Security Automation: Lessons Learned and the Path Forward

Patrick Orzechowski

May 3rd, 2019

JHU APL - Integrated Cyber Conference

deepwatch

Introduction and Background

- “PO”
- VP of R&D - deepwatch
- MS in CS from JMU
- 20 years in cybersecurity
  - Blue/Red Team
  - IC for a bit
  - Cliche 80s “hacker” - you had me at WarGames
  - First MSSP experience: Symantec in early 2000s

deepwatch

- Started in 2015 as an MSSP under GuidePoint Security
- Analytics focused
- Splunk based
- 0-100 customers in less than 4 years
- Single Tenant Data Environments
- **Automation was initially an afterthought..**

Press + Hype vs. Reality

,391 views | Feb 21, 2019, 10:59am

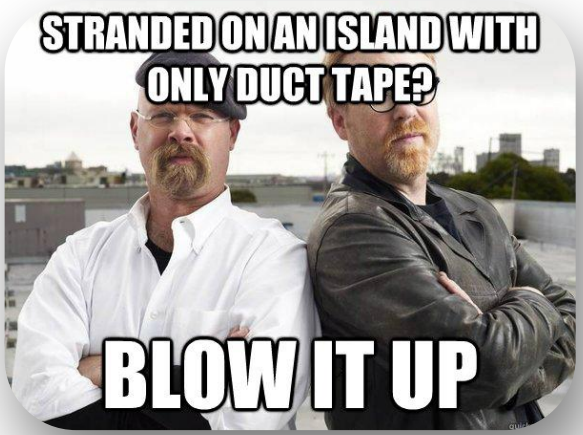
Automation Is Key To Thwarting Cloud Security Threats, New Oracle-KPMG Research Shows

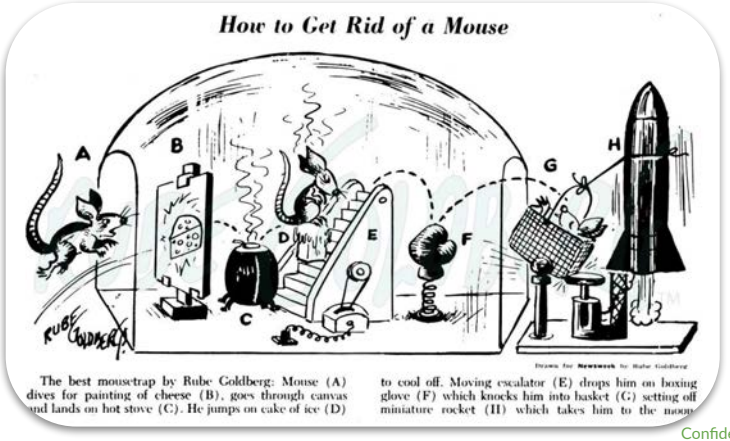
Alan Zeichick Brand Contributor
Oracle BRANDVOICE

Phishing attacks, unpatched systems, and unauthorized cloud applications are creating unrelenting risk for enterprise security teams. Automation of threat monitoring and patching of software vulnerabilities is often the best way—and increasingly the *only* effective way—to tackle those challenges.

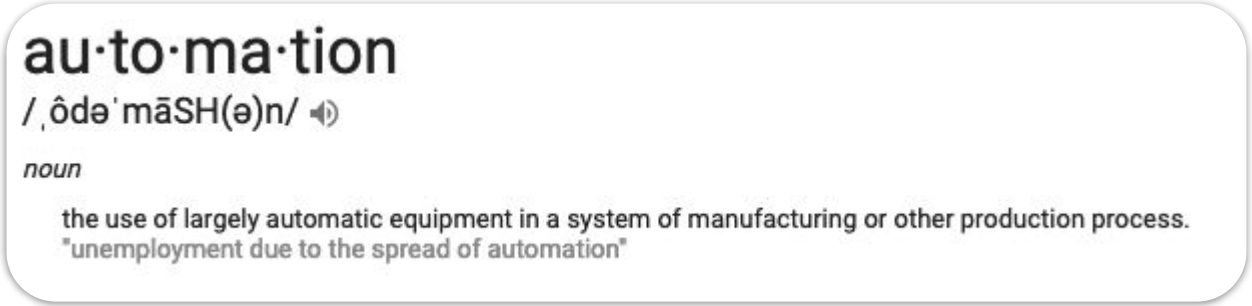
Automation Myths

- Automation is new…
- Automation is complicated…
- Automation is “AI” or “ML”...
- Automation requires fancy products or tools...





Level Set - Definition of Automation


au·to·ma·tion

/ˌôdəˈmāSH(ə)n/

noun

the use of largely automatic equipment in a system of manufacturing or other production process.
"unemployment due to the spread of automation"

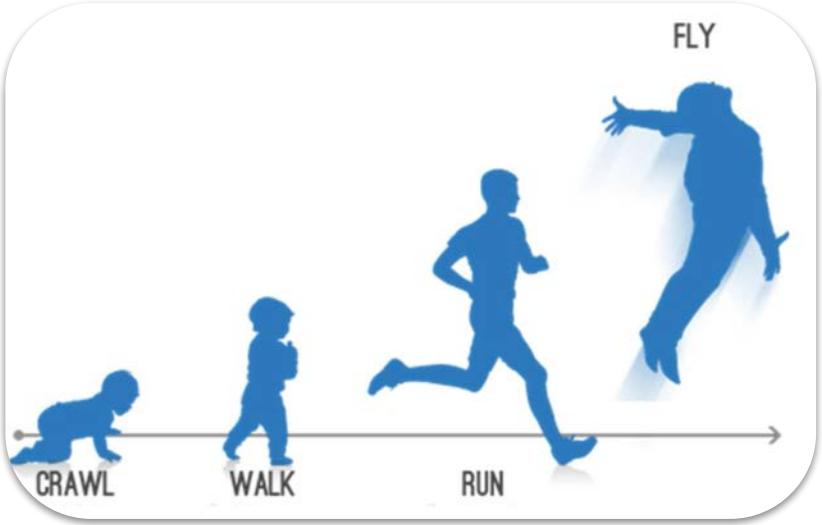
“Anything that programmatically completes manual task in a repeatable fashion”

In the beginning… deepwatch non-automation

- Services oriented
- Manual environment builds
- Manual Content Creation and Distribution
- Manual Threat Intelligence Configuration
- Manual Application Pushes
- Manual Threat Hunting

Approach to Automation

- Phases:
  - Customer Builds
  - Blocking / Tackling
  - Contextualization
  - Playbook Development
  - Active Response
  - Metrics! (more in a sec)
- Tools:



ANSIBLE

HashiCorp Terraform

python™

DEMISTO
A PALO ALTO NETWORKS® COMPANY

All the fails..Automation style

1. API Integrations
    a. Keys go bye-bye
    b. “Trust” is important...apply CIAr to API’s
2. Ticket Creation
3. Git distribution automation
4. ...worse than human error?
5. ...fixes are permanent...

The Automation Story Today

Architecture Automation

Platform is self-aware to notify and escalate when any form of expected input or outage occurs in the platform.

+

Content Automation

Security content is released through a management network to all customers to enable new security features and responses to emerging threats.

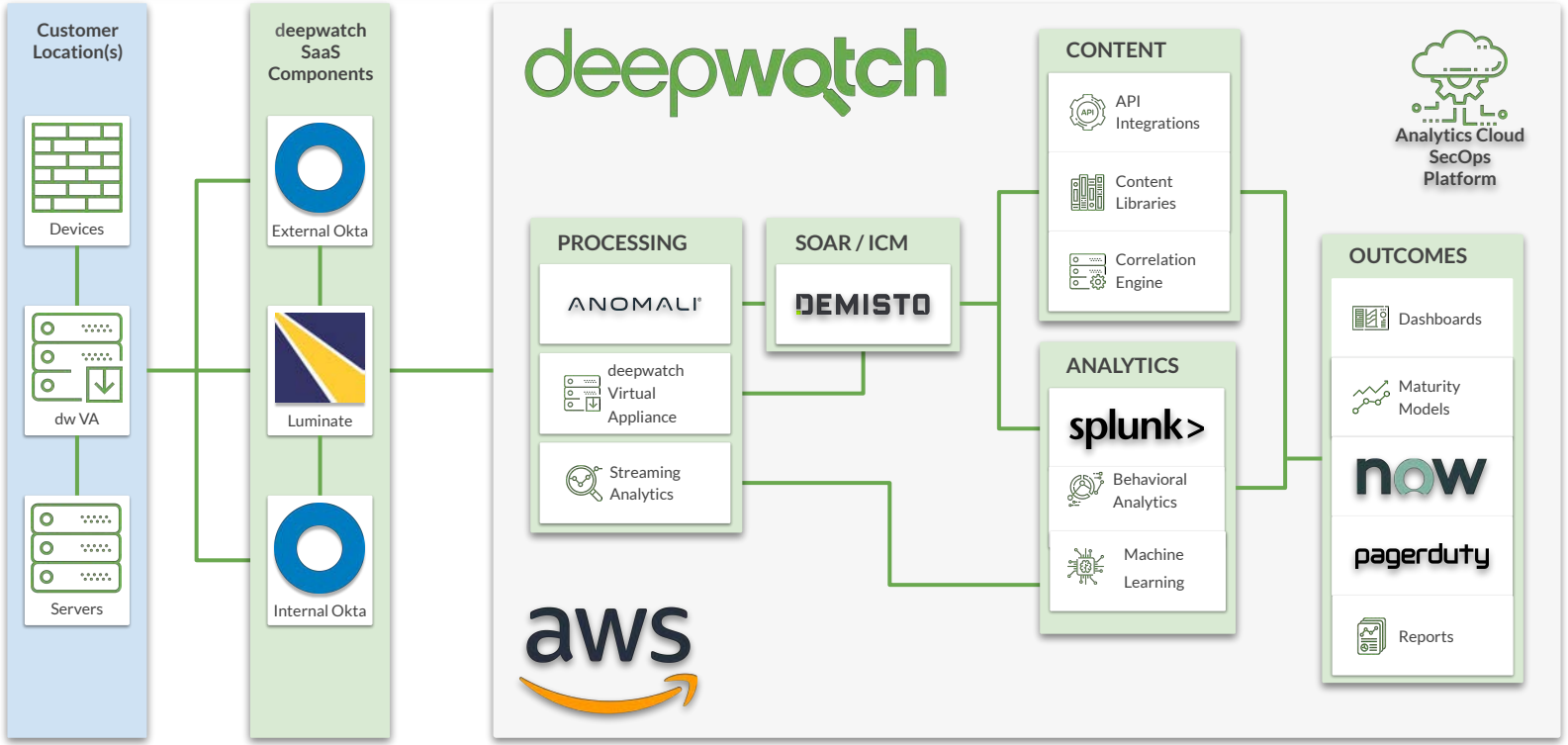
→

Automation as Customer Value

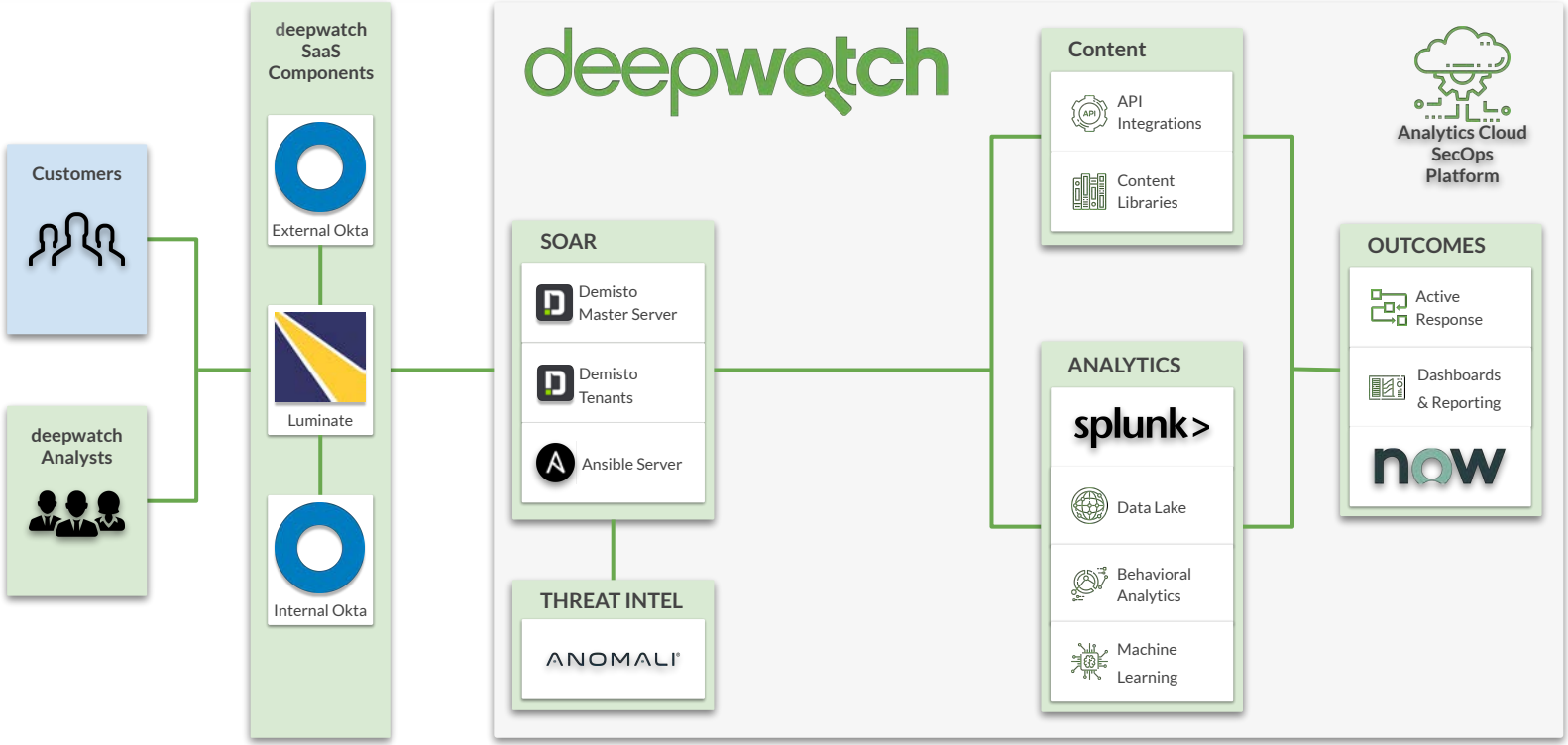
Between a highly available/responsive platform and a high-speed delivery mechanism for security content, customers receive what they want without the headaches of all the care-and-feeding of manual tasks.

deepwatch

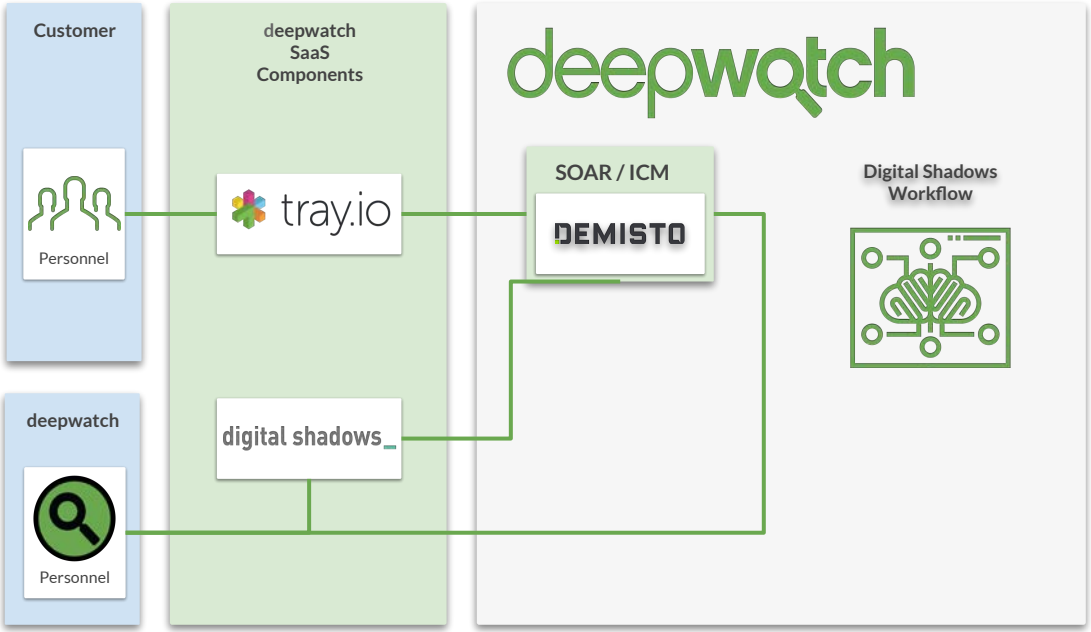
deepwatch Detect Analytics Architecture



deepwatch SOAR/Respond Architecture

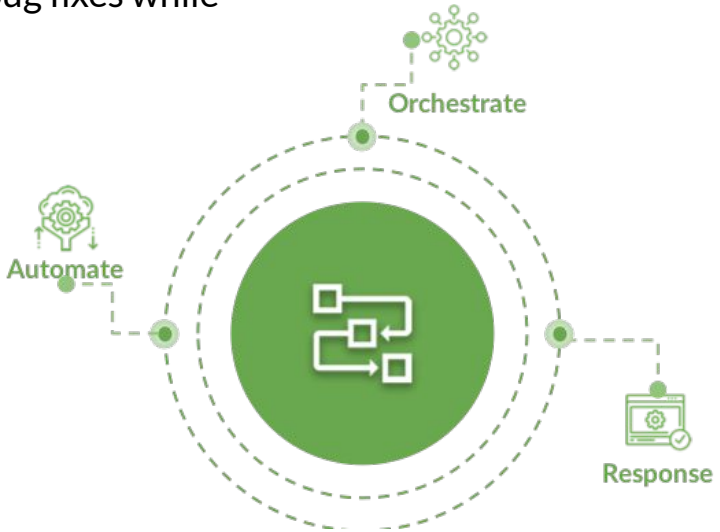


Threat Intelligence Workflow Automation



deepwatch Respond Content Library Highlights

- SOAR service offered by leveraging Demisto + deepwatch Content Library
- Pioneered SOAR integrations with customer platforms
- Developed code into Demisto platform & multiple bug fixes while working at scale
- Playbooks developed in-house
- Mapped to CIS and MITRE ATT&CK Frameworks



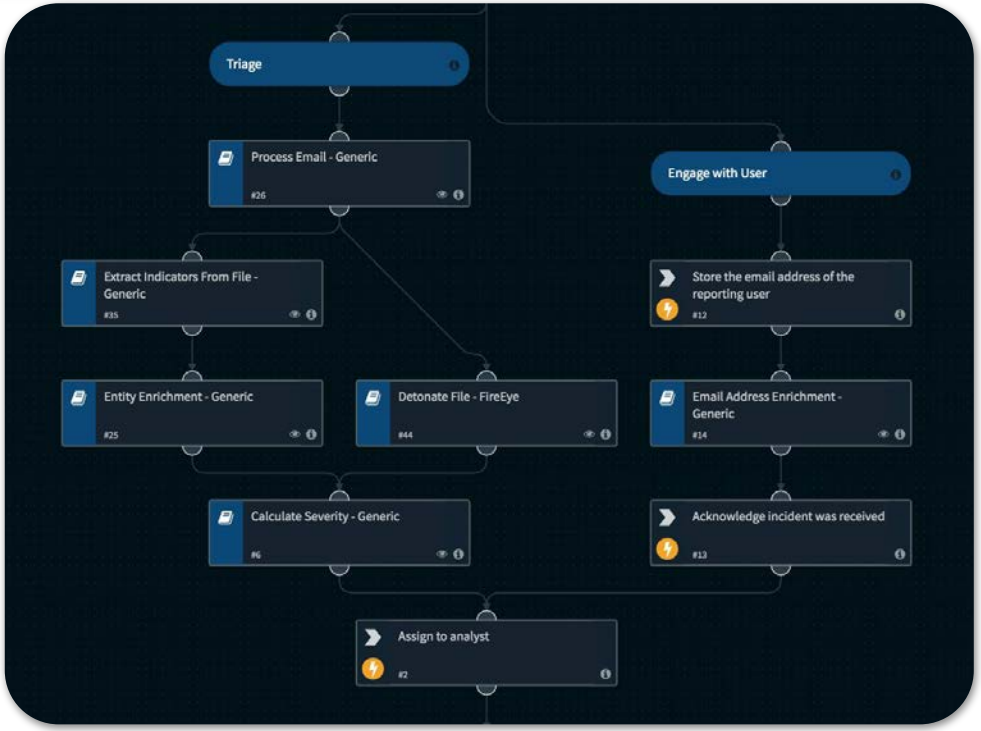
deepwatch SOAR Highlights - 2018

- All customers have SOAR tenants (multi-tenant environment)
- Created and managed Demisto systems (13 servers, 90 tenants, 3 separate systems)
- Customized Splunk Demisto Technical Addon (TA) to create solution for all customers via Luminate, code base integrated by both Luminate and Demisto branches
- Playbook Development
  - Created Infrastructure monitoring playbook to help Engineers resolve system issues faster
  - Continuously developing playbooks
    - Squad Requests
    - R&D Roadmap
  - Advanced Demisto & Ansible integration for self-healing playbooks and further automation

Example Playbook

Phishing Detonation Playbook

- Similar to technologies like Cofense and Wombat
- Customer personnel send suspected emails to an inbox for evaluation
  - *phishing@acme.com*
- Email payload detonated within FireEye appliance
- Positive results are assigned to Squad
- Negative results notify forwarder



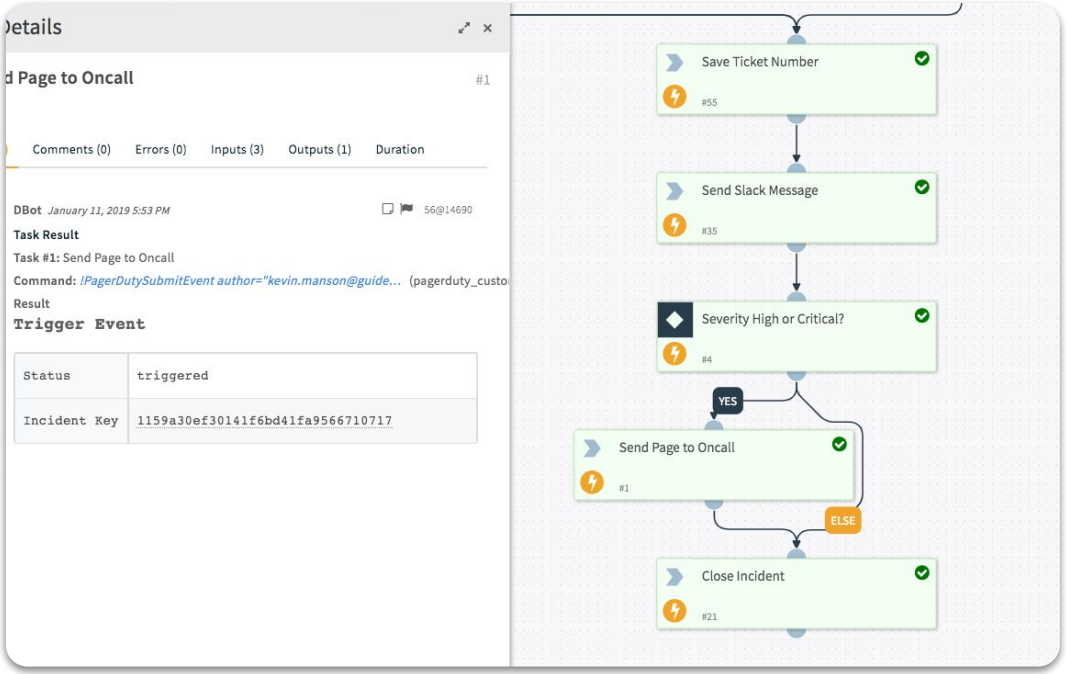
Example Playbook - Pagerduty

Before

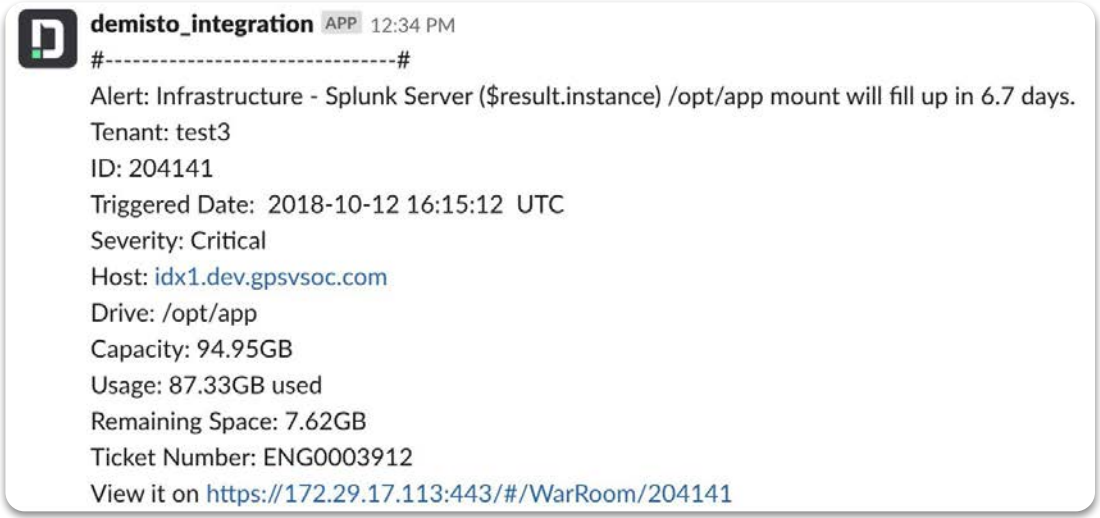
- Manual analyst triage of Operations Incidents
- Workflow required multiple handoffs and timing lag for engaging resources, and customer notification

Now

- Automation validates need to page support engineer
- Configuration has escalation process to ensure action
- Automation performs starts necessary ticketing & documentation

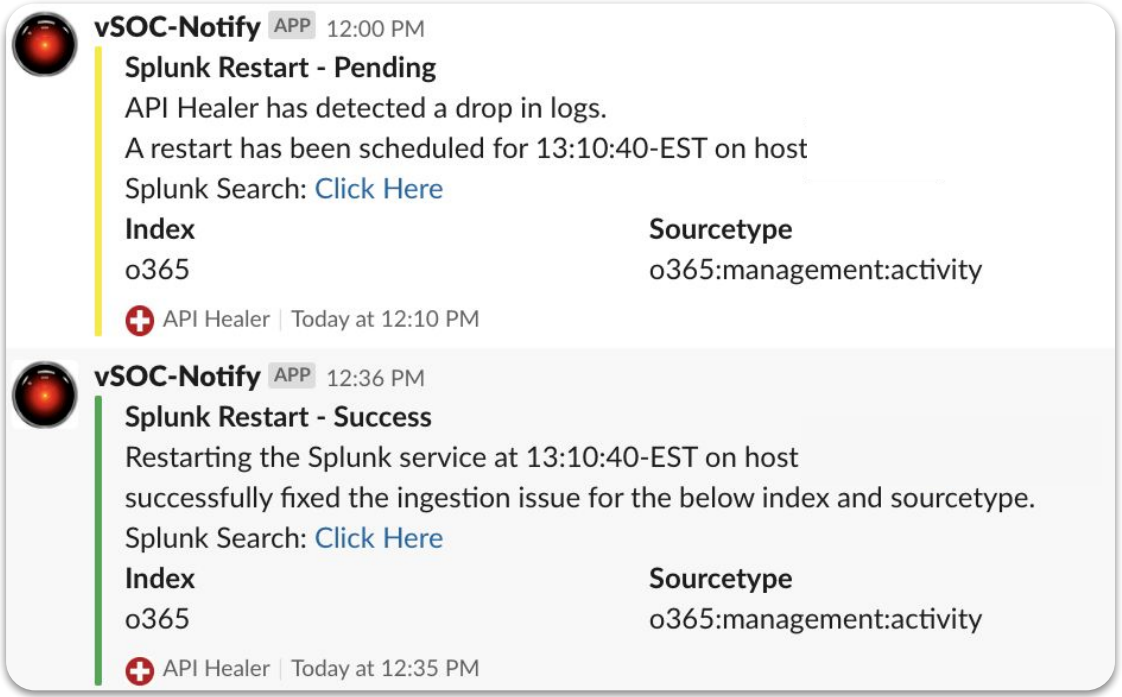


Example API Integration: Slack



splunk> → DEMISTO → slack

Example Automated Response - API Healer

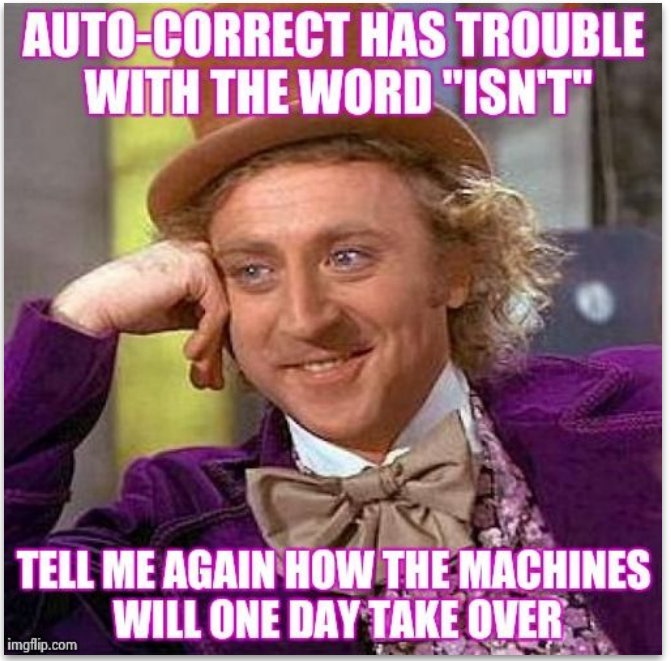


Metrics: A Cautionary Tale

- Most SOAR platforms have an “hours saved” dashboard
- These metrics can be misleading…
- In the wrong hands, these can lead to bad decisions...

The Future… in the year 2000

- All API (No VPN)
- Zero Trust
- Host Isolation
- Host Rebuild
- VPC Wipe
- Chaos Monkeys
- Active Response
- Human Mediated Orchestration



deepwatch

Outline / Notes - REMOVE

- Who am I?
- What is deepwatch?
- In the beginning…vSOC (manual builds, etc.)
- Automation Initiatives
- deepwatch SOAR approach
  - Blocking / Tackling
  - Contextualization
  - Automation of Analyst and Engineer Tasks
- The path forward - automating all the things
  - Analyst tasks (contextualization, click gos)
  - Engineering tasks (server / service restarts)

deepwatch