Self Learning Networks
An Overview

Alvaro Retana
aretana@cisco.com
Distinguished Engineer, Cisco Services

Slides by JP Vasseur and Jeff Apcar.
What Self Learning Networks is About…

• SLN is fundamentally a hyper-distributed analytics platform …

• Putting together analytics and networking …
  • Goldmine of untouched data on networking gear (sensing)
  • Network learns and computes models on premise (analytics)
  • The Network adapts, modifies its behavior (control)

• SLN for Security: attacks are incredibly sophisticated and targeted, ex-filtration of data being a major concern, requiring a next-generation approach => Stealthwatch Learning Networks
Harsh environments: instability of links, limited bandwidth, constrained nodes, stochastic networks (random probability distribution).

Still need for some determinism, tight SLA and hyper-scale networks.

And the network needs to be adaptive: every single network is different!

From this SLN was incubated.
Predictive models for large scale networks, enable:

- High performance
- High Resiliency
- Detection of disruptive subtle DDoS attacks

Predict network behavior and traffic patterns based on multivariable and time-based modeling.

Automatically select and optimize network path in real-time, adapt QoS, based on Business SLAs.

Detect of multi-layer subtle DoS attacks and Anomaly Detection

Auto learn new threats

Massively Distributed, Global, real-time protection
SLN Architecture Principles For Security

- Fundamentally distributed, building models for visibility and detection at edge
- Mix of Machine Learning (ML) and Threat Intelligence
- Enrichment of context
- Ability to adapt to user feed-back (Reinforcement Learning)
- Advanced control handling networking complexity
Why Predictive Analytics?

• Multi-layered defense architectures no longer sufficient to prevent breaches caused by advanced malware ...
  • No longer a question of “if” or “when” but “where” ...

• Many of the well-known assumptions are no longer true
  • eg. Attacks come from the outside, deterministic, well understood

• Attacks are more and more “subtle” (Hard to detect ...)

• Signature-based architectures vulnerable to mutating attacks (polymorphic)

• Dramatic increase of the number of 0-day attacks
What Is a Self Learning Network (SLN)?

- The network is truly adaptive thanks to advanced analytics
- A true paradigm shift!
  - Move from Trial-and-Error model to a proactive approach using models built using advanced analytics
  - The hard part is not just the “analytics” but the underlying architecture for self-learning and the “how to”
SLN Architecture
Distributed Learning Agent (DLA)

- Sensing (knowledge): granular data on control and data plane & local states
- Machine Learning: real-time embedded behavioral modeling and anomaly detection
- Control: autonomous embedded control, advanced networking control (police, shaper, recoloring, redirect, ...)

SLN Centralized Agent (SCA)

- Orchestration of DLAs.
- Advanced Visualization of anomalies
- Centralized policy for mitigation
- Interaction with other security components such as ISE and Threat Intelligence Feeds
- North bound API to SIEM/Database (e.g. Splunk)
- Evaluation of anomaly relevancy
The DLA Can Have Many Data Sources

- DLA has been designed for low footprint both in terms of memory and CPU
- Feature computation, ID & classification are performed locally
- Lightweight techniques employed with no significant impact on the edge device
SCA Context Enrichment

- Component to SLN
  - Enhanced context, ML+Threat Intelligence
  - Edge Control

Cisco Live!
On-Premise Edge Control

Controller infrastructure

Honeypot (Forensic Analysis)

Control Policy
Smart Traffic flagging
According to {Severity, Confidence, Anomaly_Score}
Traffic segregation & selection
Network-centric control (shaping, policing, divert/redirect)

Public Internet

SCA

DSCP ReWrite CBWFQ

DSCP ReWrite CBWFQ

DLA

DLA

DLA

Shaping

CiscoLive!
Anomaly Detection
Botnets and Data Ex-Filtration Techniques

- Size can range from thousands to millions of compromised hosts
- Botnet can cause DDoS & other malicious traffic (spam, ...) to originate from the inside of the corporate network
- C&C (C2) servers become increasingly evasive
  - Fast Flux Service Networks (FFSN), single or double Flux
  - DGA-based malware (Domain Generation Algorithms)
  - DNS/NTP Tunneling
  - Peer-to-Peer (P2P) protocols
  - Anonymized services (Tor)
  - Steganography, potentially combined with Cryptography
  - Social media updates or email messages
  - Mixed protocols ....
- Timing Channels
SLN Paradigm Shift

- (Current) Generation of Security Architectures and Product
  - Specialized Security gear connected to the network (FW, IPS, ...)
  - Heavily signature-based ... to detect *known* Malwares
  - Dynamic update of signatures

- SLN is Machine Learning based and pervasive
  - Use of adaptive Machine Learning (AI) technology to detect advanced, evasive Malware: build a model of normal pattern and detect outlier (deviations)
  - High focus on 0-day attacks
  - Use every node in the network as a security engine to detect attacks
  - Complementary to all other technologies (FW, IPS, ...)

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 16
SLN Anomaly Detection

Anomalies are patterns/data points that do not conform to expected behaviour.
In algorithmic terms, they significant statistical deviations.

Challenges

- Model what is normal behaviour
- Recognising malicious behaviour that adapts to look “normal”
- Normal behaviour changes over time and anomalies evolve (adaptive models required)
- Differentiate noise from anomalies

SLN allows detection of previously unknown malware complimentary to firewalls & IDS.
Categories Of Anomalies

Point Anomaly
A specific instance is abnormal compared to other instances

Collective Anomalies
A collection of an instance that is abnormal in regards to an entire set

Contextual Anomaly
A data instance looks normal individually, but abnormal when taken in a specific context
SLN Visibility
Graph-Based Visibility

- Vertices (Nodes, hosts, sites, disks, router, laptop…)
- Edge (Comms links, flows…)

- Graph structure usage in SLN:
  - Infer information on the roles of hosts
  - Detect unusual change in graph structure
  - Capturing and modeling the dynamic of the flows in the network

<table>
<thead>
<tr>
<th>SLN Usage</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vertices</td>
<td>Clusters</td>
</tr>
<tr>
<td></td>
<td>Physical: Country, City, Building, DC, Floor, Logical: DC Function, Organisational Group</td>
</tr>
<tr>
<td>Edges</td>
<td>Traffic Flows</td>
</tr>
<tr>
<td></td>
<td>Applications, protocols, bandwidth, seasonality</td>
</tr>
</tbody>
</table>
Visualising Anomaly Detection Process

- Lack of visibility of flows between remote sites (clusters) is an issue
- Difficult to detect Malware/data exfiltration involving lateral movement
Visualising Likely/Unlikely Flows

- Static Versus Dynamic cluster computation
- ML algorithms are used to computed inter-cluster relationship
- Colored graphs
- Simple property of likelihood
Visualising Seasonality

- ML computes models of seasonality per application
Visualising Behavioural Analytics

A vector of properties (models of behavioural analytics)

\[ v = [\nu_1, \nu_2, \ldots, \nu_{n-1}, \nu_n] \]
Host Anomalies Using Feature Vectors

Hosts whose behaviour do not match known models (cannot be explained) may point to an anomaly.
## SLN Targeted Outcomes For The User

<table>
<thead>
<tr>
<th>Normal Behaviors</th>
<th>Anomalous Behaviors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who talks to whom?</td>
<td>Detection of new applications where never used</td>
</tr>
<tr>
<td>Active applications between clusters</td>
<td>Detection of abnormal behaviours (data exfiltration)</td>
</tr>
<tr>
<td>Applications displaying seasonal behaviours</td>
<td>Adaption: Is abnormal event of interest?</td>
</tr>
<tr>
<td>Additional application characterisation</td>
<td>Upon detecting anomalies; Explain why? What has changed?</td>
</tr>
<tr>
<td>Contextual data; usernames, domains...</td>
<td>Ability to perform advanced control (Shape, route, redirect...)</td>
</tr>
</tbody>
</table>

SLN adapting to user expectations!
Summary

• SLN is a disruptive approach for malware detection using behavioral analytics, relying on dynamic learning, fully auto-adaptive

• Network data is analyzed locally by SLN using advanced and lightweight analytics

• The router can perform local mitigation

• Lightweight and distributed architecture that is scalable

• Visualization is key with simple understandable UI
TOMORROW starts here.