FARSIGHT SECURITY

Solution Paper

Helping With Regulatory Compliance and Enterprise Risk Management

Today's Challenge: Compliance, Risk Management AND Technical Security

Enterprise cyber security is as much about regulatory compliance and risk management as hardcore technical attention to attempted hacking attacks or malware outbreaks.

Non-compliance incidents can lead to:

- **embarrassing media coverage**
- **lost business opportunities**
- **decreased shareholder value**
- **financial penalties, and even jail time.**

In these times of tight budgets and seemingly never-ending new threats, cyber security risks need to be intelligently prioritized and effectively managed -- Board members and C-level executives will accept nothing less for their cyber security dollar. Farsight Security can help meet those requirements, with unique new category-creating products.

A Few Quick Examples of How Farsight's Solutions Can Help

While every compliance framework is somewhat different, we want to illustrate just a few ways that Farsight believes it can help you more readily comply with selected items from one very popular compliance framework, the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), version 3.0.1.*

Non-compliance incidents can lead to:

Infrastructure & Virtualization Security -- Network Architecture (IVS-13): "Network architecture diagrams shall clearly identify high-risk environments and **data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns** (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denialof-service (DDoS) attacks." [emphasis added]

One of the most popular ways to exfiltrate sensitive intelligence from tightly controlled networks is via DNS. Is your company showing due diligence by instrumenting DNS traffic that's passing through your company's network perimeter?

Maybe it's time to quit ignoring DNS as a potential surreptitious PII data exfiltration channel? Running a Farsight DNS sensor may help give you visibility into one covert channel you may be currently overlooking.

Security Incident Management, E-Discovery & Cloud Forensics Incident Management (SEF-02): "Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and **ensure timely and thorough incident management**, as per established IT service management policies and procedures." [emphasis added]

When you experience a security incident, you need the ability to rapidly investigate the indicators of compromise you've uncovered. Nothing compares to Farsight's passive DNS service, DNSDB(tm), when it comes to chasing forensic indicators such as suspicious IP addresses, unexpected domain names, and odiferous name servers you may have noticed.

Threat and Vulnerability Management -- Anti-Virus / Malicious Software (TVM-01): "Policies and procedures shall be established, and supporting business processes and technical measures implemented, **to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.**" [emphasis added]

Farsight's NOD zone can help prevent many types of new malware from running by temporarily blocking automatic or incidental access to brand new malware C&C's and other brand new malicious domains.

Give Farsight Security a chance to help with ALL your compliance requirements, in surprisingly cost effective ways!

*** https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/**