Georgia Tech Research Institute

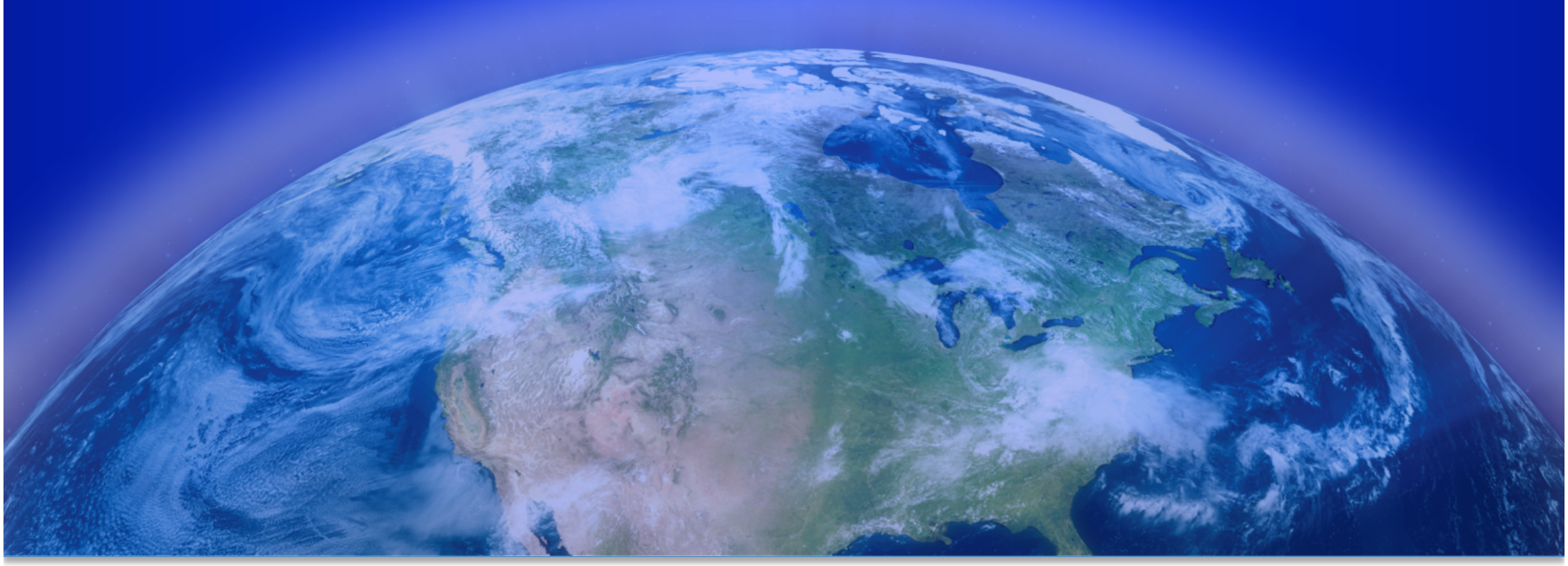
Problem. Solved.

Developing a Framework to Improve Critical Infrastructure Cybersecurity

National Institute of Standards and Technology (NIST)
Request for Information
Docket Number 130208119-3119-01
Document Number 2013-04413

Submitted by:

Thomas Dunn
Cyber Technology and Information Security Laboratory
Georgia Tech Research Institute
250 Fourteenth St.
Atlanta GA 30318



Georgia Tech Research Institute Cybersecurity Framework

The Georgia Tech Research Institute (GTRI) is the Georgia Institute of Technology's applied research institution. Established in 1934, GTRI pursues a strategically focused and synergistic model of research, innovation and education that is continually enhanced and applied to solve the problems of a complex world. GTRI's strengths are based on: world-class subject matter experts in systems engineering, sensors, and information and telecommunications technology; a unique laboratory infrastructure; and collaboration with Georgia Tech's academic colleges as well as access to the vast intellectual resources of one of America's premier research universities.

GTRI plays a "white-hat" role between industry and government by performing cutting edge work to help secure national critical infrastructure entities. We research the backbone that our nation's critical infrastructures depend on. GTRI has developed a unique cybersecurity framework that is both minimally disruptive and cost-effective. As our framework has evolved, we have identified key practices that pertain to securing critical infrastructure computer networks. The GTRI framework focuses on the following three interrelated core practices:

- Preventing, Detecting and Responding to Cyber Weaknesses
- Threat Intelligence
- Continuous Testing

Preventing, Detecting and Responding to Cyber Weaknesses

GTRI implemented an Information Security Operations Center (ISOC) that functions as the key player in all our cyber incident responses. It detects anomalies, categorizes incidents based on the impact they have on the GTRI environment and informs the appropriate response leads for remediation. Part of our incident response framework is learning from the incident, determining what went well and what we should change to prevent future incidents.

The core of the ISOC is an event correlation engine that consolidates all of our security, authentication and network traffic logs regardless of data source. These logs are useful for both detection as well as later forensics. GTRI has researched standards to guide which logs to correlate and which devices to fully log. This engine allows the ISOC staff to search for any indicators of a cyber incident, such as a source IP address or DNS name, regardless if it was logged by a firewall, IDS, or antivirus suite. A correlation engine such as this is a critical first step in cybersecurity response. No organization responsible for critical infrastructure will be able to respond to an incident without it.

It's imperative to know exactly what is going into and out of critical infrastructure communication networks. We have integrated a full network forensics capability with our correlation engine. Full network forensics provides the infrastructure for full-packet capture of critical nodes in an organization's network. The needs of the organization, as well as its risk profile will determine the length of time to preserve both security logs and network forensics.

Threat Intelligence

Sharing intelligence about ongoing cyber attacks is critical. The more "good guys" know about the threat landscape, the better we can collectively fight the threat. At the same time companies are, understandably, hesitant to share information about incidents they experience (such as the discovery of malware on one of their systems). GTRI has developed Titan to help overcome that problem. Titan community members can anonymously contribute malware samples, which are then analyzed and all results are shared with the community. Through Titan, all members benefit from sharing information. The Titan community is a diverse group of those interested in security: ranging from companies, government agencies, academia and individual researchers.

GTRI curates one of the largest catalogs of malware, which can be invaluable during the early stages of incident response. The Titan software framework performs malware analysis and threat intelligence based on about 150,000 malware samples from contributions around the world each day. New samples are triaged and scheduled for appropriate behavioral analysis modules. Analysis modules can determine with which hosts malware communicates (by IP address or hostname), capture malware's raw network traffic, identify files it accesses, identify registry records it alters, record its call stack trace, etc. Additionally, Titan correlates disparate sample submissions to provide linkages to similar samples submitted by other users, thereby creating a unique connection between samples that look different externally but behave similarly when executed. Once analyzed, each malware's results are made available to all the Titan members, who can search for attributes of specific samples, compare it to what they've seen, comment on individual samples and pull statistics from Titan's malware repository.

In addition to receiving anonymized information about attacks and responses at other organizations, members will receive quick reports on malware samples they submit. Based on what they have learned from the malware repository and by reverse-engineering malicious code, GTRI researchers will provide information on the potential harm from an attack, the likely source, the best remedy for it and the risks to the organization.

Titan is especially valuable to organizations that lack the resources to operate their own security evaluation labs. GTRI uses Titan to perform an initial malware analysis during the first phase of incident response. Automated behavioral analysis can tell responders what malware is doing in within their environment, what it changes, what it accesses and where it communicates; this information is invaluable during eradication. Users may also use Titan to proactively identify threats seen within other industries, for example, that have yet to target their own industry. In these cases, proactive measures may be taken to prevent future threats from being realized against their organization.

Ongoing Testing

The threat landscape is constantly evolving. To ensure an organization's controls remain up to date against new threats, ongoing self-assessment is essential. Iterative penetration tests, each building on the previous tests, strengthen critical cybersecurity at a low-cost. GTRI is unique in that we train the next generation of world-class penetration testers and cyber-researchers in-house. Regardless of whether in-house teams or third-party independent penetration testers are used to verify security policies are adequate, the important aspect is developing an extremely focused, targeted report as relevant to leadership as possible, such as a "top-ten list." Doing it right isn't about volume. Our goal is to achieve security buy-in; we want leadership to request penetration testing support as much as the system owners.

Everything we do in penetration testing is about relationship building. We strengthen security by establishing a trust partnership; we don't want the person responsible for a targeted system to feel like we're "out to get them." We want system owners to desire our support just as much as leadership, not think our penetration testers as a hindrance.

Unless specifically requested, we conduct tests in a non-destructive manner; no Denial of Service, dangerous exploits or destructive scans. We test from both inside and outside our networks. A public IP space carries a higher criticality and time sensitivity since it introduces actors and systems external to GTRI control. We have learned to not only emphasize classic remote access vulnerabilities that compromise confidentiality, integrity or availability but also unintentional information disclosure (to prevent adversaries from building an accurate profile of their target). Continuously monitoring private IP space is just as important to thwart insider threats, but may not be as time sensitive.

Conclusions

GTRI's core practices are broadly applicable across sectors and throughout industry. These practices should be widely used throughout critical infrastructure and industry. Additionally we can draw the following conclusions from our experience with our framework:

1. The GTRI framework is **cost-effective** – we focus on incrementally cleaning house rather than engaging in wholesale infrastructure replacement. Organizations without the expertise to develop their own security research lab can join communities to give them actionable threat intelligence.
2. **Relationship Building** – Everything we do is geared towards building a trust partnership.
3. **Sharing is key**. This includes understanding your duty to share information.
4. Hire **experienced personnel** rather than just buying expensive tools – Simply buying a device won't make you secure without skilled personnel who understand what the device is telling you. Every system must be tuned to find actual threats.
5. Apply **Defense in Depth within the network**, rather than just at the perimeter. Control what they can do once adversary gets on your network. Organizations must be able to continue business (by creating isolated enclaves, for example) even if adversaries are on their network. You won't be able to eradicate a threat without knowing exactly what got into your network and what goes out.