Shun technology and security incident life-cycle

We've all seen reports of credit card numbers, employee information, passwords or client records being pilfered in a cyber attack. The attacker's goal is usually to exfiltrate sensitive data from your network. Most cyber-attacks include elements of this lifecycle:

Reconnaissance > Delivery > Exploitation > Post-compromise/Exfiltration

Post-compromise (Pivoting, Escalation, Enumeration, C&C, etc.) may not happen at all, or it may happen before, during or after data exfiltration. Attackers' activities in any or all of these phases may be detected by security solutions. For example, port scans, web-based reconnaissance and exploit attempts are often detected by an IDS or Web Application Firewall. Anti-virus and end-point protection suites look for malware in the delivery phase and may even include data loss prevention technologies, which can help identify exfiltration attempts.

Most enterprise IT departments have some sort of incident response plan. This might be an extensive collaborative plan on an internal wiki or SharePoint, or it could simply be a few pages of hand-written bullet-points in the firewall administrator's notebook. Regardless, the lifecycle of an incident usually progresses something like this:

Preparation > Detection > Analysis > Containment/Remediation > Post-mortem

Preparation includes log monitoring, security awareness training, configuration reviews, audits and most other daily tasks involving an enterprise's security stance. Detection of an incident triggers the response plan. This may be as obvious as an email from an IDS, or perhaps something suspicious discovered in the periodic review of logs. Until the threat has been thoroughly contained and/or remediated, the attack is be presumed to be active.

Attacks will happen. Successful defense means containing or remediating the incident before the attacker can successfully exfiltrate confidential data.

RiskAnalytics' Shun technology is not based on signatures. It does not detect bad activity. Is simply blocks all traffic from a list of the Internet's worst malefactors, and we're constantly researching to grow that list and keep it current. Shunning works complementing other security technologies. Since well-known hotbeds of malicious activity are blocked, many casual attackers may simply be unable to see the target network. To a dedicated attacker, Shun technology may pose significant stumbling blocks to reconnaissance, distributed attacks and exfiltration attempts. This can significantly increase the amount of time it takes for each phase of the attack, giving IT staff more time to respond to the incident.

Currently, Shun technology is implemented in our IntelliShun™ and ThreatSweep™.

IntelliShun is a small, efficient Ethernet bridge that indiscriminately blocks any and all IP addresses on the lists chosen by the customer. It is an excellent solution for protecting offices, distributed sites and home networks of employees who frequently work remotely with access to sensitive information.

IntelliShun™
ADVANCED SHUNNING

ThreatSweep puts Shun technology into a full-featured IDS/IPS with much higher performance as well as redundant power and network failsafe technology. With our escalation engine, Sentinel alerts can be prioritized. Alerts are also monitored and analyzed by our expert team, who are available to answer questions and assist with analysis of incidents. This high-powered solution can defend much larger networks and provides tools to help IT staff investigate incidents more efficiently.

ThreatSweep™
DETECTION + RESPONSE

Call us at 1.855.639.4427 to put us to the test.

RiskAnalytics™
THE ART OF SECURITY™

ShadowNet™

/ GLOBAL THREAT INTEL

RA

RiskAnalytics.com