40-235: Channels Related to Global Computer Emergency Readiness and Incident Response Teams Activities: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams → Review current snapshot of global CERT and CIRT activity	<a href="#">CERT Data Dashboard</a>
	<b>Company Data Dashboard</b> Company Data Dashboard: Channels 400-999: Channels Related to Leading Product and Service Companies in Cyber Security: IT Security: ICS Security: Information Security → Review key companies related to and impacted by Industrial Cybersecurity.	<a href="#">Company Data Dashboard</a>
	<b>Custom Data Dashboard</b> Custom Data Dashboard: Channels 236-399: Custom Channels based on Users requests for specific custom content-based channel(s). → Review custom data channels developed based on specific user requests or demands	<a href="#">Custom Data Dashboard</a>
	<b>Research Library</b> Technical Research Library: Papers: Presentations: Reports → Review technical library of technical and research documents, this library development is driven by a combination if work group activities and user project activities or demands.	<a href="#">Research Library</a>
	<b>Table of Channels</b> Listing of All Channel Contents → Review all active channels her, channels not listed are usually either in development or revisions.	<a href="#">Table of Channels</a>
	<b>My Vendor Alert Dashboard</b> My Cyber Vendors: OT: IT: ICS: Vendors of all hardware and software components utilized in support of operations. → This is a monitoring tool. This lists updates on all key vendors you are monitoring via the My Cyber Vendors dashboard.	<a href="#">My Vendor Alert Dashboard</a>
	<b>My Cyber Vendors</b> My Cyber Vendors: OT: IT: ICS: Vendors of all hardware and software components utilized in support of operations. → This is a customs monitoring tool. Review and update the key vendors you want to monitor, the list of vendors can be customized, imported and exported.	<a href="#">My Cyber Vendors</a>

	<p><b>My Cyber Vendors Alerts</b>                  My Cyber Vendors: OT: IT: ICS: Vendors of all hardware and software components utilized in support of operations.                  → This is a monitoring tool. This lists updates on all key vendors you are monitoring via the My Cyber Vendors dashboard. Click on each vendor to see current search activities and results.</p>	<p><a href="#">My Cyber Vendors Alerts</a></p>
	<p><b>My Cyber Inventory</b>                  My Cyber Inventory: OT: IT: ICS: Assets Inventory: Components Inventory: Production-Centric ICS Assets: Traditional IT-Centric Assets: Inventory of all hardware and software components utilized in support of operations.                  → This is a custom monitoring tool. Review and update the key inventory or products you want to monitor, the list of products can be customized, imported and exported.</p>	<p><a href="#">My Cyber Inventory</a></p>
	<p><b>My Cyber Inventory Alerts</b>                  My Cyber Inventory: OT: IT: ICS: Assets Inventory: Components Inventory: Production-Centric ICS Assets: Traditional IT-Centric Assets: Inventory of all hardware and software components utilized in support of operations.                  → This is a monitoring tool. This lists updates on all key inventory you are monitoring via the My Cyber Inventory dashboard. Click on each inventory item to see current search activities and results.</p>	<p><a href="#">My Cyber Inventory Alerts</a></p>
	<p><b>My Channel Bookmark Dashboard</b>                  My Channel Bookmark Dashboard                  → This is a monitoring tool. This allows user to select specific channels to generate current snapshot of key headlines in each selected channel.</p>	<p><a href="#">My Channel Bookmark Dashboard</a></p>
	<p><b>My Channel Bookmarks Horizontal Scroll</b>                  Horizontal Headline Feed Scroll                  → This is a monitoring tool. This displays selected channels' headlines based on channels selected in My Channel Bookmark Dashboard in a Horizontal Scroll format.</p>	<p><a href="#">My Channel Bookmarks Horizontal Scroll</a></p>
	<p><b>My Channel Bookmarks Vertical Scroll</b>                  Vertical Headline Feed Scroll                  → This is a monitoring tool. This displays selected channels' headlines based on channels selected in My Channel Bookmark Dashboard in a Vertical Scroll format.</p>	<p><a href="#">My Channel Bookmarks Vertical Scroll</a></p>
	<p><b>My Email Report Alert Dashboard</b>                  My Email Alert Dashboard                  → This is a monitoring too generate and delivery scheduled emails based on clients selected and customized data via previous dashboards.</p>	<p><a href="#">My Email Report Alert Dashboard</a></p>
	<p><b>SEC Security Briefings</b>                  Technical Briefings and Highlights based on                  Editor Paper Extracts: Work Group Papers: White Papers Research Papers: Paper Extracts: Presentation Papers                  Editor Picks Articles: Key Articles: Highlighted Articles: Alert Articles: Research Articles                  Editor Picks Reports: Key Reports: Highlighted Reports: Alert Reports: Research Reports</p> <p><b>SEC Working Group Briefings</b>                  Technical Briefings and Highlights based on Work Group</p> <p><b>SEC In Development</b>                  Technical Briefings and Highlights based on Work Group</p>	<p><a href="#">SEC Security Briefings</a></p> <p><a href="#">SEC Working Group Briefings</a></p> <p><a href="#">SEC In Development</a></p>

## Strategic Efficiency Consortium Industrial Security Intelligence Data Platform Services

### SEC Industrial Security Intelligence Data Platform Content Map

This Platform Data Content Map is below, clients are encouraged to collaborate, influence, drive and develop channels and content development. Content Map is developed and updated in weekly, monthly and yearly phases of development and expansion.

	<b>SEC+ Content Data Map Strategic Efficiency Consortium</b>	<b>January 2019 Content Data Map 93 channels</b>
	<u>SEC Channel Name</u>	<u>Description</u>
1	000 SEC Latest News All	000 SEC Latest News All: All Channels: All Cybersecurity: All Information Security: Industrial Control Systems Security: IT Security
2	001 SEC Alerts Advisories	001 SEC Alerts Advisories: Cybersecurity: Latest Risks: Threats Risks: Advisories: Vulnerabilities: Alerts: Threat Defense: Bulletins: Event Response: Security Response: Virus Spyware Malware: Product Security Incident Response Teams PSIRT: Threat Outbreaks: Threats Defenses: Security Advisories: Threats Activists: Threats Cybercrime: Threats Economic: Threats Strategic: Crypto Vulnerabilities: Firmware Vulnerabilities: Hardware Vulnerabilities: Network Vulnerabilities: OS Vulnerabilities: Threat Research: SCADA Alerts: Adware: Virus: Spyware: Network Protection: IIOT: IOT Security
3	002 SEC Anti-Virus Malware	002 SEC Anti-Virus Malware: Anti-Virus Anti Malware Markets: Anti-Virus Malware Vendors: Anti-Virus Malware Software: Updates: Vendor Advisories
4	003 SEC CERT Global	003 SEC CERT Global: Global Government CERT: All Countries Regions CERT: Global Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams Global: Computer Security Incident Response Teams Global
5	004 SEC Consultants Research	004 SEC Consultants Research: Information Security Consultants: Management Consultants: Cybersecurity Consultants: Reports: Research
6	005 SEC Media Reports Articles	005 SEC Media Reports Articles: Information Security Reporting: Cybersecurity Media Coverage
7	006 SEC Governments Organizations	006 SEC Governments Organizations: Governmental Cybersecurity Initiatives: Governmental Cybersecurity Entities: Information Security Organizations Initiatives: Industry Organizations
8	007 SEC Software Hardware	007 SEC Software Hardware: Software Vendors: Hardware Vendors: Integrated Software Hardware Vendors
9	008 SEC Systems Networks Telecom	008 SEC Systems Networks Telecom: Telecom Providers: Networking Vendors: Telecom Network Systems Vendors
10	009 SEC ICS Automation	009 SEC ICS Automation: Industrial Control Systems Vendors: Industrial Automation Vendors: SCADA Vendors: Distributed Control Systems Vendors
11	010 SEC ICS CERT	010 SEC ICS CERT: Industrial Control Systems CERT: SCADA CERT
12	011 SEC ICS Cybersecurity	011 SEC ICS Cybersecurity: Industrial Control Systems Cybersecurity: SCADA Cybersecurity: ICS Cybersecurity Vendors
13	012 SEC IIOT Platforms Data Analytics	012 SEC IIOT Platforms Data Analytics: Industrial Internet of Things IIoT: Internet of Things IoT: Big Data: IoT IIoT Platforms: IIoT Standards: IIoT leaders: IoT Application Enablement Platforms: M2M Platforms: IaaS Infrastructure-as-a-Service: IIoT Platform Ecosystems: IIoT Predictive Maintenance: Industrial Analytics: Industrial Data Analytics
14	039 SEC Cybersecurity Learning	039 SEC Cybersecurity Learning: Cybersecurity Education: Cybersecurity Training
15	040 SEC CERT NA	040 SEC CERT NA: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT North America: CERT Canada: CERT USA
16	042 SEC CERT SA	042 SEC CERT SA: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT South America Region
17	043 SEC CERT EU	043 SEC CERT EU: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT Europe

18	047 SEC CERT SEA	047 SEC CERT SEA: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT South East Asia
19	050 SEC CERT Canada	050 SEC CERT Canada: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT Canada
20	051 SEC CERT USA	051 SEC CERT USA: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT USA
21	053 SEC CERT Austria	053 SEC CERT Austria: Computer Emergency Response Team Austria: Austrian Energy CERT: AEC
22	061 SEC CERT Denmark	061 SEC CERT Denmark: DKCERT: Danish Computer Security Incident Response Team
23	063 SEC CERT Finland	063 SEC CERT Finland: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT Finland
24	064 SEC CERT France	064 SEC CERT France: Agence Nationale de laSécurité des Systèmes d'Information
25	070 SEC CERT Italy	070 SEC CERT Italy: CERT Nazionale: Computer Emergency Response Team
26	074 SEC CERT Luxembourg	074 SEC CERT Luxembourg: Cyber Emergency Response Community Luxembourg
27	079 SEC CERT Netherlands	079 SEC CERT Netherlands: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT Netherlands
28	089 SEC CERT Spain	089 SEC Spain: Spain: Computer Emergency Response Team for Security and Industry: CERTSI
29	093 SEC CERT United Kingdom	093 SEC CERT United Kingdom: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: United Kingdom
30	116 SEC CERT Brazil	116 SEC CERT Brazil: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT Brazil
31	121 SEC CERT Mexico	121 SEC CERT Mexico: Mexico: La Coordinación de Seguridad de la Información: CSI: UNAM-CERT
32	130 SEC CERT China	130 SEC CERT China: National Computer Network Emergency Response Technical Team: Coordination Center of China: CNCERT: CNCERT CC
33	131 SEC CERT Australia	131 SEC CERT Australia: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: CERT Australia
34	137 SEC CERT Japan	137 SEC CERT Japan: Japan JPCERT CC: CSIRT
35	178 SEC CERT Saudi Arabia	178 SEC CERT Saudi Arabia: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: Saudi Arabia
36	230 SEC CERT Tanzania	230 SEC CERT Tanzania: CERT Computer Emergency Readiness Teams: CIRT Computer Incident Response Teams: Tanzania
37	236 SEC Custom ICS Automation	236 SEC Custom ICS Automation: Industrial Control Systems Automation: Custom Search Channel: Custom Search News Topic: ICS Automation
38	237 SEC Custom ICS Malware	237 SEC Custom ICS Malware: Industrial Control Systems Malware: Custom Search Channel: Custom Search News Topic: ICS Malware
39	238 SEC Custom ICS PLC Security	238 SEC Custom ICS PLC Security: Industrial Control Systems PLC Security: Custom Search Channel: Custom Search News Topic: ICS PLC Security
40	239 SEC Custom ICS Ransomware	239 SEC Custom ICS Ransomware: Industrial Control Systems Ransomware: Custom Search Channel: Custom Search News Topic: ICS Ransomware
41	240 SEC Custom ICS Security	240 SEC Custom ICS Security: Industrial Control Systems ICS Security: Custom Search Channel: Custom Search News Topic: ICS Security
42	241 SEC Custom ICS Smart Grid	SEC241 ICS Smart Grid: Industrial Control Systems ICS Smart Grid: Custom Search Channel: Custom Search News Topic: ICS Smart Grid
43	242 SEC Custom SCADA	242 SEC Custom SCADA: ICS Supervisory Control And Data Acquisition: Custom Search Channel: Custom Search News Topic: SCADA
44	400 SEC ABB	400 SEC ABB: ASEA Brown Boveri: Industrial Digitalization: Electrification Products: Robotics and Motion: Industrial Automation: Power Grids: Source ABB
45	415 SEC Emerson	415 SEC Emerson: Emerson Automation Solutions: Emerson Commercial Solutions: Emerson Process Management: Emerson Industrial Automation: Source Emerson
46	418 SEC Festo	418 SEC Festo: Festo Group: Process Control: Factory Automation Solutions: Source Festo
47	424 SEC Hitachi	424 SEC Hitachi: Hitachi Above Security: Source Hitachi

# Strategic Efficiency Consortium



48	441 SEC Rockwell Automation	441 SEC Rockwell Automation: Rockwell Software: Allen-Bradley: Rockwell Industrial Automation: Rockwell Control Systems: Rockwell Industrial Networks: Source Rockwell Automation
49	445 SEC Siemens	445 SEC Siemens: Siemens: Siemens Government Technologies: Industry: Energy: Healthcare: Infrastructure: Cities: Source Siemens
50	457 SEC Yokogawa Electric	457 SEC Yokogawa Electric: Industrial Automation: Test and Measurement: Control Systems: Data Acquisition: Field Instruments: Process Analyzers: Industrial Networking: Components: Life Science: Source Yokogawa
51	500 SEC A10 Networks	500 SEC A10 Networks: Application Delivery Controllers: Software: Hardware: Source A10 Networks
52	501 SEC Absolute Software	501 SEC Absolute Software: Absolute Software: Self-Healing Endpoint Security: IT Asset Management: Data Visibility and Protection: Source Absolute Software
53	502 SEC Accellion	502 SEC Accellion: Secure File Transfer: Secure External Collaboration: Governance And Compliance: Enterprise Integration: Source Accellion
54	505 SEC Adobe	505 SEC Adobe: Adobe Software Systems: Multimedia Creativity Software: Creative Cloud: Experience Cloud: Document Cloud: Source Adobe Systems
55	509 SEC Akamai	509 SEC Akamai: Akamai Technologies: Distributed Computing Platforms: Cloud Delivery Platforms: Content Delivery Networks: CDN Services: Source Akamai Technologies
56	521 SEC Appthority	521 SEC Appthority: Appthority Mobile Threat Protection: MTP: Source Appthority
57	522 SEC Arbor Networks	522 SEC Arbor Networks: ATLAS Threat Intelligence Infrastructure: DDoS Solutions: Advanced Threat Solutions: Network Security Management: Network Visibility Solutions: Source Arbor Networks
58	523 SEC Argus Cyber Security	Argus Cyber Security: Automotive Cyber Security: Source Argus Cyber Security
59	526 SEC ATT	526 SEC ATT: AT&T: AT&T Telecommunications: AT&T Cybersecurity: Source AT&T
60	531 SEC Avast	531 SEC Avast Security: Avast Cybersecurity Network Protection: Avast Consumer: Avast Mobile: Avast Business: Avast Platform: Avast Cyber Security: Source Avast
61	542 SEC Bayshore Networks	542 SEC Bayshore Networks: Bayshore Networks IT/OT Gateway: Industrial Infrastructure: Cybersecurity: Networking: Industrial IOT: Source Bayshore Networks
62	561 SEC Bromium	561 SEC Bromium: Enterprise Security: Bromium Secure Platform: Virtualization Based Security: Endpoints: Malware: Source Bromium
63	566 SEC CA Technologies	566 SEC CA Technologies: CA Identity Suite: CA Single Sign-On: CA Privileged Access Management: Source CA Technologies
64	574 SEC Check Point Software Technologies	574 SEC Check Point Software Technologies: Check Point Infinity: Network: Cloud: Mobile: Endpoint: Security Management: Advanced Threat Prevention: SaaS Security: IaaS Security: Mobile Threat Defense: Unified Security Management: Source Check Point Software Technologies
65	578 SEC Cisco Systems	578 SEC Cisco Systems: Cisco Security: Advanced Malware Protection: Cloud Security: Email Security: Endpoint Security: Network Visibility and Enforcement: Next-Generation Firewalls: Next-Generation Intrusion Prevention Systems: Router Security: Security Management: VPN Security Clients: Web Security: Source Cisco Systems
66	580 SEC Claroty	580 SEC Claroty: OT Networks: OT Environments: Claroty Platform: Continuous Threat Detection: Secure Remote Access: Enterprise Management: Security Assessments: OT Security Platform: Source Claroty
67	620 SEC Dell	620 SEC Dell: Dell Technologies: Secureworks: Managed Security Services: Secureworks Counter Threat Unit: Security Operations Centers (SOCs): VMware: VMware Security: Source Dell
68	664 SEC FireEye	664 SEC FireEye: FireEye Helix: Network Security: Endpoint Security: Email Security: Threat Analytics Platforms: Threat Intelligence: Mandiant Consulting: Source FireEye
69	667 SEC Flexera Software	667 SEC Flexera Software: Secunia Research: Advisory Databases: Vulnerability Research: Vulnerability Intelligence: Personal Software Inspector: Software Vulnerability Management: Source Flexera
70	671 SEC Fortinet	671 SEC Fortinet: Next-Generation Firewalls: SD-WAN: Virtualized Next-Generation Firewall Endpoint Security: Secure Wi-Fi: Email Security: SIEM: Identity and Access Management: DDoS: Threat Intelligence: Threat Landscape: Threat Map: Source Fortinet



# Strategic Efficiency Consortium

# SEC

71	685 SEC Google	685 SEC Google: Google Security Chrome Security: Source Google
72	702 SEC HP Enterprise	702 SEC HP Enterprise: HPE Security and Digital Protection Advisory: HPE Adaptive Security and Digital Protection: Source HP Enterprise
73	706 SEC IBM Security	706 SEC IBM Security: IBM Security: Security Intelligence: X-Force Research: Source IBM
74	713 SEC Indegy	713 SEC Indegy: Industrial Cybersecurity: Industrial Control Systems ICS Security: ICS Network Security: ICS Environments: Control Networks Inspection: Agentless Controller Verification: Industrial Security Platforms: Industrial Cyber Security Platforms: Source Indegy
75	720 SEC Intel Wind River	720 SEC Intel Wind River: Intel: Aerospace: Defense: Automotive: Industrial: Networking Security: Source Intel Wind River
76	731 SEC Juniper	731 SEC Juniper: Firewalls: Advanced Threat Prevention: Visibility Management and Analytics: Juniper Sky Advanced Threat Prevention: Secure Analytics: Source Juniper
77	732 SEC Kaspersky	732 SEC Kaspersky: Cybersecurity Services: Anti Targeted Attack: Endpoint Security: Cloud Security: Kaspersky Total Security: AO Kaspersky Lab: Securelist: Source Kaspersky
78	757 SEC McAfee	757 SEC McAfee: Cloud Security: Dynamic Endpoint: Threats Management: Optimization Operations: Safeguard Data: Source McAfee
79	758 SEC Malwarebytes	758 SEC Malwarebytes: Malwarebytes Endpoint Protection: Malwarebytes Incident Response: Malwarebytes Endpoint Security: Source Malwarebytes
80	764 SEC Microsoft	764 SEC Microsoft: Microsoft Security: Microsoft Secure: Source Microsoft
81	794 SEC Nozomi Networks	794 SEC Nozomi Networks: SCADAguardian: Central Management Consoles: Operational Anomalies: Real-time Cybersecurity and Visibility for Industrial Control Networks: Source Nozomi Networks
82	806 SEC Oracle	806 SEC Oracle: Source Oracle
83	810 SEC Palo Alto Networks	810 SEC Palo Alto Networks: Application Frameworks: Cloud Security: Endpoint Protection: Next-Generation Firewalls: Remote Network & Mobile Security: Threat Detection and Prevention: Source Palo Alto Networks
84	832 SEC Pulse Secure	832 SEC Pulse Secure: Converged Management: Pulse Secure Enterprise Solutions: Secure Access to Cloud Apps: Source Pulse Secure
85	838 SEC Qualys	838 SEC Qualys: Infrastructure Security: Cloud Infrastructure Security: Endpoint Security: DevSecOps: Compliance: Web App Security: Source Qualys
86	844 SEC Radware	844 SEC Radware: Application Delivery Load Balancing: Application Network Security: Management Monitoring: Cloud Services: Source Radware
87	914 SEC Sophos	914 SEC Sophos: Unified Endpoint Management (UEM): Mobile Security Solutions: SophosLabs: Source Sophos
88	931 SEC Symantec	931 SEC Symantec: Endpoint Security: Endpoint Protection: Data Center Security: Cloud Workload Protection: Information Centric Security: Data Loss Prevention: Encryption: Advanced Threat Protection for Email: Messaging Gateway: Content Malware Analysis: WAN Optimization: Encrypted Traffic Management: Network Forensics Security Analytics: Source Symantec
89	940 SEC Tenable	940 SEC Tenable: Tenable.io: Vulnerability Management: Web Application Scanning: Container Security: Source Tenable
90	952 SEC Trend Micro	952 SEC Trend Micro: IOT Security: Security Intelligence: Source Trend Micro
91	973 SEC Vectra Networks	973 SEC Vectra Networks: Cognito: Threat Detection Response Platforms: Source Vectra Networks
92	975 SEC Veracity Industrial Networks	975 SEC Veracity Industrial Networks: Cerebellum: Source Veracity Industrial Networks
93	993 SEC Waterfall	993 SEC Waterfall: Unidirectional Gateway Solutions: Secure Bypass: Waterfall BlackBox: Waterfall CloudConnect: Source Waterfall

Prepared By:

**Strategic Efficiency Consortium Security  
Intelligence Data Workgroup + Digital Platforms Workgroup  
Security Intelligence Data Platform Services**

Document Release 7.00: January 2019  
Confidential & Proprietary  
Copyright 2019  
Strategic Efficiency Consortium Corporation

**SEC+ Blog**

[security.strategiefficiency.org/blog/](http://security.strategiefficiency.org/blog/)

**twitter**

[twitter.com/strategiefficiencyplus](https://twitter.com/strategiefficiencyplus)

**LinkedIn**

[linkedin.com/company/strategic-efficiency-consortium/](https://linkedin.com/company/strategic-efficiency-consortium/)