Detecting and Profiling Hidden Threats Using Deception and Splunk

Satnam Singh | Chief Data Scientist, Acalvio Technologies

October 2, 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

Agenda

- Hidden threats
- Introduction to deception and use cases
- Triage of deceptive alerts with security events in Splunk
- Profiling threats: Demo

Hidden Threats

- Adversaries move within the network to find valuable or vulnerable assets
- Perimeter-based controls can't detect the threats that have already infiltrated and are hiding within the enterprise network
- Adversaries are using "living off the land" tactics → makes it difficult for Endpoint detection tools to detect them

How to Defend?

1. Slowdown the Attacker

2. Speed up the Defender

Deception

- Deception needs to blend with the environment
- Multiple types of Deception
- Deception needs to dynamic, morph and adapt over time

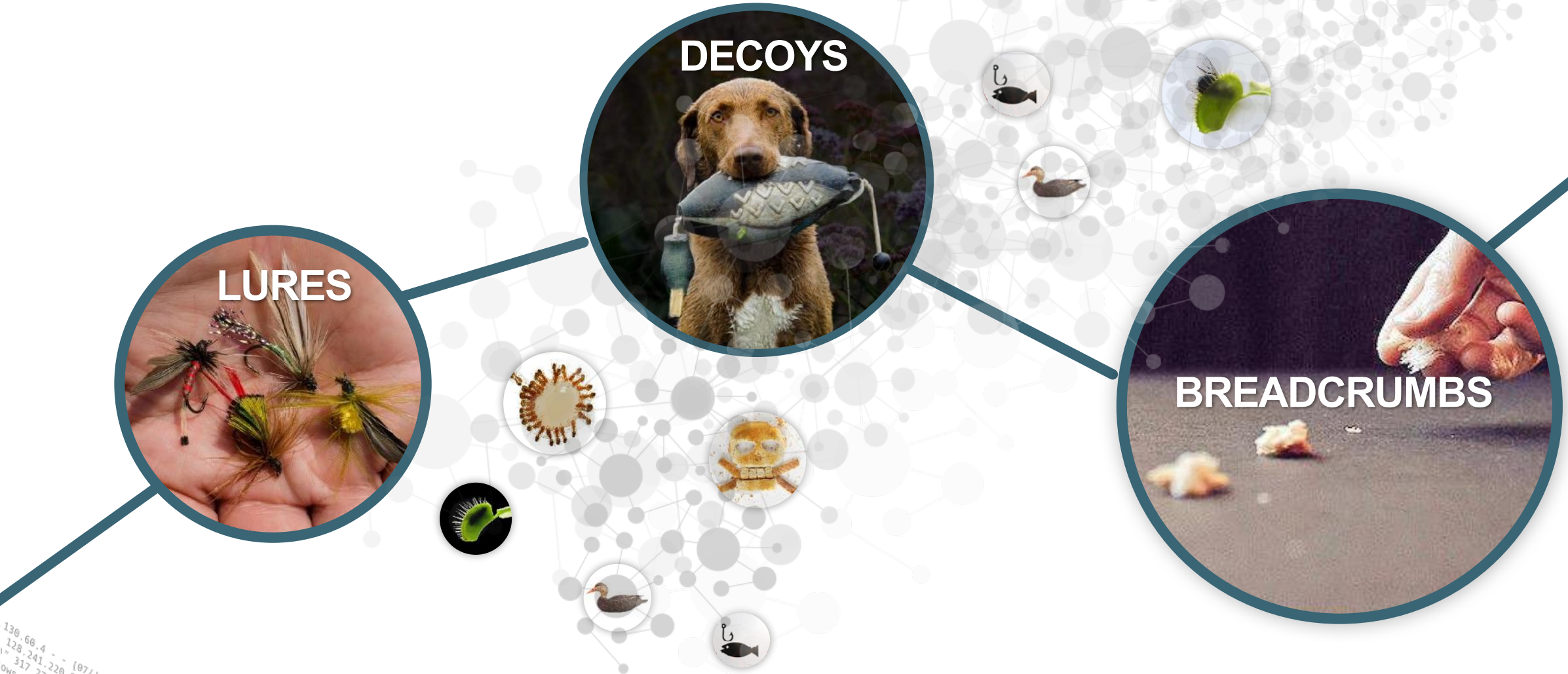
Deceptive Security - Use Cases

- Detect Lateral Movement in the Corporate Network
- Detect Network Scans, Ransomware
- Detect advanced threats that are targeting specific verticals e.g., SWIFT, ICS

Deceptive Security - Use Cases

- Get visibility of threats in unmanaged networks, encrypted traffic, IOT devices
- Generate actionable threat intelligence with high fidelity alerts
- Need only a few resources to deploy another security layer

Deception Types



Decoys

- Interaction Types - Low, Medium, High
- Services - SSH, Telnet, SMB, FTP, …
- Workstations
- Databases
- Servers
- Routers, Switches
- …

Breadcrumbs

Extends deception to production devices

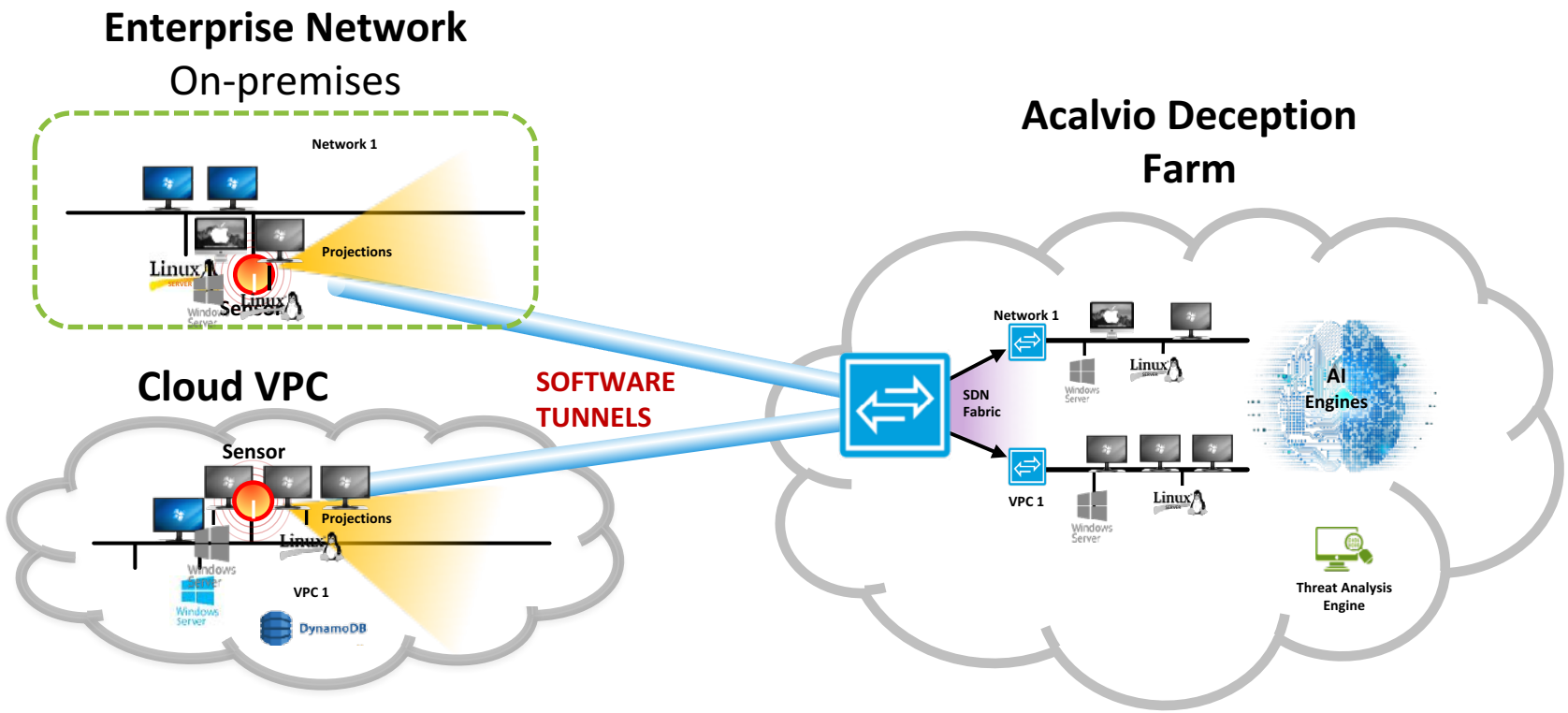
- Credentials - Shares, Servers
- In-Memory hashes
- Files
- Registry entries
- Browser Cookies
- …

Lures & Baits

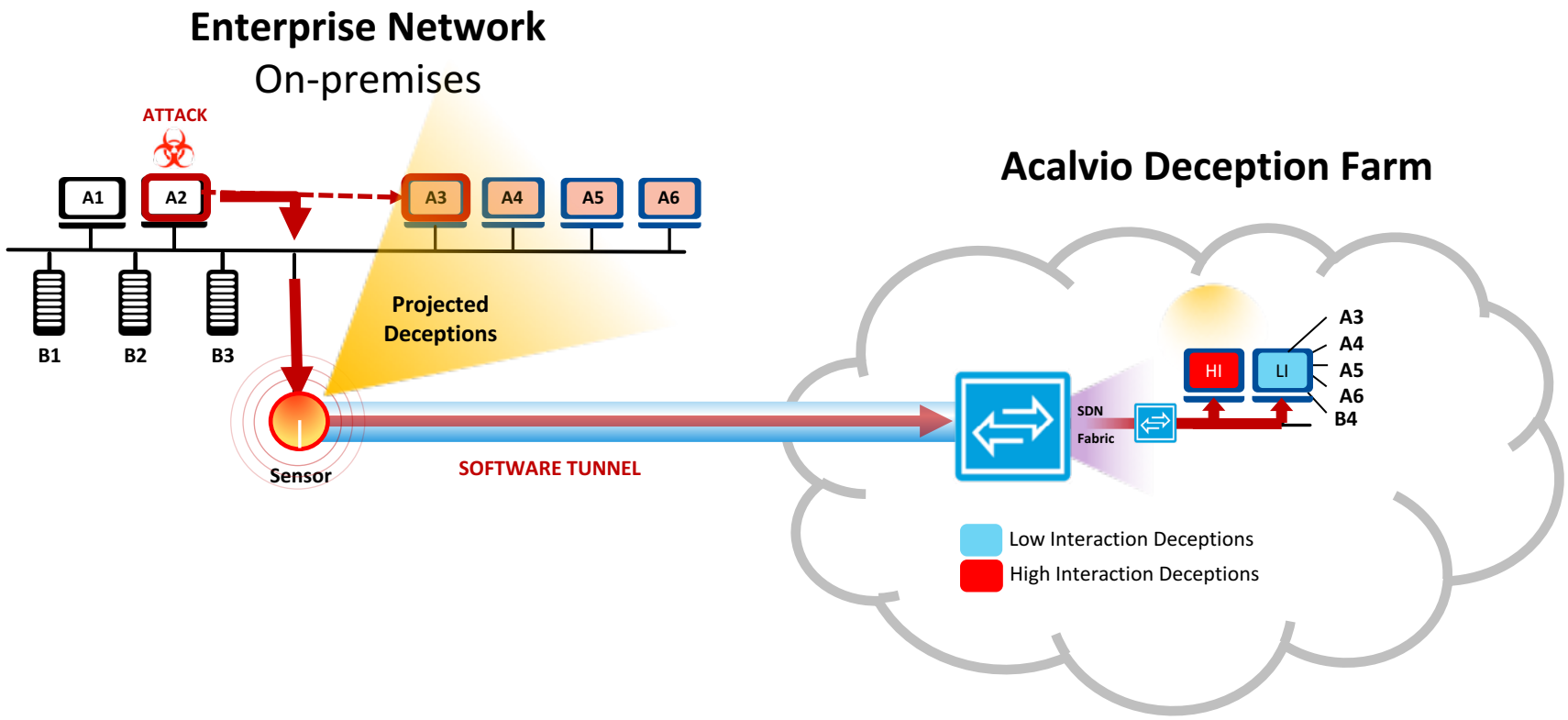
Makes deceptions more attractive

- Vulnerable Shares
- Network Printer
- Vulnerable Webserver
- PACS DICOM Server
- Contents of breadcrumbs and decoys (ex: files, user account, share, database, address book)
- ….

Deception Farms



Fluid Deception



Threat Profiling

Splunk App

1. Customise Deception
- Customise decoys to blend
- Determine Deception Strategy

2. Deception Platform
Deploy Deceptions

3. Triage with Deception Alerts

Demo

Threat Profiling

Key Takeaways

1. Deception provides an ability to detect hidden threats
2. Deception needs to be customized and dynamic
3. Triage deception alerts with network, endpoint logs in Splunk to generate actionable internal threat intelligence