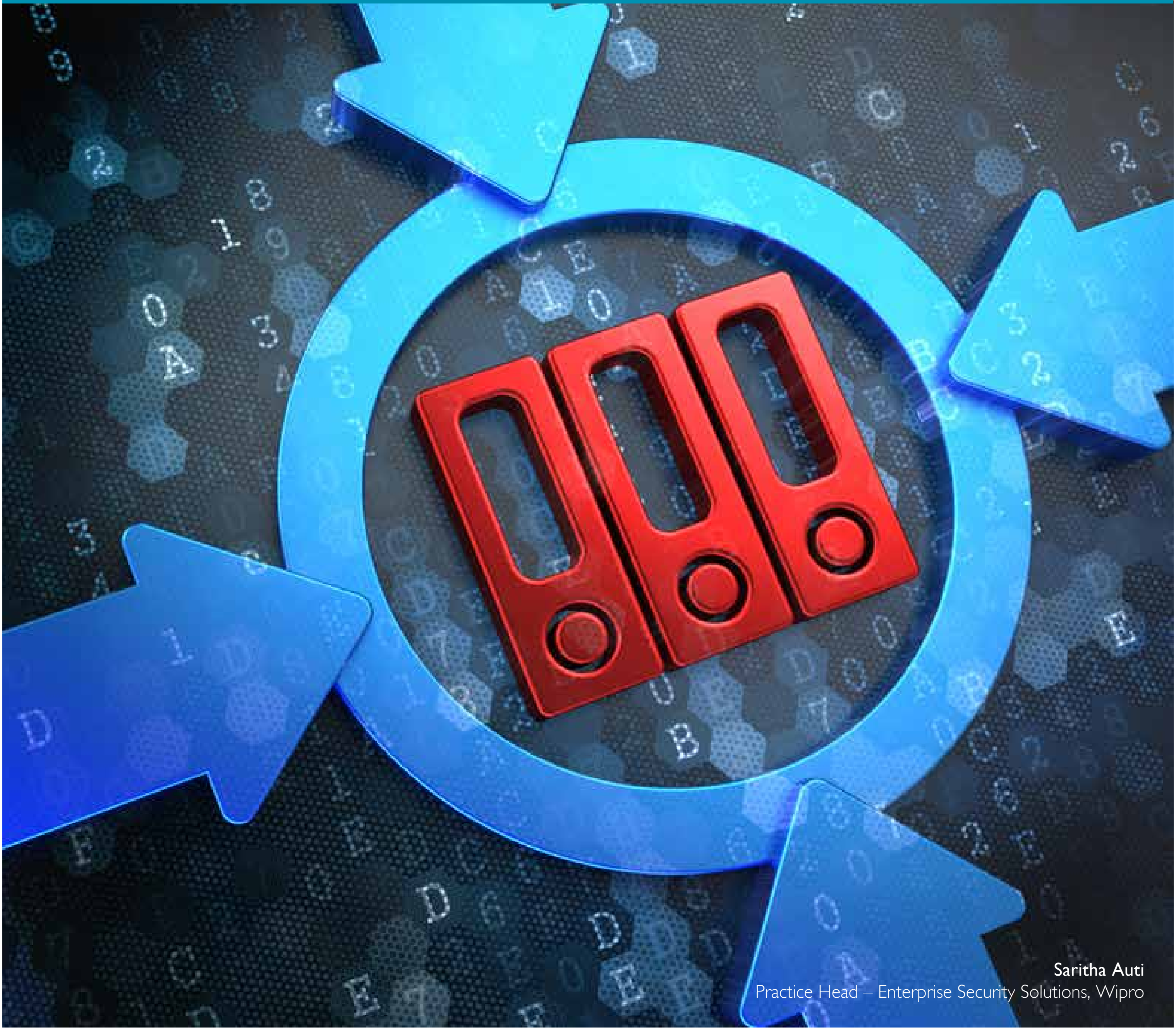
SECURITY ANALYTICS & INTELLIGENCE FOR CRITICAL INFRASTRUCTURE



Saritha Auti
Practice Head – Enterprise Security Solutions, Wipro

Table of Contents

Executive Summary

Organizations around the world today are dealing with a dramatic increase in the volume of digital information, and critical infrastructure is not any exception. It's not only business applications but also communication links and underlying control systems that are susceptible to cyber-attacks. This would also include critical infrastructure such as Energy, Oil & Gas, Banks, Retail, Healthcare, Pharmaceutical, Nuclear, and Natural Resources. Cyber Security is all about identifying critical information assets and protecting them from adversaries, assessing security posture, predicting threat actions, and preparing the ecosystem to handle visible and invisible threats.

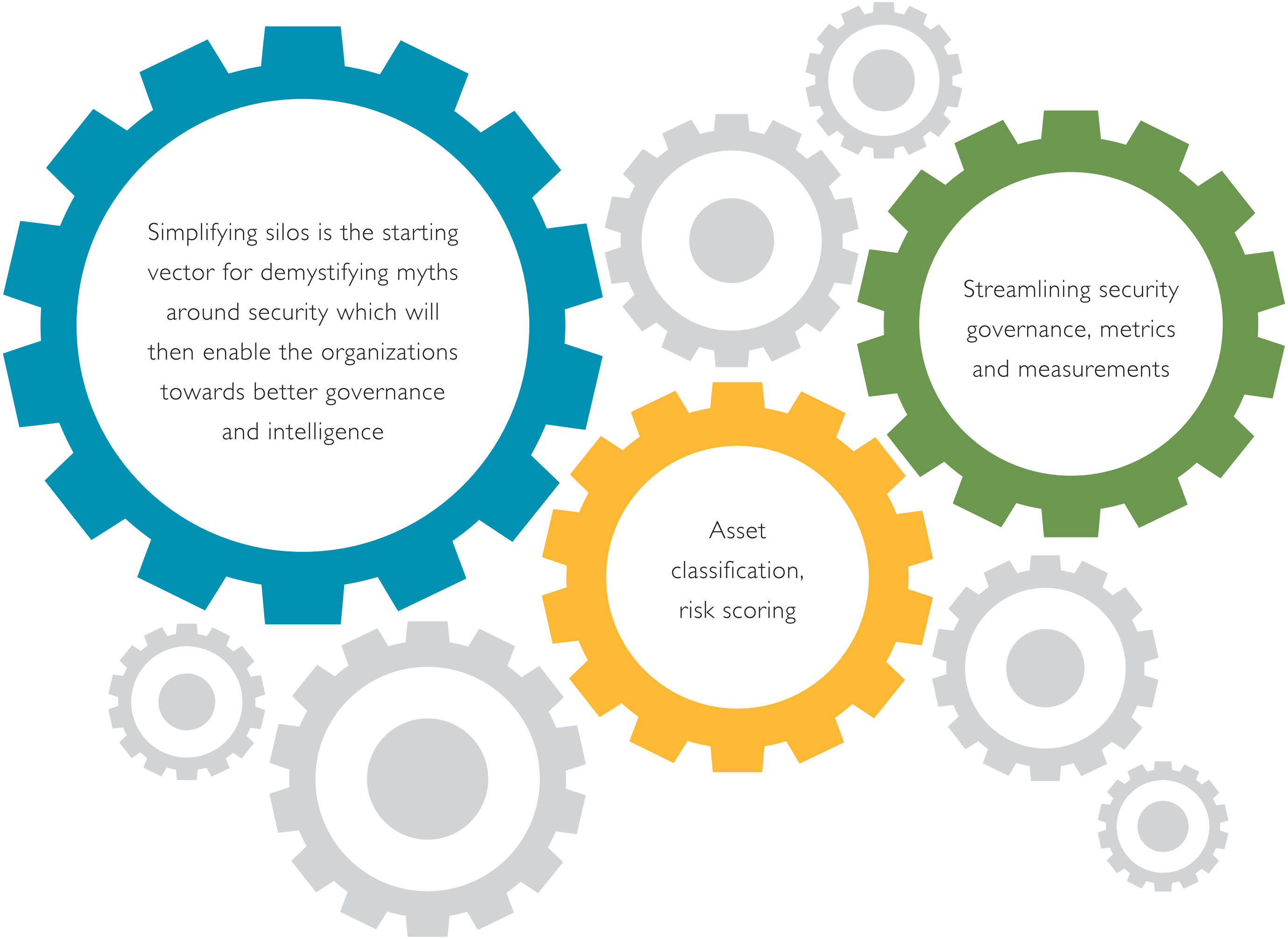
Cyber-attacks are an easy weapon for a wide range of adversaries with varied intentions since it is an easy route to covertly capture information and cause damage at specific points of critical infrastructure processes and devices where the true identity of an attacker can still be concealed. Increased level of automation in industrial networks, sophistication of threat matrices, lack of intelligence information about threat patterns, and upcoming threats have made cyber-attacks an organized crime sector with prime focus on economic, environmental and reputational impact.

In this paper, we will focus specifically on the nuances of cyber threats and how Security Analytics & Intelligence can lend industries a better security posture.

Demystifying "Myths" around Security

We are in an information-based economy where every information asset is valuable for a business process, product and service. Silos of information assets managed by yet another set of silos of systems, applications and products create redundancies and operational nuances and may create pathways for adversaries to enter the business and information ecosystem. Needless to say, this evolution has brought down the concept of air-gap networks, extending seamless operations across boundaries, opening the network for the new possibilities, business expansion and last but not the least, adversaries. Industries are not yet ready with appropriate governance to handle this, struggling to manage silos and trying to handle huge security operational data but not knowing how to utilize this data to obtain a better security posture.

The top three things organizations need to do before focusing on Security Analytics & Intelligence:



Simplifying silos is the starting vector for demystifying myths around security which will then enable the organizations towards better governance and intelligence

Streamlining security governance, metrics and measurements

Asset classification, risk scoring

Security Analytics & Intelligence in a Digital World

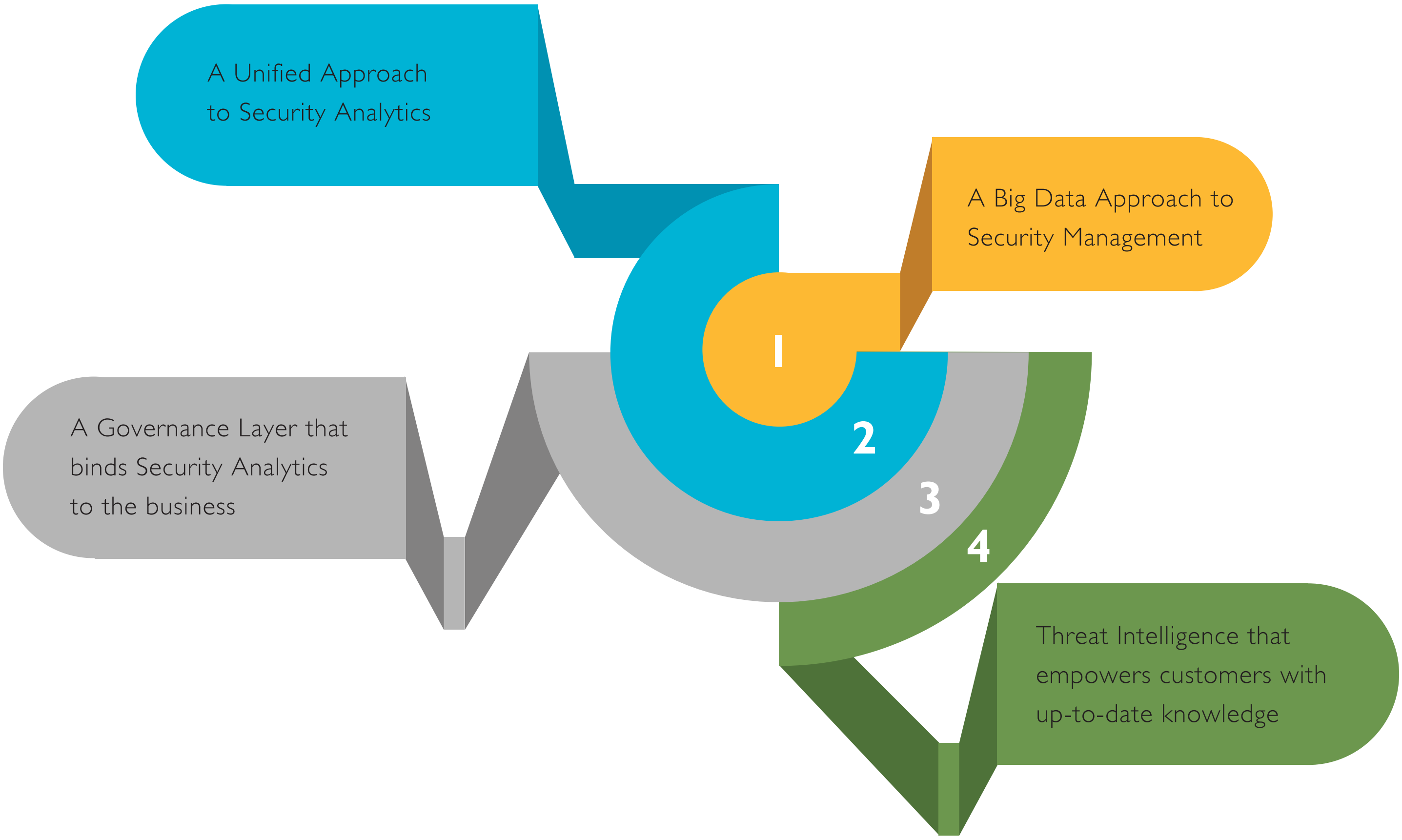
The hyper-connected nature of the digital world is delivering computing that not only creates incredible new opportunities for collaboration and innovation but at the same time, new vulnerabilities that adversaries have learned to exploit. Hyper-connectivity makes the nature of attacks more targeted, sophisticated and capable of being triggered from remote locations with minimal human intervention. It is for these reasons that organizations are considering to deploy a Defense-in-Depth security solution including Security Analytics & Intelligence.

A typical security intelligence platform heavily depends on Social, Mobile and Analytics to create predictive intelligence patterns that help protect information assets. Organizations as well as governments have vast quantities of data that can help detect threats and areas of high risk. However, this can be achieved only if there is a mechanism to collect, aggregate and, most importantly, analyze data from point security products, network device configurations, servers, network traffic telemetry, applications, end users, and their associated activities.

Security Intelligence reduces risks, facilitates compliance and is primarily driven by three aspects:

1. **'What We Know' and their associated actions** This involves collecting tons of data from internal and external sources, creating a pattern of threats and vulnerabilities and directing security applications and devices to handle the threats
2. **Preventive measures** – This involves timely feeding of security controls into the Security Analytics framework
3. **Forensics** – This involves carefully articulating "lessons learnt" and the subsequent corrective actions taken to understand the root cause of the vulnerability

There are multiple ways of implementing Security Analytics & Intelligence platform in a network:


A Unified Approach to Security Analytics
A Big Data Approach to Security Management
1
2
3
4
A Governance Layer that binds Security Analytics to the business
Threat Intelligence that empowers customers with up-to-date knowledge

?

What we know

Facts about intrusions reveal the need for continuous monitoring, need for robust security operational processes and security analytics for ICS/SCADA networks. 78% of intrusions are by "not specialized" hackers, 76% of intrusions exploited weak/stolen credentials, 84% intrusions happened in minutes, 66% of intrusions were undetected for months, and 69% of intrusions were first recognised by external parties

Security Analytics for ICS/SCADA network can:

Identify who is doing what, when, why and how in your network

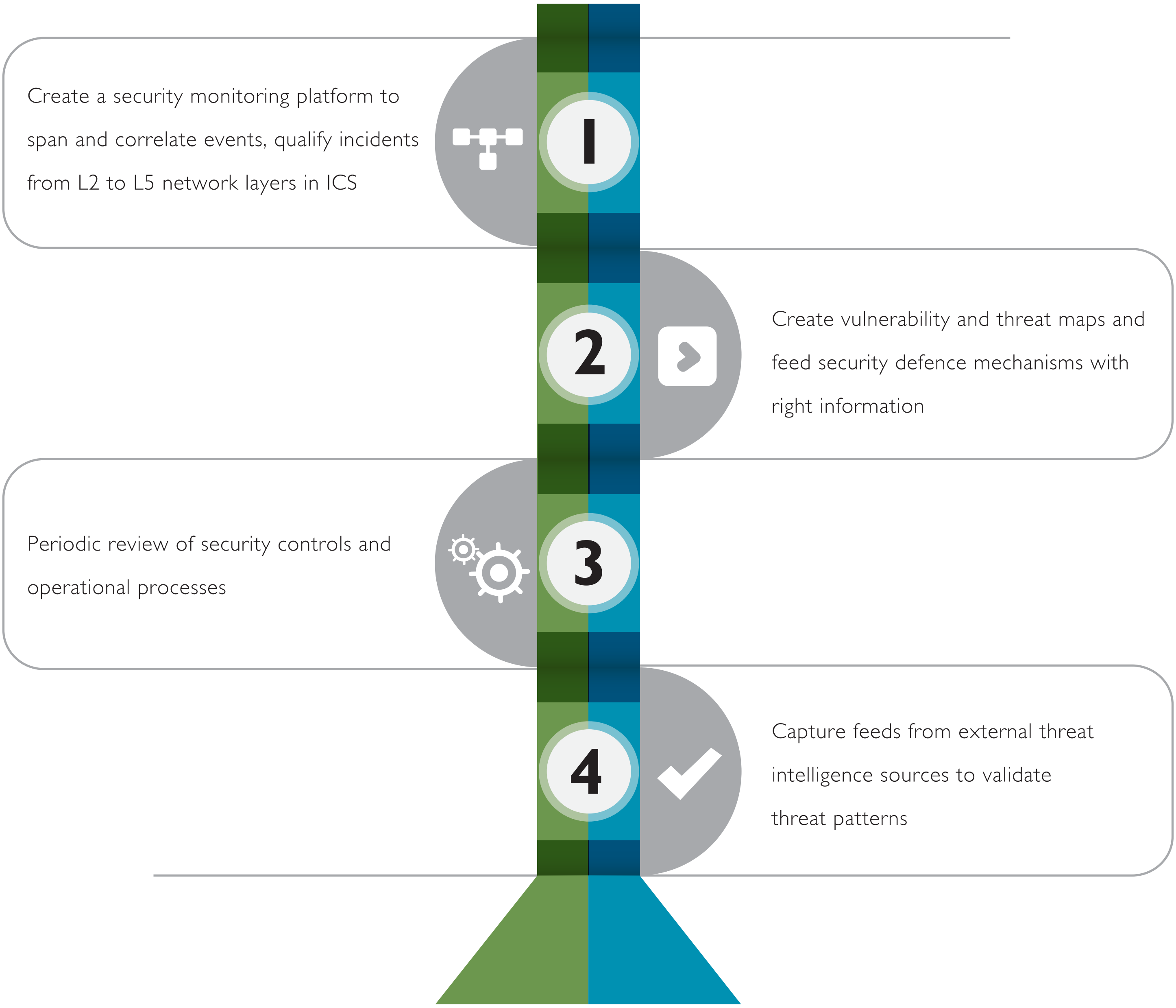
- Identify and evaluate threats to information assets based on the pattern mapping and correlation
- The presence or absence of the vulnerability
- The likelihood of an exploit based on attack-path threat models
- Configuration information which may indicate, for example, that the server is not accessible because a default setting has been changed
- The presence of protective controls such as an intrusion prevention system

Detect abnormalities in the network

- Map feeds from RTUs, IED and PMUs to the intelligence information, outage management, oscillation management and customer behavior to predict the threat actions
- Identify the operations pattern to identify the presence of a malware or suspicious transaction within the ICS
- The value the organization assigns to the asset or data

Although the above aspects are trivial, it can still bring down an ICS/SCADA network in less than a minute.

Preventive Measures



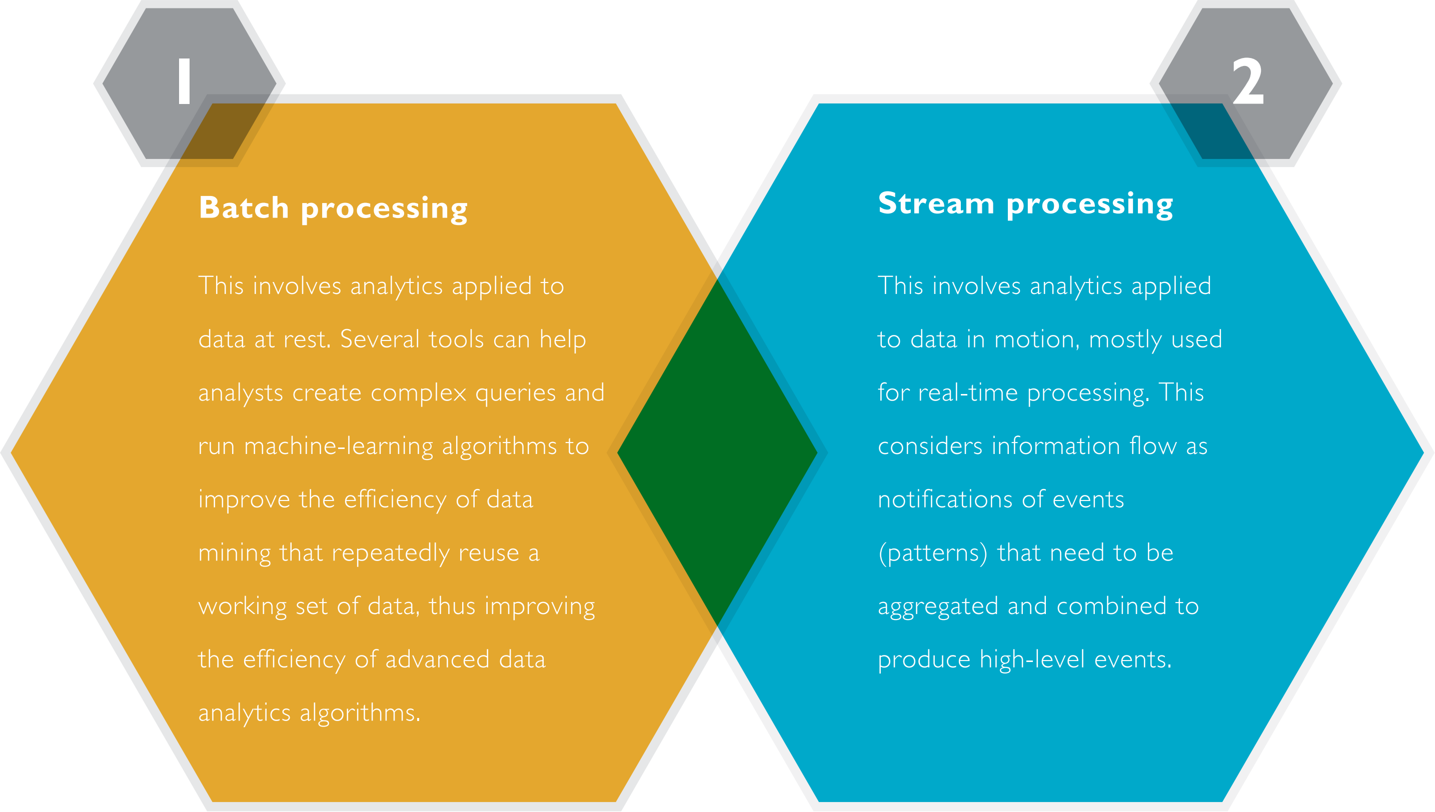
1. Create a security monitoring platform to span and correlate events, qualify incidents from L2 to L5 network layers in ICS
2. Create vulnerability and threat maps and feed security defence mechanisms with right information
3. Periodic review of security controls and operational processes
4. Capture feeds from external threat intelligence sources to validate threat patterns

By applying the Business Context to threat preparation, security teams will be in a stronger position to confidently allocate resources in a controlled manner in line with the impact values placed on assets that may be simultaneously under attack by multiple yet unrelated threats. Security Analytics includes capturing and analyzing a variety of data such as DNS transactions, emails, documents, social media data, full packet capture data, and business process data; all collected over years of activity. Security Intelligence platforms can provide organizations with vital details of malicious activity present within the organization's data through comprehensive analysis of structured and unstructured data.

Security Analytics leveraging a Big Data Platform

Most enterprises are moving from traditional Data Warehousing Platforms to the Big Data Platform in order to reduce cost of operations, increase the speed of query execution, correlation, and computing.

Big Data technology can be divided into two categories:



1

Batch processing

This involves analytics applied to data at rest. Several tools can help analysts create complex queries and run machine-learning algorithms to improve the efficiency of data mining that repeatedly reuse a working set of data, thus improving the efficiency of advanced data analytics algorithms.

2

Stream processing

This involves analytics applied to data in motion, mostly used for real-time processing. This considers information flow as notifications of events (patterns) that need to be aggregated and combined to produce high-level events.

The Impact of Big Data on the Critical Infrastructure

For instance, in the context of smart meter management, organizations are generally subject to multiple operational triggers (such as triggering of meter disconnect commands). However, there needs to be proper access controls which ensure that these triggers are not directly initiated from the control center, thereby preventing the Meter Data Management logs from failing. This would eliminate the possibility of a DDoS (Distributed Denial of Service) kind of attack. By creating behavioral patterns for control center commands and leveraging machine learning, companies can recognize and prevent such DDoS attempts.

Security Analytics for SmartGrids (Substation)

A real-world use-case of preventing grid failure due to anomaly

Preventing grid failure due to anomaly requires the integration of a Security Analytics & Intelligence platform with multiple network traffic management systems or data collection points in a control center. The entire setup may take about 3-4 months of time to build a pattern base for anomalies. Inputs considered to build a pattern are typically inputs from the process LAN and Station LAN such as sensor data, IED behavior, commands which trigger overloading of grids, changes in the oscillation of PMU, multiple login attempts, password reset attempts, mismatch of command initiation, time slot for the execution, etc.

By analyzing the converged network traffic in real-time and mapping this to the security pattern base, security analytics can contextualize the patterns based on the rule sets to validate events and incidents, determine threat levels, and create a threat perception. It can also trigger alerts, notification and remediation workflows based on a Set of Procedures (SOP) configured in Security Monitoring or Alert Management systems.

This convergence helps get a unified view of the network thereby enabling more efficient use of Security Analytics & Intelligence to prevent grid failure.

Conclusion

Security management across organizations tends to be more mature for the enterprise side of the business rather than the operational networks that form a bulk of critical infrastructure. These operational networks are still in the architecture transformation phase of moving from silos into the layered network architecture.

Implementing Security Analytics & Intelligence requires data feeds from all sources, be it security operations, management platforms, control center operations of grids, oscillations from the PMUs, frequency of the wind turbines, inputs from PLC, detecting the changes to the comtrade files, IED configurations, etc. along with the feeds from unstructured data sources for computing and correlation. Though Security Analytics & Intelligence look like essential technology requirements in the context of Critical Infrastructure, the reality is that it is still in the process of embracing this platform by shredding the silos, deploying Defense-in-Depth security solutions, streamlining governance and classifying critical assets. Once these processes are adopted, Security Analytics & Intelligence will play an instrumental role in critical infrastructure protection.

About the Author

Saritha has over 17 years of experience in Enterprise Security & Architecture, spanning a wide gamut across product development, application security, systems integration, enterprise architecture and security architecture consulting. She heads Enterprise Security Architecture and Industrial Security Practice for Wipro with specific focus on Critical Infrastructure Security. She has devised several security solutions and architecture strategies for Oil & Gas, Telecom, Financial Sectors, Utilities, Defense, and has led Security Architecture transformation programs. Apart from technology she is an ardent trekker, culture enthusiast and loves connecting with people.

To know more, contact: saritha.auti@wipro.com

About Wipro Ltd.

Wipro Ltd. (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology" - helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation and an organization wide commitment to sustainability, Wipro has a workforce of 140,000 serving clients across 60 countries.

For more information, please visit www.wipro.com.

WIPRO
Applying Thought

DO BUSINESS BETTER

NYSE:WIT | OVER 140,000 EMPLOYEES | 60 COUNTRIES

CONSULTING | SYSTEM INTEGRATION | OUTSOURCING

WIPRO TECHNOLOGIES, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA. TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256, Email: info@wipro.com

North America South America United Kingdom Germany France Switzerland Poland Austria Sweden Finland Benelux Portugal Romania Japan Philippines Singapore Malaysia Australia China South Korea New Zealand

IND/BRD/APR 2014-JUN 2015