Nevelex Labs' Security Flow:
Land O'Lakes / (S)OAR / CrowdStrike

Real World Experience from Land O'Lakes

March 25th, 2021

NEVELEXLABS™

NEVELEXLABS™

SECURITY FLOW
Introduction

Introduction

- Introductions
  - Lucas Tesh
  - Adam Lenart
  - Steve Goers
  - Michel Dalal
- Where We Came From

Introduction

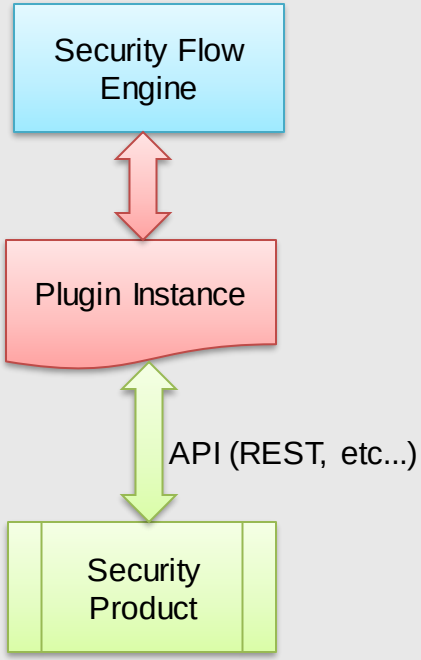
- Headwinds
  - Lacking Time
  - Lacking People
  - Existing Scripts

- Why?
  - Non security related IT process inconsistencies leading to security challenges.
  - Disparate tools with minimal integration capabilities.
  - Resource optimization (focus on the important tasks).

SECURITY FLOW
Terminology

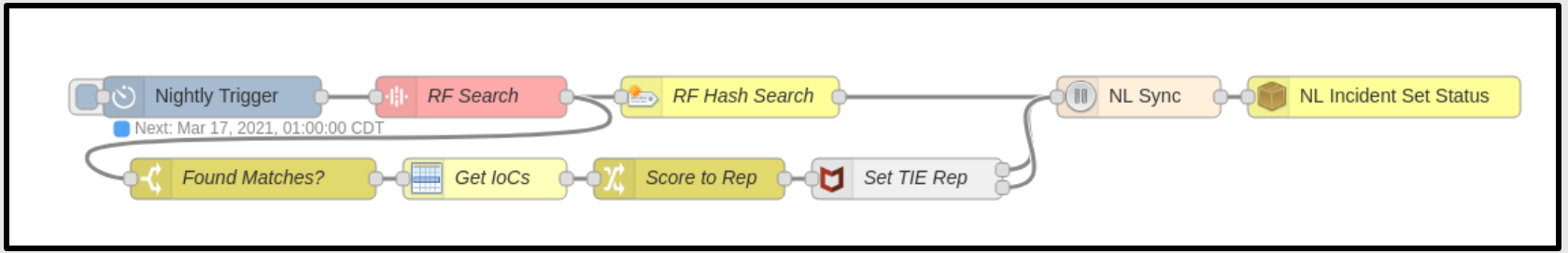
Terminology

- API – Application Programmer's Interface
- Plugin
  - Security Flow Integration with a 3rd Party Vendor Tool or Service.
  - Flow Programming Nodes
  - Defines API Configuration Parameters
- Plugin Instance
  - Uses Plugin Code
  - Device Specific Settings



Terminology

- Flow – A single tab containing a set of nodes.
- Node – A functional block within a Flow.
- Message – A JavaScript Object traversing a Flow.



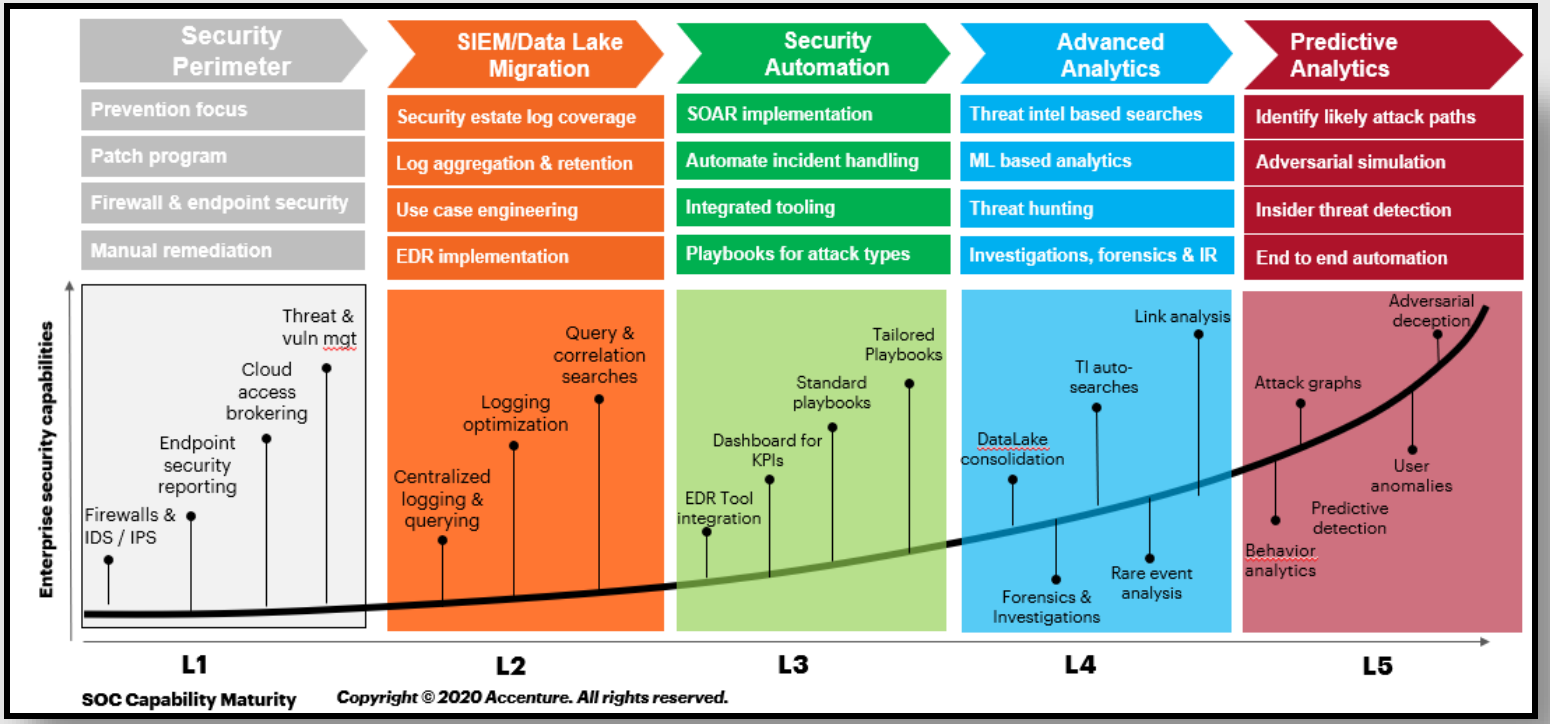
- Timeline – Incident page summarizing operations performed.
- Data Renderer – Transforms JSON to a User-Friendly Interface.
- Injection – A manually initiated event trigger from a Dashboard.

NEVELEXLABS™

NEVELEXLABS™

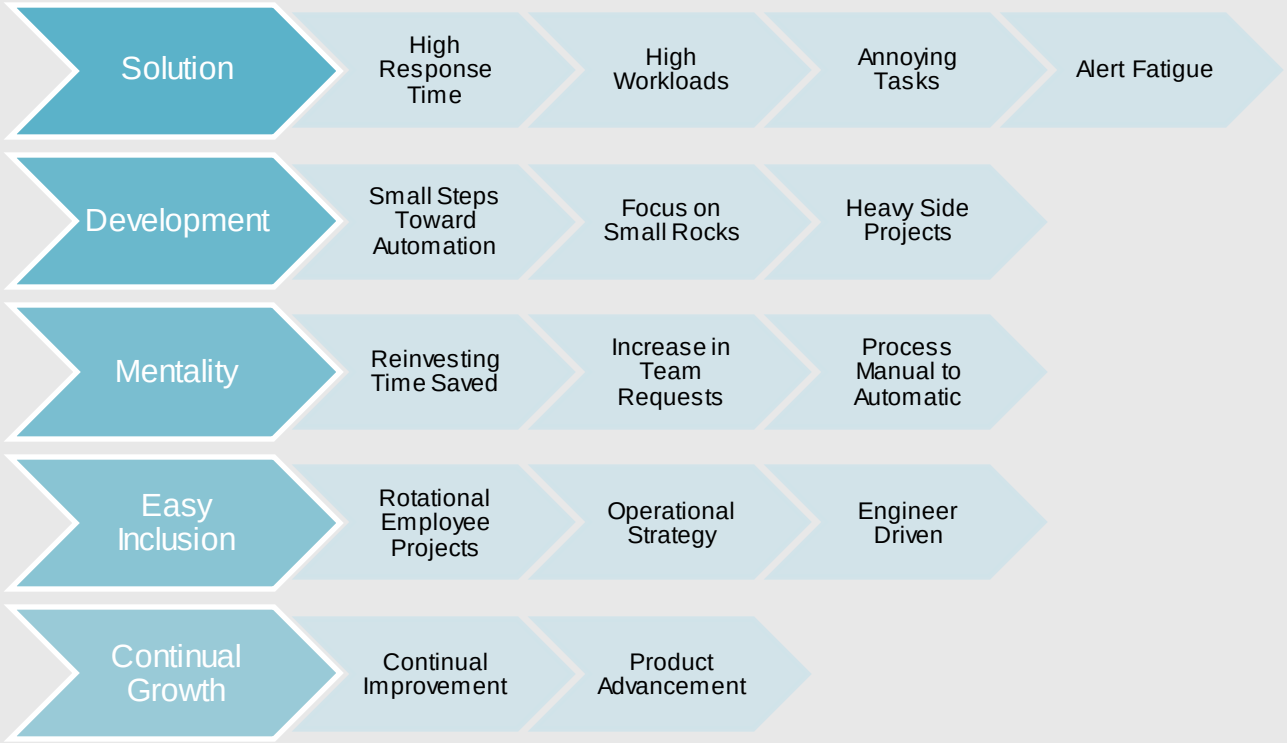
SECURITY FLOW
Land O'Lakes Journey

Land O'Lakes Journey



NEVELEXLABS™

Land O'Lakes Journey



NEVELEXLABS™

Land O'Lakes Journey – Flow Creation

NEVELEXLABS TM

Land O'Lakes Journey – Current Use Cases

Substantial Flows

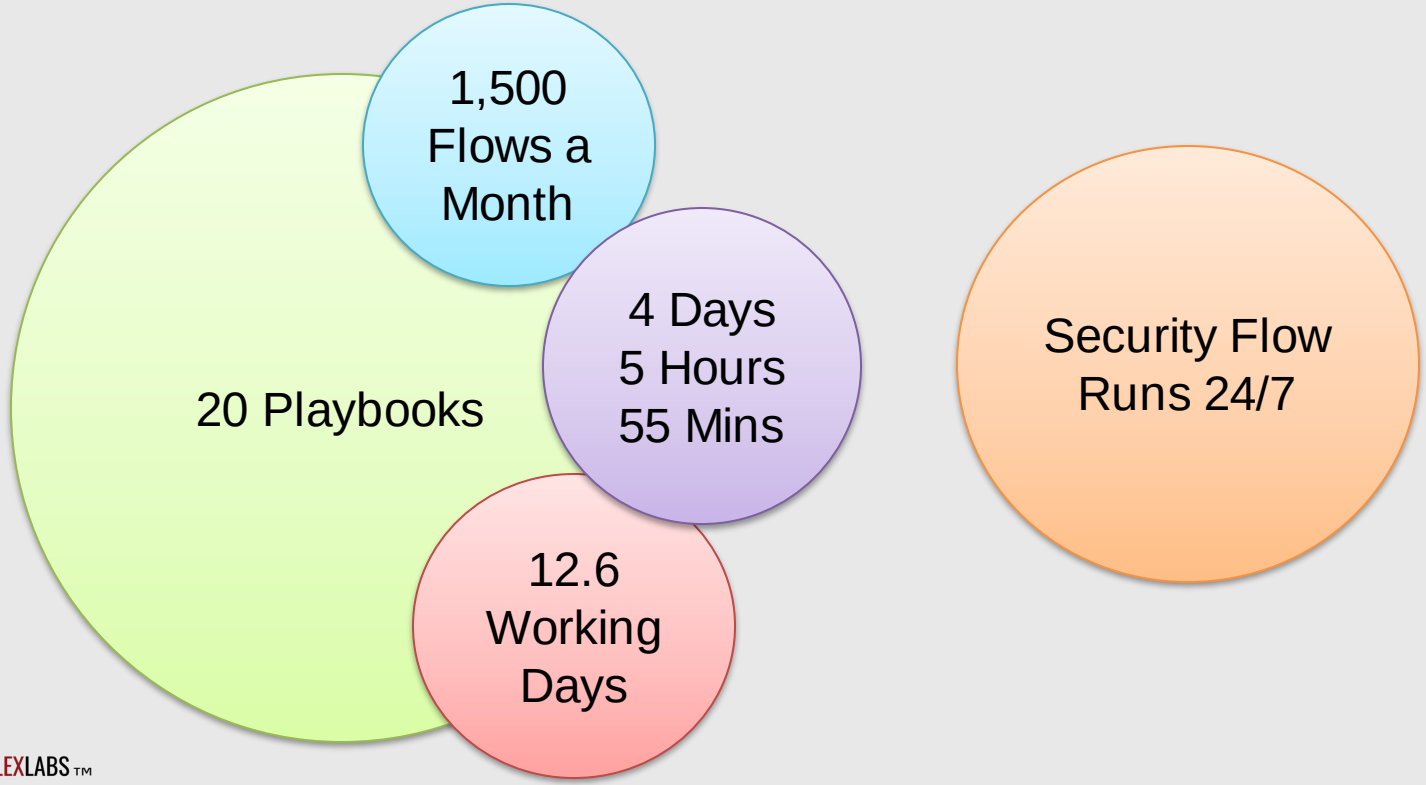
- Phishing Remediation
- Privilege Access Management
- Typosquatting Prevention
- Network Change Security Updates
- Leaked Credentials

Planned Use Cases

- Complete Security Metrics to PowerBi
- Compromised Credentials
- Automatic WAF Scanning Update

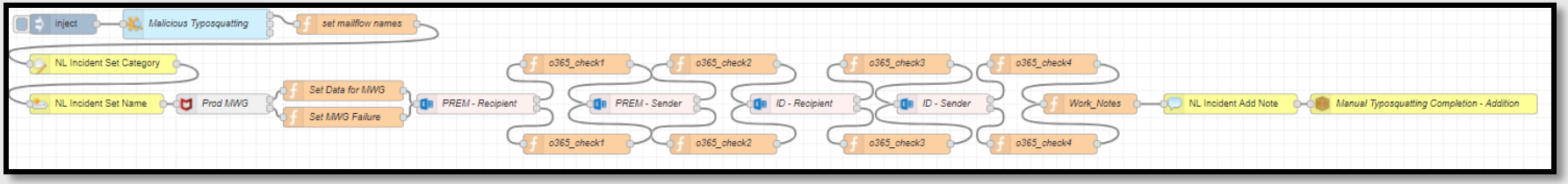
NEVELEXLABS™

Land O'Lakes Journey – Time Savings

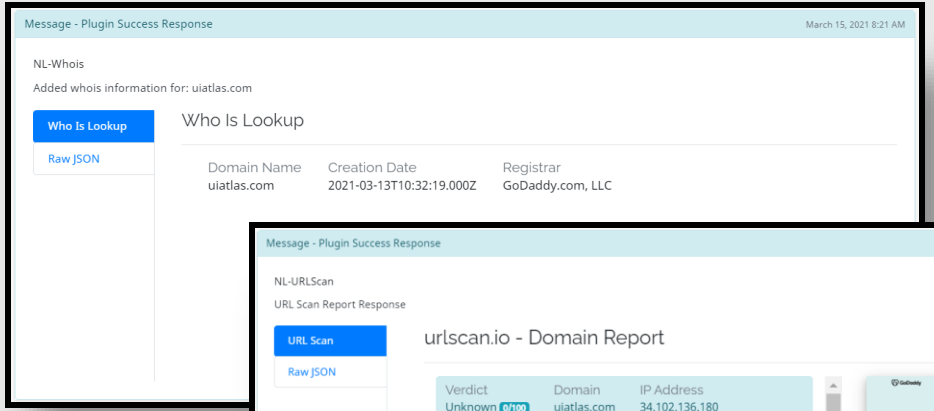


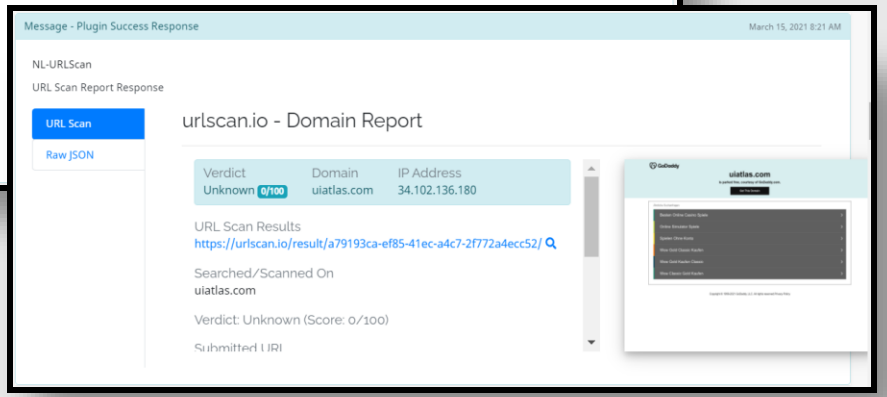
NEVELEXLABS TM

Land O'Lakes Journey - Typosquatting



- Typosquatting
  - Ticket Creation – Quick and easy tracking in Service-Now
  - API Checks – URLScan, Who Is Lookup
  - Remediation – Proxy / Mail Flow Rule Blocking





NEVELEXLABS TM

NEVELEXLABS™

SECURITY FLOW
Differentiators

Differentiators

- Beyond the Powerful Feature Set, the Flexibility to Expand Features.
- Broadcast Event Mechanism to decouple flows (playbooks) from plugins (integrations).
- Professional Service Hours Included with Licenses
  - 30 hrs. of professional services included with Professional Tier License.
- Flexible Licensing Model
  - Unlimited actions and unlimited seats

NEVELEXLABS TM

Differentiators - Why

- Flexibility to expand upon existing features.
- Broadcast Event Mechanism to reduce/eliminate flow changes.
- We are here to accelerate the automation planning and flow development process.
- Our goal is to get your team up and running and utilizing the product within hours.
- Known cost structure without limitations

NEVELEXLABS TM

What's First?

NEVELEXLABS TM

SECURITY FLOW

Demos

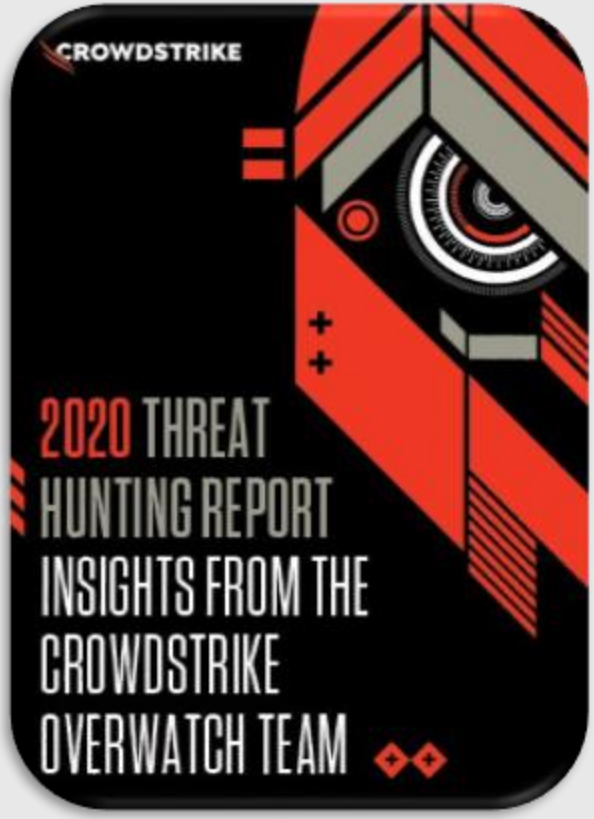
Demo: Contain CrowdStrike Hosts & Execute RTR Scripts

- Batch host containment – handling devices "in bulk"
- Additional actions using Real Time Response – since CrowdStrike is on every endpoint
  - Log off a batch of users
  - Gather browser history
  - Gather hotfix/browser extension data

NEVELEXLABS TM

Demo: Azure AD Onboarding

- In late 2020, CrowdStrike released the Overwatch Threat Report:
  - In nearly every single e-criminal breach, credentials were mis-used, or stolen.
  - Many of those instances utilized latent/expired/disabled/over-privileged accounts.
- Consider this additional advanced use case:
  - Land O'Lakes: They are monitoring previledge escalation by monitoring domain admin groups and validating that a proper ServiceNow ticket was utilized. If not, the user is removed from the group and a security alert is generated.



NEVELEXLABS™

Demo: Phishing Investigation

- Consider Resource scaling - What really takes place in a normal phishing investigation?
  - User reports email (2-3 minutes)
  - Analyst looks for IoC within the email (3 minutes)
  - Have these IoC been accessed? (6 minutes)
  - Who has accessed these IoCs? (10 minutes)
  - Are the IoCs bad? (2 minutes)
  - Now what? (and how much time to decide?)
- An individual email may not be a significant amount of time but consider how often this occurs. How many times per day or per week?

NEVELEXLABS™

SECURITY FLOW
Potential Next Steps

Potential Next Steps

- One-on-One Conversation / Discussion About Current State
- Customized Demos are Always Available
- Welcome POC's

NEVELEXLABS TM

Questions / Comments?

sales@nevelexlabs.com
nevelexlabs.com | @nevelexlabs
2950 Metro Drive, Suite 104, Bloomington, MN 55425 | 952.500.8921