21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2015 Grid of the Future Symposium

Threat Intelligence Management (TIM)
Transmission Security Operations Center (TSOC)

B.L. GAINES
FirstEnergy
USA

SUMMARY

Attacks are becoming more sophisticated, the attack techniques are constantly evolving, and defensive security measures are predictable. According to *Under cyber attack; EY's Global Information Security Survey 2013* (GISS)*, 59% of respondents have seen an increase in external threats in the last 12 months. A target's systems are going to have a firewall, antivirus, email, and passwords. Their facilities will have a fence, an alarm, and maybe some cameras. Determined, malicious actors will stop at nothing to compromise or attack an organization. It has been said that compromise is not a question of *"if"* but *"when*." Very sophisticated attacks will evade detection - potentially for weeks or even months.

With every operational and technical advance that we make for the sake of productivity: remote access, mobility, bring your own device; organizations broaden their attack surface and exposure. We have complex systems and their management is distributed across the enterprise. High value targets, such as SCADA systems, further entice attackers to take advantage of an organization. Many organizations, are doing an excellent job with prevention. They have layered defenses, real time alerting, operational monitoring and security awareness training. In the light of threats and vulnerabilities in world today, it would be prudent to focus more attention from reacting to attacks and instead to getting ahead of threats, while quickly mitigating vulnerabilities and minimizing the impact, damage, and loss to the business from potential compromises that could occur. "Leading organizations are doing more than improving on their current state. They are seeking to expand their efforts — take bolder steps — to combat cyber threats. Rather than waiting for the threats to come to them, these organizations are prioritizing efforts that enhance visibility and enable a proactive response through monitoring and prompt detection. Organizations may not be able to control when information security incidents occur, but they can control how they respond to them. The best way to reduce that impact is to catch and remediate those attacks as quickly as possible. To accomplish this, it's important to increase our awareness of indicators, detect threats and respond to incidents in a quick and efficient manner. The data needed to achieve this goal exists, however, there is not only an overload of data, but it's acquired using different tools, stored in discrete systems, and monitored by different teams.

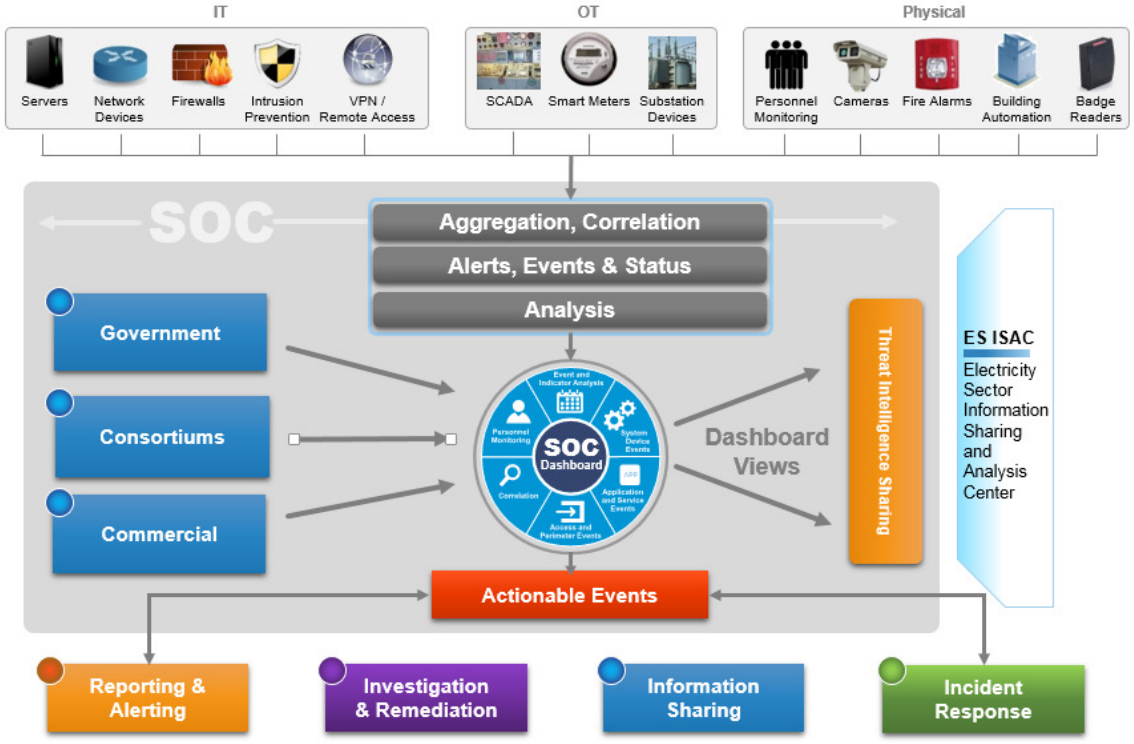
KEYWORDS

Threat Intelligence Management, Transmission Security Operations CenterConvergence

bgaines@firstenergycorp.com

1. Solution

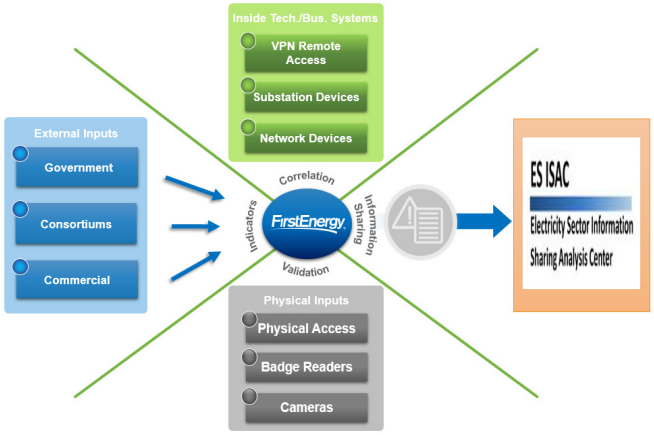
The answer to this need is to create a Threat Intelligence Management program. This critical function would provide enhanced visibility of the enterprise security posture. This is accomplished by unifying the monitoring of Cyber Security, Physical Security, Information Technology, and Operations Technology. Upon aggregation and event correlation, advanced analysis is performed to provide an early warning system for security incidents and rapid mitigation of vulnerabilities.



Further advanced analysis is performed on the correlated data by security teams - to augment real time correlation from the Security Information and Event Management (SIEM) and related tools. Using this analysis, the teams develop requirements and identify indicators while designing the logic for additional use cases to identify trends and emerging threats. The resultant output would then be validated to ensure that the use cases are appropriate to accurately identify those threats and the overall picture regarding the organization's security posture. The ultimate use of this data is to share with internal business units and external partners, such as the Federal Government or sector specific information sharing organizations, as part of an overall threat intelligence collaborative. The benefits of this collaborative would assist in: identifying and communicating previously undetected Advanced Persistent Threats (APTs); communicate precursors of upcoming attacks; provide indications of 0-day vulnerabilities; and develop and share mitigation strategies, use cases, firewall and IPS rulesets, etc.

1.1 Framework

As a practical matter, an organization can achieve these objectives by integrating global intelligence into their established security technologies and practices, following a framework that includes these elements:



Planning—Organizations need to decide what levels of protection they need to apply to their information assets on a granular basis, department by department. This allows them to prioritize intelligence requirements, establish a strategic blueprint for protection, and outline intelligence workflows with both internal and external roles and responsibilities.

Collection—Typically, spending on internal intelligence collection, using intrusion detection solutions, for example, is already significant. Augmenting it using external global intelligence networks and third-party data feeds like botnets, Darknet, and peer-to-peer alternatives extends protection to cover emerging threats and preserves the value of legacy security investments. Collection infrastructure often includes a console or portal to make collected information available inside the organization.

Analysis—The "heavy lifting" of intelligence, analysis includes integration across multiple information sources, correlation to identify potential threats, and evaluation to determine the degree of risk each threat represents—culminating in the identification of root causes and bad actors, with recommendations for defenses or countermeasures.

Dissemination—Typically shared by organizations and their external intelligence partners, dissemination includes early warning communications, customized action reports, and personal contact between internal security specialists and external intelligence analysts.

Adaptation and enhancement—"Closing the loop" is also a shared responsibility in which intelligence partners develop event metrics and use cases and identify protection, detection, infrastructure, and analysis.

A new generation of security data-mining tools uses innovative techniques to collect and analyze massive amounts of data: data from PCs, mobile devices and servers; data from internal networks, including the composition and content of network packets; and threat intelligence about attacks on other organizations and the tools and methods used. In addition to analyzing these traditional information sources, "big data" security tools also can obtain information from non-traditional sources such as building key card scanners, personnel records and even Microsoft Outlook calendars. Such data may be used, for instance, to assess the legitimacy of remote log-ins by employees.

The heightened visibility provided by the big data capabilities of new security analytics platforms create unprecedented opportunities to identify anomalies, uncover evidence of hidden threats or even predict specific, imminent attacks. More data creates a richer, more granular view: it presents the threat landscape in high definition, as opposed to grainy black-and-white. Security-related details can be seen in sharper focus and irregularities can be found faster.

1.2 Security Indicators

As stated previously, it is important to see the threat landscape as a concern. Therefore, inputs from external sources are critical to threat intelligence. A number of sources are available, from the government, consortiums and commercial providers. The established sources we are using today include: CISCP, a threat awareness cooperative between DHS, US-CERT, ICS-CERT and private organizations; ES-ISAC, the information sharing and analysis center for the electric sector; Commercial services that informs customers of vulnerabilities and patches via alerts; and most recently, CRISP, the cybersecurity risk information sharing program which uses automated sensors to detect malicious traffic attempting to compromise networks.

The data from these sources is important to the overall security vision, as it provides additional alarms and events that the organization is not experiencing at the present time. The knowledge gained from other organizations witnessing these attacks and events allows for use cases that are proactive to quickly identify when such events occur on the company's systems.

Department of Energy

Cybersecurity Risk Information Sharing Program (CRISP)

The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership that provides for the sharing of cyber threat information and producing situational awareness tools to identify, prioritize, and coordinate the protection of the Electrical Sector's critical infrastructure. CRISP allows for critical infrastructure owners and operators to voluntarily share, in near-real-time, cyber threat data, analyze this data, and receive machine-to-machine mitigation measures from other participants.

CRISP began as a partnership between the Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE/OE), the North American Electric Reliability Corporation (NERC)'s Electricity Sector Information Sharing and Analysis Center (ES-ISAC), Pacific Northwest National Laboratory (PNNL), Argonne National Laboratory (ANL), and participating companies. More companies are being added as participants, of which, FirstEnergy is one.

Department of Homeland Security

Enhanced Cybersecurity Services (ECS)

As the federal government's lead agency for coordinating the protection, prevention, mitigation, and recovery from cyber incidents, DHS works regularly with business owners and operators to strengthen their facilities and communities. To accomplish this, the DHS Enhanced Cybersecurity Services (ECS) program was expanded in February 2013 by Executive Order - Improving Critical Infrastructure Cybersecurity.

ECS is a voluntary information sharing program that assists critical infrastructure owners and operators as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops indicators based on this information and shares them with qualified Commercial Service Providers (CSPs), thus enabling them to better protect their customers who are critical infrastructure entities. ECS augments, but does not replace, an entities' existing cybersecurity capabilities.

North American Electric Reliability Corporation (NERC)

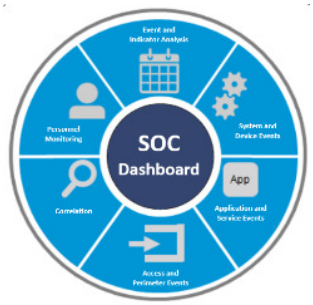
NERC was founded in 1968 by representatives of the electric utility industry, for the purpose of developing and promoting voluntary compliance with rules and protocols for the reliable operation of the bulk power electric transmission systems of North America.

NERC's mission is to improve the reliability and security of the Bulk-Power System in the United States, Canada and part of Mexico. The organization aims to do that not only by enforcing compliance with mandatory reliability standards, but also by acting as a catalyst for positive change—including shedding light on system weaknesses, helping industry participants operate and plan to the highest possible level, and communicating lessons learned throughout the industry.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The ICS-CERT partners with members of the control systems community to help develop and vet recommended practices, provide guidance in support of ICS-CERT incident response capability, and participate in leadership working groups to ensure the community's cyber security concerns are considered in our products and deliverables.

The ICS-CERT facilitates discussions between the federal government and the control systems vendor community, establishing relationships that foster a collaborative environment in which to address common control systems cyber security issues. The ICS-CERT is also developing a suite of tools, which will provide asset owners and operators with the ability to measure the security posture of their control systems environments and to identify the appropriate cyber security mitigation measures they should implement.



1.3 Security Operations Center

The Transmission Security Operations Center (TSOC) is a concentrated set of sophisticated technologies and processes that provide enhanced visibility, correlation, real-time analysis and incident awareness of security events. The goal of the TSOC is to provide a single pane of information spanning IT, OT, Physical and Cyber security. The TSOC would monitor and handle investigations with high efficiency and greater effectiveness than previously experienced in most organizations.

Threat Scerino

Take a scenario that could easily play out in any electric utility, at 0300 a contractor badges into a substation. He has access to this substation as part of a build-out initiative that is underway throughout the company and has been working to install the network at that location. A network device was installed earlier in the week and the network was turned up, providing connectivity to the

substation and corporate networks. The contractor unplugs the device and connects a laptop he brought with him. He begins a portscan and host sweep to identify targets on the system that could be used at a later date to compromise or degrade systems on the network. In the past, these events would be alarmed and dealt with separately with no correlation to identify a major event.

The TSOC would correlate these events based on location, a use case would exist that identifies the badge access at an unconventional time, loss of device connectivity and a portscan originating on the substation network to become a high priority event. Correlation as it exists in most products today, may identify the two logical instances. The physical portion identifying the access to a location prior to the beginning of the events, would quickly identify a possible actor and what scenario is playing out.

Investigation & Remediation

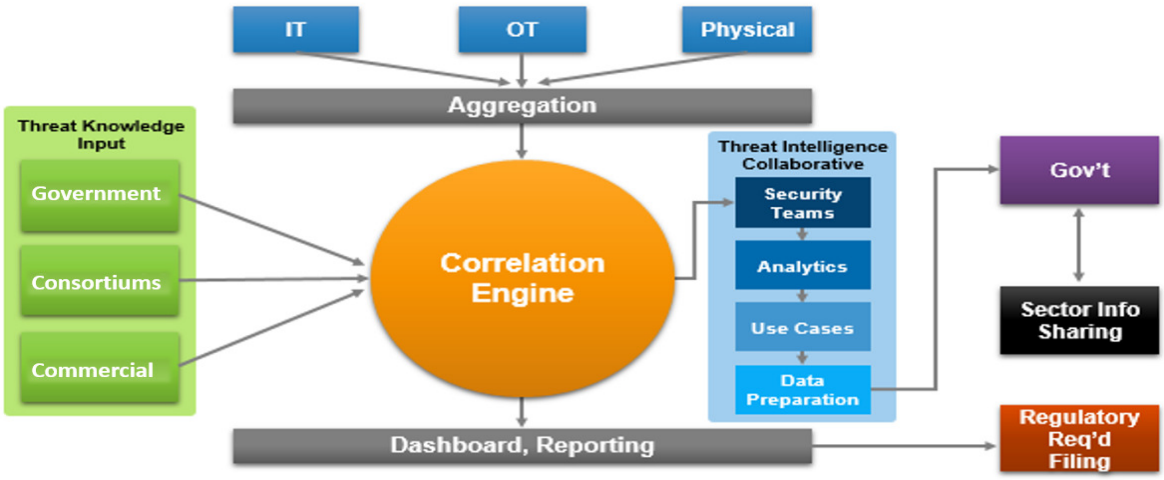
The TSOC, upon identification of the high event, could immediately begin viewing/recording feeds from the camera at the site to obtain license plate data and photos of the actor. Logs could be gathered from the SIEM tools and other devices at the location. These investigative processes would feed into the Incident Response phase.

Incident Response

As part of incident response procedures, network ports could be shut down to stop the device attached by the contractor. Voice announcement systems, if available at the site, could be used to alert the actor that his actions are being monitored and recorded.

Reporting & Alerting

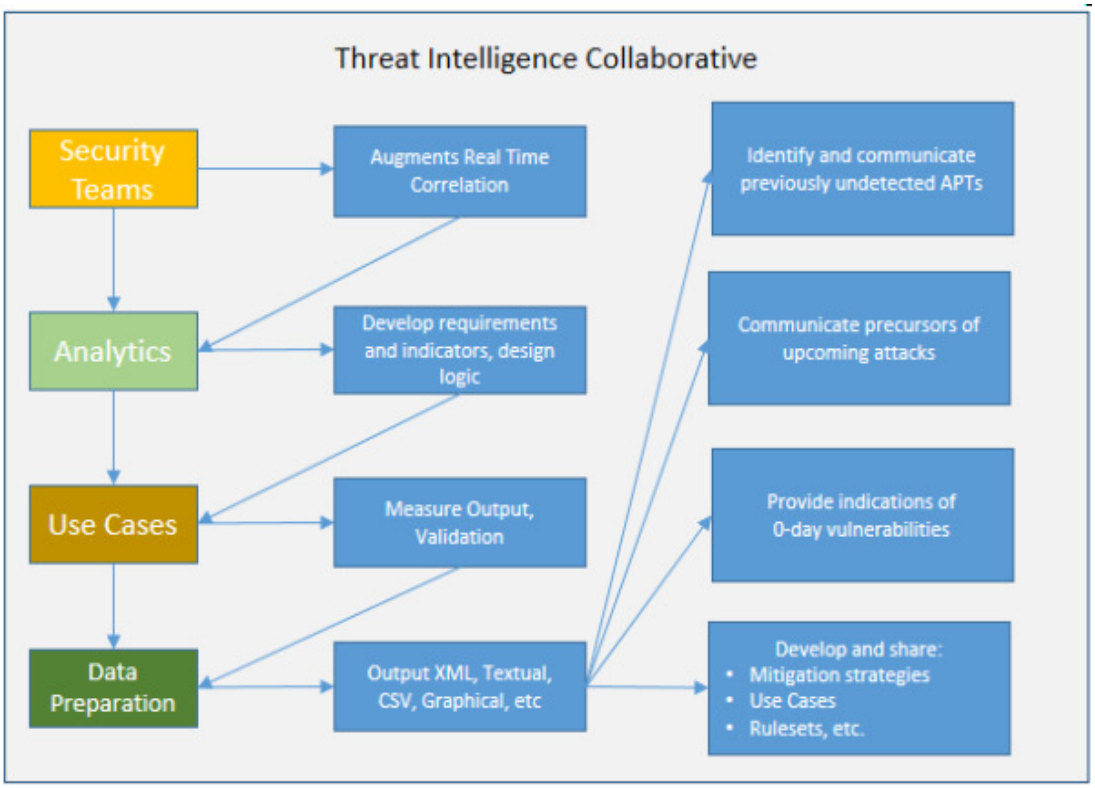
Prior to shutting down ports and announcing to the actor that he has been identified, law enforcement could be contacted to apprehend the contractor to face prosecution. Evidence gathered by the investigative phase will supply the needed data for prosecution efforts. Additionally, this information could be shared to alert others in the industry that there may be others like our contractor and to watch their remote locations for such actions.



1.4 Threat Intelligence Management

Information Sharing

One of the paramount goals of TSOC is to provide threat intelligence that can be shared. In order to ensure protection of critical infrastructure there must be a flow of information from every corner of critical infrastructure to anticipate and detect threats. The data obtained as part of TIM can be shared amongst government and industry partners to provide awareness of threats and early warning information for better mitigation of attacks. By providing this information, a better security posture can be achieved for critical infrastructure. Industry information sharing centers can share this information further with other industries to ensure the entire critical infrastructure landscape is protected.

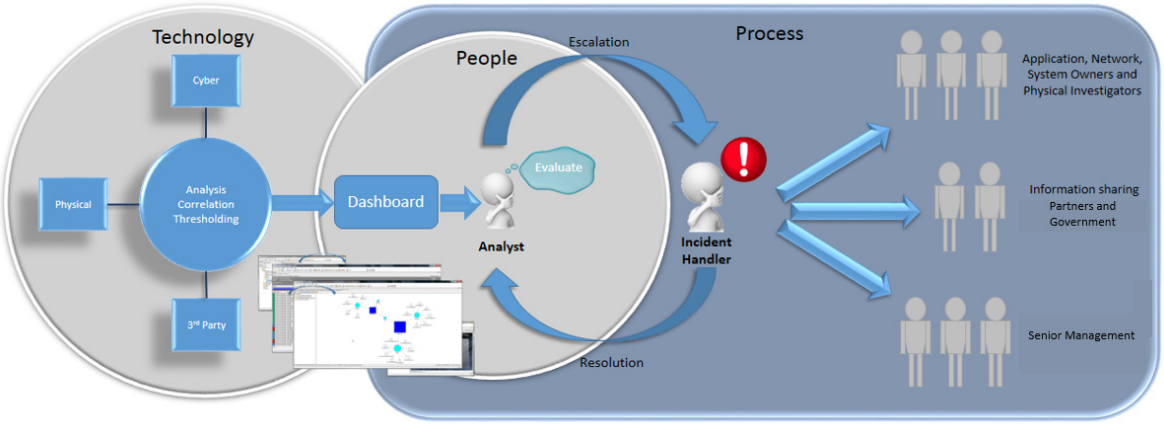


What type of information gets shared? The obvious answer is information which would be actionable by other organizations. While IP addresses, file hashes and phishing characteristics make perfect sense to share, more holistic information regarding nature of attacks, e.g. flood of packets directed to network with a source port of X, targeting one host, along with mitigation strategy – blocked all traffic with a source port of X, directed at Y host, with payload Z. This removes the simplistic blocking method of using reported bad hosts attacking networks and provides the patterns of the attack to not only detect, but also to prevent the attack from occurring. Previously, simply blocking offending hosts was sufficient, however with spoofed traffic becoming the de facto method of attack, it is important to look beyond simple IP blocks and move toward prevention based on pattern matching the attack.

The data will require sharing in a number of formats based on its expected use. XML and CSV feeds will be generated for use within filtering or log parsing functions, creation of firewall or IPS rules, or any number of products or processes that would make use of data regarding IP addresses, hashes, filenames, email addresses and other indicators. Use cases created for certain SIEMs could be shared to allow other organizations to detect and correlate threats in their environments. Firewall and IPS rules will be shared to assist other organizations an efficient source of mitigation assistance against

new vulnerabilities and attacks. Finally, reports regarding security disposition will be generated and shared to provide an overall view of the health and safety of critical infrastructure within the US.

2.0 Requirements



2.1 Technology

Support of Disparate Data Feeds

It is imperative that the solution will be able to handle data from numerous systems. Traditionally it was focused on purely IT and Cyber Security data (firewall, IPS, security logs). TIM will go beyond that to include, not only IT and Cyber Security data, but Operational Technologies (for our industry SCADA and other BES devices), Physical Security (such as cardkey, thermal cameras, alarms), External feeds (3rd party threat information from DHS or vulnerability feeds from Security Tracker), Ad-hoc data that can be inputted manually and information from our vulnerability scanners to determine exactly what is the exposure on our cyber assets.

Aggregation and Normalization of Data

A cornerstone to the function of TSOC is to normalize the data received from very different sources and aggregate this data into meaningful occurrences of events. The tools used to perform this task must have: a filtering capability that can separate the "wheat from the chaff"; the functionality to provide a summary of identical/similar events; the ability to define additional custom aggregations; and be able to map key data elements from disparate logs as part of its "normalization" of events (using time, host, location, etc.).

Identity Management

Due to the TSOC functionality of pulling together feeds that do not always have specific matches amongst all of the data, it is important that the solution normalizes the data to map people to the devices and locations they use or frequent. This would involve such scenarios as mapping the IP address of a workstation to a user based on the ID used on that workstation. Identifying use of shared accounts, not only the functions performed and one which systems, but by the personnel using that account. Additionally, flagging use or attempted use of terminated employees/contractors accounts and ID badges. Production of personnel-based activity reports to determine their status during any point in time, will be a key output as part of TIM for the internal organization.

Location Awareness

The solution must contain location awareness, to tie those events that come from different domains (physical, cyber) to a building, room, etc. A series of small events that different teams would be made aware of would provide a bigger picture and indicate a larger incident at a location if analysts are

provided a contextual location for the events. A perimeter breach alarm at a remote substation would be alarmed to a physical security team which may elicit a call to authorities or personnel to investigate. The sudden loss of network connectivity for a device at that substation would be alarmed to an entirely different function and a separate team dispatched for investigation. The two events, however, taken together would indicate a malicious actor is within the substation and that the intent is to disrupt operations in some way. Law enforcement could quickly be dispatched to reduce the risk to personnel, should that perpetrator be armed and dangerous.

Correlation

- Pre-built use cases
- Custom use cases
- Thresholding (x events in y time)
- Associate events based on key data (location, identity, IPs, time, signatures)
- Filtering capability
- Pattern detection

Dashboard

It's important for the dashboard of the solution to be fully customizable so that the analyst's view can be tailored for specific needs. This would include the minimization of superfluous events, the ability to view graphs of bandwidth utilization (both internal and external), the ability to view video surveillance, and the integration of real time threat feeds.
Additionally, the ability to create custom dashboards tailored for a specific user experience would be required. This would allow the creation of executive dashboards, custom operational dashboards, and facilitate a tiered analyst approach.

Reporting

The solution will need to be able to both generate reports for interdepartmental collaboration and export data that can be sanitized and shared with government and industry partners.

2.2 Process

Event Detection

Event detection will occur on the SIEM Console, individual events can be displayed, but it is important that those correlated events "roll-up" to a more substantial event when necessary and are predominant amongst the less critical events. Individual event interfaces, such as those for AV, facility security Access and monitoring, Building Automation, Firewalls and IPS should be available for situations that require a deeper inspection into the source of events.

Triage and initial research

Threat Intelligence Management will require the ability to perform triage and intial research on those events that have or could develop into incidents. The goal to minimize the impact to the organization and ensure swift closure.

Problem Correction

In those cases where misconfiguration or process breakdowns occur that do not rise to the level of an incident, there is value provided to quickly identify the issue and inform the responsible parties of the problem. Those parties can perform the necessary steps to remedy any items or processes that would or could contribute to a greater outage, hazard or breach. This increases overall organizational efficiency and uptime. Doing this will require numerous inputs that, while not necessarily prima face security events, can contribute to or indicate a threat or vulnerability if left unaddressed.

Security Systems and Software

As we start generating events and output from the tools used by TSOC, it is inevitable that there will be use cases that are going to generate false positives and others that never generate actionable data because the thresholds are too low. There will need to be a process by which we're constantly reevaluating our existing use cases and looking for opportunities to create new ones based on the events being sent into the tools. That process will involve review of events generated, examining trends and testing the use cases within the tools. From the output, the process will foster creating corrective IDS/IPS and Firewall rules in those cases for network based traffic and additional detection routines for physical security measures.

Persistent Threat Investigation

A process that will have immediate value is the persistent investigation of threats and attacks. Currently, most organizations have a reactionary process around threats. One of the goals of TSOC, is to ensure a proactive approach to identify threats and perform mitigation to either eliminate or minimize any impacts from those threats. A continual investigative process to security threats ensures that focus in on the health and safety of the organization and its people and assets. Instead of juggling events and incidents as they come to light and escalate quickly, a methodical approach to identifying and addressing those contributing threats allows for little or no effect on the organization.

3.0 Conclusion

Building a well thought out Threat Intelligence Management program will result in more threat indicators, improved security, greater critical infrastructure resilience, and ultimately more industry and government collaboration. Presidential Policy Directive 21 identifies “critical infrastructure security and resilience” as the shared responsibility of "Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure".

President Obama, in the *National Strategy for Information Sharing and Safeguarding*, writes:

> "As President, I have no greater responsibility than ensuring the safety and security of the United States and the American people. Meeting this responsibility requires the closest possible cooperation among our intelligence, military, diplomatic, homeland security, law enforcement, and public health communities, as well as with our partners at the state and local level and in the private sector. This cooperation, in turn, demands the timely and effective sharing of intelligence and information about threats to our nation with those who need it, from the President to the police officer on the street."

Further, in Executive Order 13636 “Improving Critical Infrastructure Cybersecurity”, the Obama Administration emphasized the need for robust information sharing amongst all critical infrastructure. The TIM program achieves a “perihelion” for information sharing. The Threat Information Management program brings us to the closest point to not only our own identification and analysis of threats and attacks, but functional and effective information sharing amongst critical infrastructure. The knowledge sharing output of the process will pave the way to foster collaboration. While any information can be shared, it must be aggregated, correlated, analyzed and distilled to be relevant and actionable. The goal is to ensure a secure critical infrastructure that is as resilient as it is protected from threats and attacks.

BIBLIOGRAPHY

[1] Under Cyber attack: EY's Global Informaiton Security Survey, 2013
[2] EMC – Storage Report, 2013
[3] Cybersecurity Risk Information Sharing Program (CRISP)
[4] Department of Homeland Security - Enhanced Cybersecurity Services (ECS)
[5] North American Electric Reliability Corporation (NERC)
[6] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
[7] Department of Homeland Security – CRADA - Cyber Information Sharing Collaboration Program (CISCP)
[8] Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
[9] Presidential Policy Directive 21
[10] Executive Order 13636 "Improving Critical Infrastructure Cybersecurity"