Triage: The Art of Threat Detection and Risk Assessment
The Modern Cyber Threat Pandemic

Motivated and Well-Funded Threat Actors
- Malicious Insiders
- Terrorists
- Nation States
- Organized Crime
- Hacktivists
- Users

Creative and Sophisticated Attacks
- Zero-Day Exploits
- Social Engineering
- Spear-Phishing
- Custom Malware
- Physical Compromise

Expanding Attack Surface
- Endpoint
- Network
- Cloud and SaaS
- Mobile Devices
- IoT

Well-Established Cyber-Crime Economy
- $0.10 to $20
  - Credit Card Number, E-mail Accounts (per 1000)
- $5 to $8
  - Cloud Accounts
- $50
  - per Healthcare Record
- Up to $3,500
  - Custom Malware
- Up to $1,000 / day
  - DDoS Attack

Source: Symantec, Underground black market: Thriving trade in stolen data, malware, and attack services. November 20, 2015; Medscape, Stolen EHR Charts Sell for $50 Each on Black Market, April 28, 2014
Signs of a good triage process

- Detecting the “Unknown”
- Coordination and Communication
- Threat Analysis
- Safe Threat Eradication
- Effectively
Setting the stage

- Operations room
- Millions of events
- Some good, some bad
- Cautious of alarm fatigue
- Operations team
  - Ready to respond
  - Monitor for the unexpected

Random detection and response doesn’t work

- Having the Right Tools Is Critical:
  - To detect suspicious events
  - To determine risk
  - To take action
Vigilance requires visibility at every vector

Holistic Attack Surface
Network wide visibility and analytics

Forensic Data

Network Devices
Security Devices
Systems & Applications
Industry Specific Devices
Identity Services

Analysis Conditioning

Time Normalization
Data Classification
Meta Data Extraction
Context Infusion
Risk Prioritization

Real-Time Analysis

Advanced Correlation
Behavioral & Statistical Baselines
Pattern Recognition
Whitelist Profiling

Forensic Analysis

Search
Visualize
Pivot/Drill Down
Manual discovery of what’s normal network activity is impractical due to the sheer volume of data across multiple types of dimensions.

- An unmanageable volume of false positives based on benign anomalies
- Significant blind spots / false negatives

Need an automated technology to learn behavioral attributes across multiple dimensions.
The question

• To escalate or not?

• RULE: Trust but verify

• WHY: You’re only as good as your last incident
Showing how AMP Threat Grid enables “Trust but Verify”
AMP Threat Grid platform allows you to correlate the sample result with millions of other samples and billions of artifacts.

- Proprietary techniques for static and dynamic analysis
- "Outside looking in" approach
- 700+ Behavioral Indicators

File Submissions

An analyst or system (API) submits suspicious sample to Threat Grid.

An automated engine observes, deconstructs, and analyzes using multiple techniques.

Actionable Intelligence

Threat Score / Behavioral Indicators

Big Data Correlation Threat Feeds

Sample and Artifact Intelligence Database

Actionable threat content and intelligence is generated that can be utilized and integrated into a variety of existing systems or used independently.
Single Click to Enable Cisco AMP Threat Grid Integration

Threat data immediately leveraged in machine-based analytics and automatic evidence corroboration.
On-the-fly Lookups provide key details at the time of need
Integrated case management preserves all evidence to expedite analysis

Reduce time to detect, qualify emerging threats
• On-the-fly Lookups provide key details at the time of need
• Integrated case management preserves all evidence to expedite analysis

Reduce time to detect, qualify emerging threats
The triage confirmation

AMP Threat Grid

Samples
Find samples via the Submission Search API.
- The **Match by** form field corresponds with the **Terms** of the search API (documented in section 5 of the Search API help).
- Utilize wildcards when searching for samples which might adhere to a pattern, for example, a **Mutant** search for the query `gazavat-svc_*` could return samples that match on the mutants `gazavat-svc_34`, `gazavat-svc_18`, and `gazavat-svc_37`. (Note that the wildcard character is significantly more efficient as the trailing element of a query, as shown above, rather than the leading element.)

Search samples
- **Query**: iybwuf.com
- **Match by**: Freeform
- **Date range**: Last 30 Days
- **Scope**: All samples

Results
- **Name**: exe
- **Type**: exe
- **Started**: 9/15/16 12:20 pm
- **VM**: winxp-x86
- **Threat score**: 100
- **Tags**: analysis.domains.domain

LogRhythm
The Security Intelligence Company
Virut is a widespread file infector that has survived a number of takedown attempts. Virut can spread itself through network shares, and is also distributed through malicious email attachments and compromised websites. Virut may also be downloaded and installed by other malware. Once executed Virut installs a backdoor. Older variants of Virut communicate over IRC, newer variants have been observed to use a custom protocol.
Quickly capture scope of incident
Enabling fast effective triage

The marriage of visibility and context

- More confidence
- Faster decisions
- Effective response
LogRhythm and Cisco AMP Threat Grid

- Correlate indicators of compromise (IOCs) to detect and respond to:
  - Dangerous IPs accessing internal infrastructure
  - Users visiting risky URLs
  - Phishing attempts
  - Malware propagation
  - Other high impact activities

- Corroborate activity and expose behavioral anomalies:
  - Raises prioritization of corroborated activities exhibiting compromise or infestation
  - Reduces false positives and delivers even higher qualified alarms
A complete solution: Integrated for ease of use and efficient workflow

- AMP Threat Grid – Greater Context and Understanding of a Threat
- LogRhythm - Internal Context, Security Analytics, Detection, Response
Questions?