ISE® AWARDS

WEST

Summit & Awards

20 YEARS

Project Threat Exterminator

Gavin Guttersen

CISO, NetApp

Nominee Showcase Presentation

Company & Team

NetApp

Project Team

Damon Love
Security Architect / Project Lead

Bartosz Jelen
Telemetry & Integrations

Jayesh Dalmet
Telemetry & Integrations

Beeson Cho
SIEM Migration & IR operationalization

Global Security Team
Deployment & System Improvements

Gavin Guttersen
CISO / Program Owner

Mignona Cote
CSO / Executive Sponsor

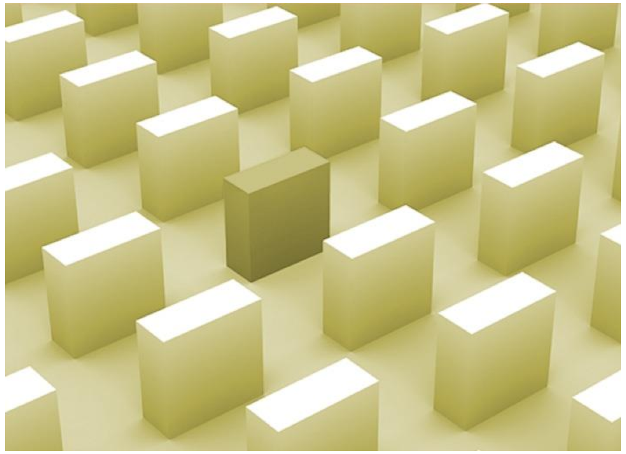
- Focused on helping your business get the most out of your data.
- NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center.
- Over 12K employees
- Over $6B in revenue
- Offices in more than 30 countries
- 98% of organizations are in the middle of their cloud journey, with three out of four reporting workloads stored on-premises, highlighting the need for a unified approach to hybrid multi-cloud architectures

Overview

- Why we took on this project
- What we did
  - Security posture at a moment in time
  - Real time security operations
- Architectural reference
- Lessons learned
- How to link up and talk more about the topic

Challenges

NetApp Global Security needed to solve three big challenges to enable our next generation SOC platform to create enterprise-wide security visibility



1. Data scale, data deduplication, data retention, and ingestion of disparate security logs across a global organization
2. Increase threat coverage while minimizing reliance on rule-writing
3. Significantly reduce time to containment and remediation

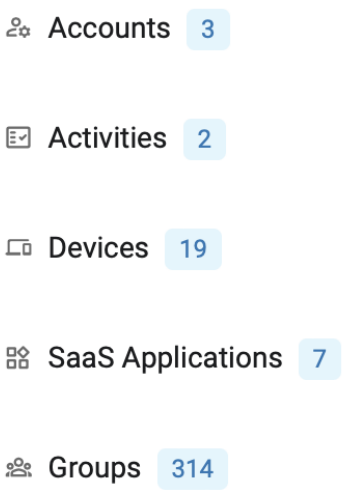
Scope

- ~15 global teams with unique tooling and diverse assets
- Over 600K assets deployed globally
- Cloud forward company, developing in all major hyperscalers
- 30-year-old company with decades of infrastructure
- Culture of innovation and independence
- Multiple tools for SIEM, EUBA, SOAR, DLP, XDR,,,,,,,,, - copying data back and forth

Posture Correlation (Moment in time)

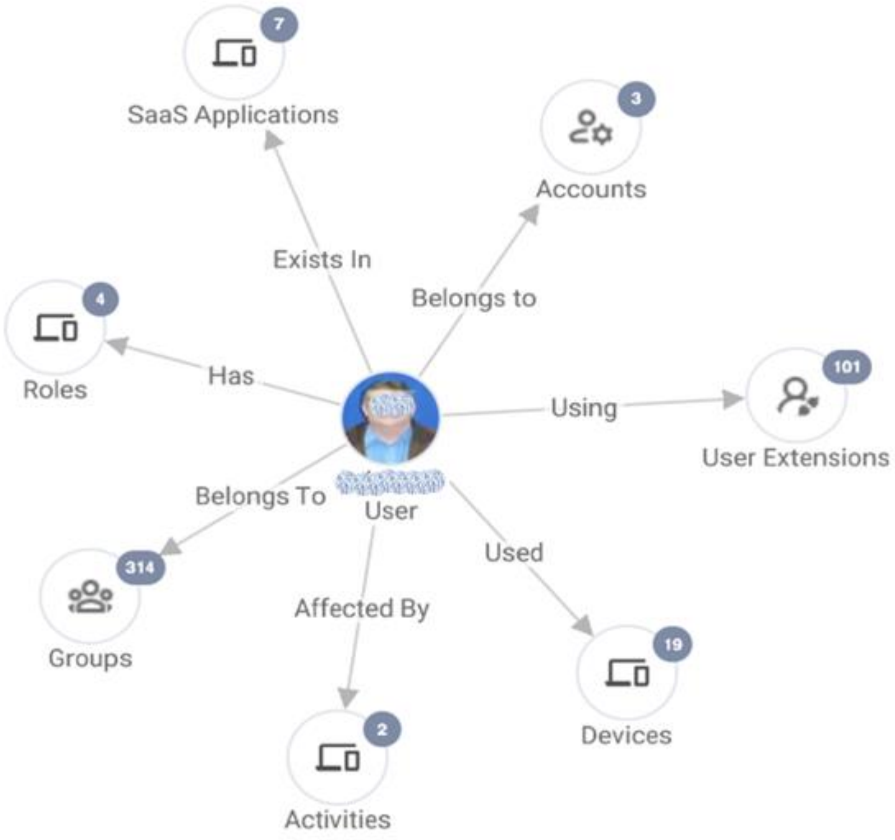
Asset Management
Device Risk Posture
Identity Risk Posture
Compliance Validation

1 User
343 data points



Accounts	3
Activities	2
Devices	19
SaaS Applications	7
Groups	314

AXONIUS



aws
Google Cloud
Microsoft Azure
RAPID7
servicenow
CMDB

50+ Tools

Current State of deployment:

- 250+ feeds
- 612k unique devices
- 357k unique credentials
- 1054 unique SaaS Apps

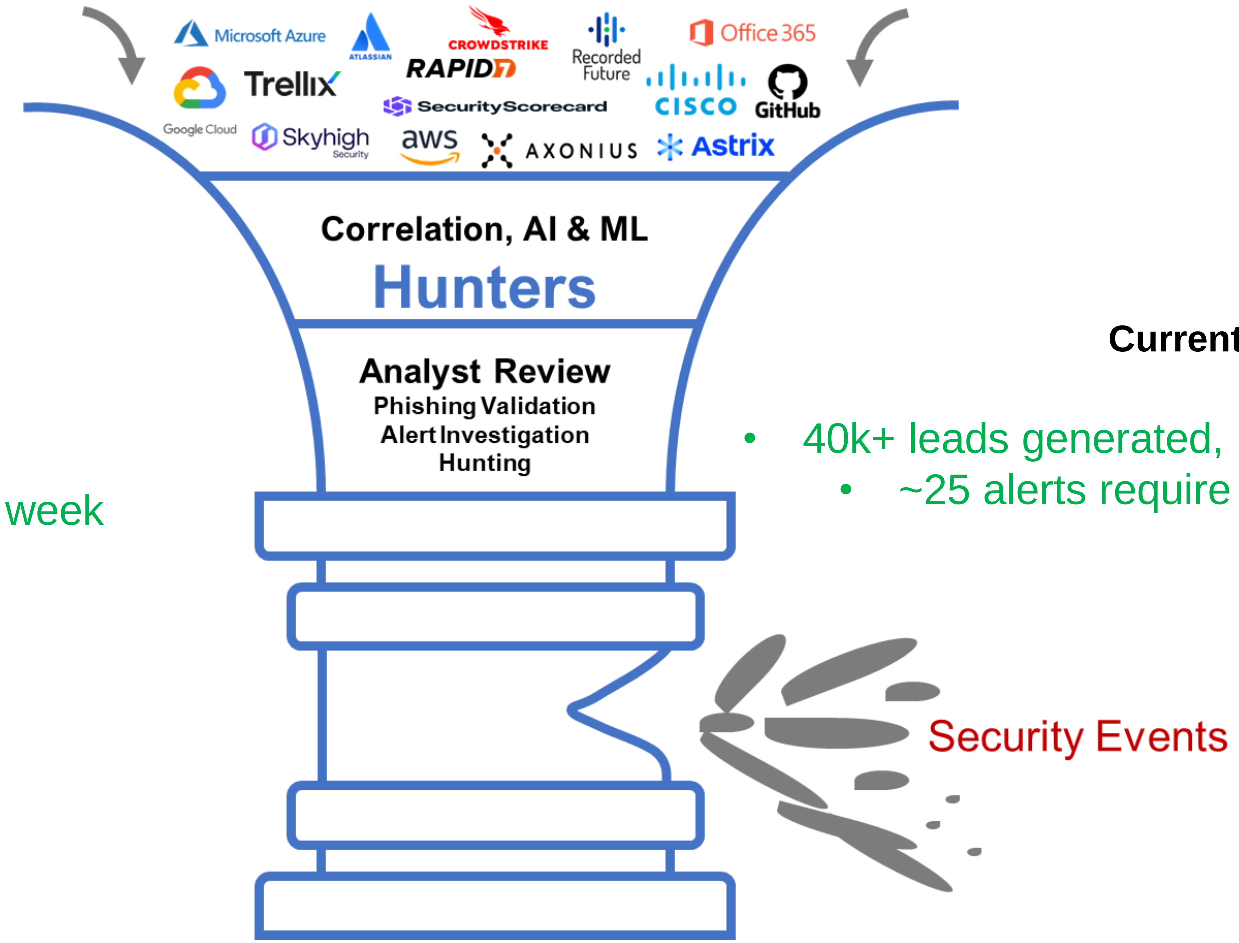
Real time correlation of events

Incident Response
Forensics
Threat Hunting

Current State by the Numbers:

- 17 platform integrations
- 102 data flows
- Data ingest: ~5TB a week
- Cloud Integrations: ~2TB+ a week
  - 600+ AWS accounts
  - 1500+ GCP accounts
  - 100+ Azure accounts
- 295 Active Detections
- 235 Auto-investigations
- 186 scoring models

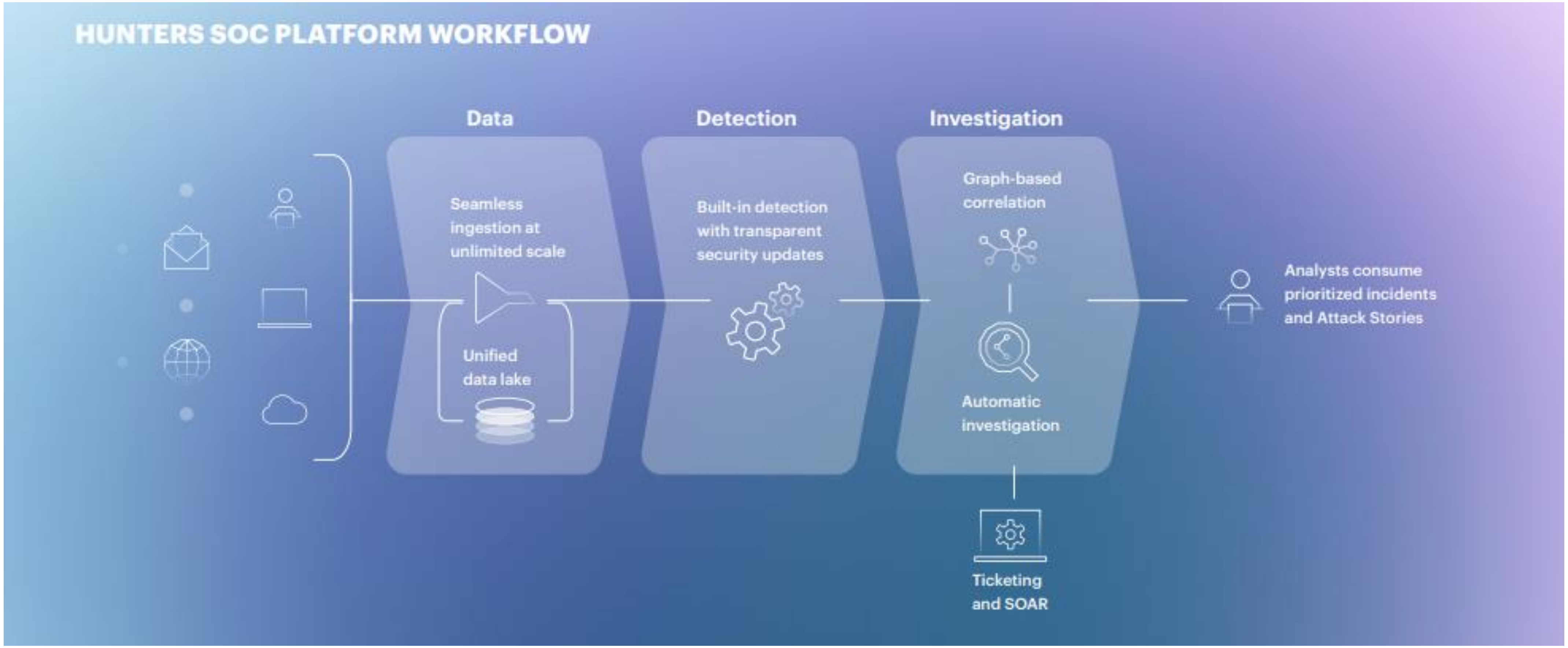
Automated Protections
Firewalls, Endpoints, WAFs (194M)



Current Effectiveness:

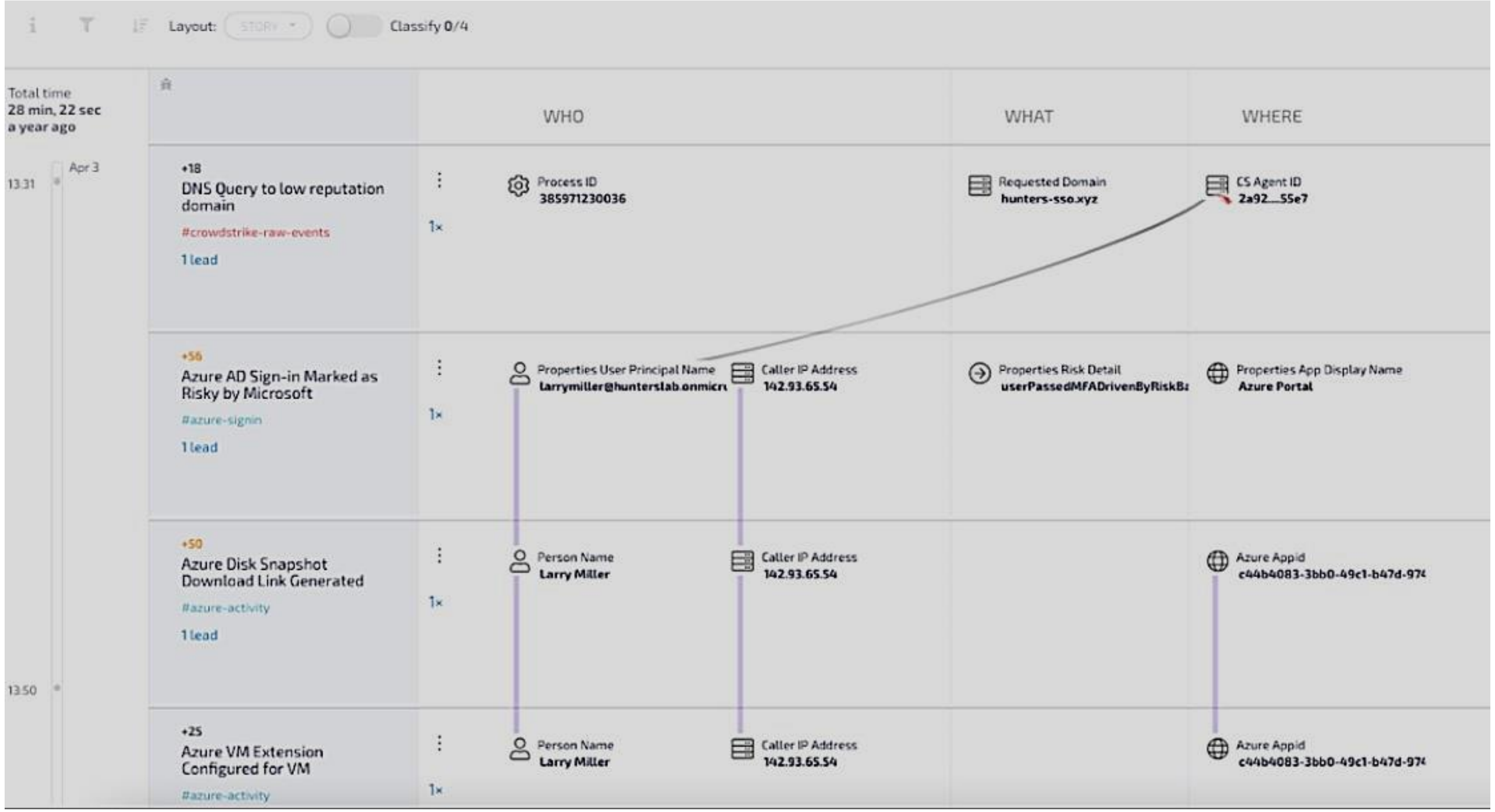
- 40k+ leads generated, corelated and auto investigated
  - ~25 alerts require SOC investigation

Architecture


HUNTERS SOC PLATFORM WORKFLOW
Data
Detection
Investigation
Seamless ingestion at unlimited scale
Unified data lake
Built-in detection with transparent security updates
Graph-based correlation
Automatic investigation
Ticketing and SOAR
Analysts consume prioritized incidents and Attack Stories

A unified security data lake allows for SIEM, EUBA, XDR, SOAR and other security tooling (industry and internally developed) to share one common set of telemetry.

Multi-Data Source Correlation Event (Story)



Layout: STORY Classify 0/4

Total time
28 min, 22 sec
a year ago

13:31 Apr 3

13:50

		WHO		WHAT	WHERE
+18 DNS Query to low reputation domain #crowdstrike-raw-events 1 lead	1×	Process ID 385971230036		Requested Domain hunters-sso.xyz	CS Agent ID 2a92....55e7
+56 Azure AD Sign-in Marked as Risky by Microsoft #azure-signin 1 lead	1×	Properties User Principal Name larrymiller@hunterslab.onmicr	Caller IP Address 142.93.65.54	Properties Risk Detail userPassedMFADrivenByRiskB	Properties App Display Name Azure Portal
+50 Azure Disk Snapshot Download Link Generated #azure-activity 1 lead	1×	Person Name Larry Miller	Caller IP Address 142.93.65.54		Azure Appid c44b4083-3bb0-49c1-b47d-974
+25 Azure VM Extension Configured for VM #azure-activity	1×	Person Name Larry Miller	Caller IP Address 142.93.65.54		Azure Appid c44b4083-3bb0-49c1-b47d-974

- Multiple detections (**leads**) are auto-correlated from various telemetry data creating an investigative snapshot (**story**)
- Stories provide a "Big Picture" canvas with security events of interest for the analyst
- Contributing leads (individual detections) can be modified based on benign-activity or false positive events

Lessons Learned/Best Practices

- ✓ Don't underestimate the scalability needed in a tool that will be deployed in a large, global organization - You will get much more data that you are told people have
- ✓ Engage with an active development partner – New use cases and security logs are encountered frequently in a project this size
- ✓ Build your scope and least privilege as early as possible – To reduce the work needed when the platform grows
- ✓ Identify value you can bring to your partners – They will gladly invest the time for your effort if they understand the benefit to their teams