A Vision for Shared, Central Intelligence to Ebb a Growing Flood of Alerts

Dan Plastina
Partner Director, Threat Protection
Microsoft Corporation
@DanPlastina
A Vision for Shared, Central Intelligence to Ebb a Growing Flood of Alerts

Dan Plastina

Director, Threat Protection
Director, Information Protection
Microsoft
@DanPlastina and https://aka.ms/DanPlastina
In the context of today, who are ‘we’

Microsoft does more than sell software.

We also are:
- a leading provider of cloud platforms.
- an operator of many large SaaS applications.
- a large org, with a complex IT footprint of our own.

We, like you, are deeply responsible for the security of our offerings...

We’re doing this for a living too!
THE MICROSOFT INTELLIGENT SECURITY GRAPH

- 200+ global cloud consumer and commercial services
- +1B Windows devices updated
- 300B monthly authentications
- 18+ billion Bing web pages scanned
- 200B e-mails analyzed
YOU (WE) HAVE A PROBLEM

DETECTION
Insights come from logs, support calls, core services, humans, 'scanners', etc.

DROWNING IN DATA

INTELLIGENCE
TI is acquired from providers, web searches, news feeds, peers, suppliers, etc.
Ingestion is difficult, untimely and ad-hoc: purchased TI is a 'lookup resource'

SIEMS
Signals growing far faster than staffing; New sources welcomed with a <sigh>
YOU (WE) HAVE A PROBLEM

WHERE WE NEED TO BE

INTELLIGENCE
should be part of the security framework, not just a referenced artefact

DETECTION
Detectors should be automated, correlated and interlinked in their findings

SIEMS
Must reduce busy work of incident roll-up, response, and management
CISOs prefer “We’re seeing a pattern similar to a peer org” vs “Oops”

EVENTS
SecOps want to review the ‘needles’, not full ‘haystacks’.

FEEDS

INCIDENTS
High skill (and pay) SecOps should be focused on the more skilled tasks.

LESS OBVIOUS, SECOND-ORDER PROBLEMS

LESS OBVIOUS, SECOND-ORDER PROBLEMS

IMPROVING YOUR EFFICIENCY

IMPROVING YOUR EFFICIENCY
(LESS) OBVIOUS, SECOND-ORDER PROBLEMS

WHERE WE NEED TO BE

INCIDENTS
Software should consolidate, de-dupe, and otherwise prepare ‘Incidents’.  

EVENTS
ML/AI should make the data work for humans, not the other way round

FEEDS
Orgs seek industry/geo specific intelligence to correlate against their signals
INTelligent Security Graph

What it means for you
Malware attacks
Phishing
Denial of service
Unauthorized data access
Data encryption
System updates
Multi-factor authentication
Enterprise security
Spam
User accounts
Device log-ins
User log-ins
DOS attacks
THE LANDSCAPE WE ARE ASKED TO PROTECT
THE LANDSCAPE WE ARE ASKED TO PROTECT

Lot of users with PCs and devices

Lot of servers/VMs

Many repositories of sensitive data (HR, Legal, R&D, M&A, Finance)

Managed network gear

Several SaaS apps

Some partners we collaborate with

Several ‘vendors’ working from outside the trust perimeter, with their unmanaged PCs and devices
CENTRALIZED INTELLIGENCE
LOCALIZED INTELLIGENCE

User/Entity Behavior Analytics (AADIP)

Cloud Directory Services (AAD)

Cloud Application Security Broker (MCAS)

Cloud DC Management (ASC)

Federation Services (ADFS)

Data Loss Prevention (Office IP/DLP)

Cloud Application Security Broker (MCAS)

Threat Intelligence (TIaaS)

Cloud DC Management (ASC)

User/Entity Behavior Analytics (ATA)

Classification and Information Protection (AIP)

Malware Detection (Office ATP/Sonar)

Cloud DC Management (ASC)

On Premises Directory Services (AD)

Endpoint Protection (Defender)

Mobile Device Management (Intune)

User/Entity Behavior Analytics (ATA)

Data Loss Prevention (Office IP/DLP)

Mobile Device Management (Intune)

Cloud DC Management (ASC)

Threat Intelligence (TIaaS)

Endpoint Protection (Defender)
ENTRUSTING THE FEW

Weaker Hub-and-spoke interconnection
Jack of all trades and thus an expert in none/few
Latent (non real time) interactions
Distance reduces auto-remediation
DISTRIBUTING INTELLIGENCE VIA THE GRAPH

Rich interconnection
Contextual Deductions
Near real time interactions
Improved ability to auto-remEDIATE
VISUALIZING THE INTELLIGENT SECURITY GRAPH

- Security Consoles
- Email / Team Security Bots
- Programmatic Access
- Advanced Visualizations
SPECIALISTS PREFER SPECIAL TOOLING

Network Specialist

Data Protection Specialist

Identity Specialist
SECOPS IS A **SPECIALIST** TOO

A console
- anchored in incident management
- to navigate ‘fused’ incidents in micrograph form
- tuned to facilitate common tasks via actions/runbooks
- enables the analyst to provide feedback to the graph (FN/FP)
Security-focused ChatBot

- In-situ assistance for tedious tasks.
- CC a Security bot on an email to get an IP address lookup.
- Be invited to a chat session to have a richer interaction.
- The tedious tasks are greatly streamlined leaving SecOps to work on the hard stuff.
100% Fidelity Programmatic Access

- Extends Microsoft Graph
- Contributors to the graph (Detectors) create securityDetection nodes
- Aggregated detections create and/or extend securityIncident nodes
- Storage for each node is the responsibility of the node provider – the graph is NOT a central store of all data; it’s the discovery mechanism and shared lingua franca across all providers.
- Enriched nodes only appear if their associated ‘product’ was purchased.
Advanced Graph Navigation

Modes of visualization have come a long way...
YOUR ROLE IN **CHANGING** THE SECURITY LANDSCAPE

- Re-examine your security posture
- Best of Breed vs Best of Suite
- Investigate SecOps inefficiencies

Share them with us [aka.ms/danpl](aka.ms/danpl)
Where to learn more about solutions mentioned today

- Active Directory
- Active Directory Federation Services
- Advanced Threat Analytics
- Azure Active Directory
- Azure Active Directory Identity Protection
- Azure Information Protection
- Azure Security Center

- Cloud App Security
- Intune
- Office 365 Advanced Threat Protection
- Office 365 Data Loss Prevention
- Operations Management Suite
- Windows Defender Advanced Threat Protection
Thank you

@DanPlastina
aka.ms/danpl