RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-R01

What you don't see WILL breach you! "Intelligizing" detection through context

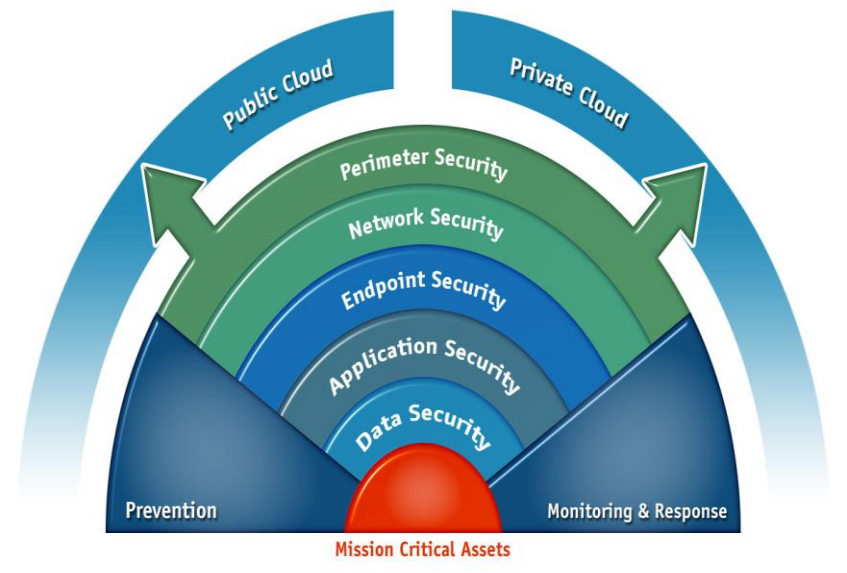
Gaurav Kapil
Cyber Architect
Information Systems Sector / Cyber
Northrop Grumman Corp

Bryan Krekel
Manager, Strategic Counterintelligence
Information Security
Northrop Grumman Corp

State of Cyber Capabilities for Insider Threat Detection

Traditional Defense-in-Depth Model Still Lacking

Layered Defensive Model



- Largely externally focused
- Host Based
- Network Based
- Weak behavioral analytics
- Relies on known signatures
- Reactive, response oriented
- Reputation based detection systems

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Enhancing Defenses Against Internal Threats

#RSAC

Conceptual Model for Insider Threat Detection

- All source integration of technical and non-technical data sources
- Create holistic view of risk, not just identification of illicit activity underway
  - Predictive, intelligence driven capability vs incident response program
- Participation by multiple stakeholders from within an organization
  - HR, Legal, Information Security, Personnel Security, Finance/Travel
- Create a capability to identify and investigate ‘precursor’ activity when risk increases
  - Predictive, risk management and counter-intelligence oriented
    - Pro-actively identify risk based on employee behavior and deviation from norm;
    - Enables intervention *before* loss occurs;
    - HR counsel and potentially support troubled employees;
    - Increase potential to retain talent.
- Organizational governance to account for multiple stakeholders, investigative procedures, data security requirements

Define Program Intent

- Proactive, holistic risk mitigation or network based incident response / data loss prevention?
  - Identify & investigate precursor activity or respond following concrete evidence of violation?
- Predictive, risk management and counter-intelligence oriented programs allow:
  - Pro-active identification of threats;
  - Potential for intervention before loss occurs;
  - Counsel and support troubled employees;
  - Improve retention, reduce risk of loss, recruiting/hiring.
- Not a semantic exercise –Practical implications for resource allocation, planning, program management

The Weighting and Scoring Black Hole

- Approaches that assign arbitrary weights and variables to individual activity can be analytic black holes
- No industry standard for scoring discrete variables associated with insider threat activity
- Lack of definitive industry standard can create legal liabilities
  - Program and analytic rigor paramount
- Alternative: analytic models comparing deviations from previously baselined behavioral norms
  - Greater deviations from standard can imply greater potential risk

Predictive Analytics vs Reactive Defense in Depth

Start Up Costs

- Data Integration targeting insider threats
- Automated analysis of large data sets
- Automated tool suite
- Dedicated staff, specialized skills
- Access controls, program security

Return on Investment

- Data removed from enterprise silos
- Improved contextual understanding of insider threat risk
- Early warning of threats to data & networks
- Shift defensive posture from reactive to proactive
- Potential remediate risk *prior* to loss

Behavioral Analytics and Modeling

- Behavioral analytics are essential
  - Reduces sole reliance on technical indicators of loss
  - Aggregation of data points defining singular events in time are meaningless without greater context to understand “normal”
- Non-technical indicators blended with network behavior
  - Psychological predicators and behavioral indicators of insider threats
  - Risk profiles and scoring mechanisms
  - Privacy rights considerations for private sector makes modeling, profiles challenging
  - Aggregate data already collected by HR, Legal, Security, etc
- Data security paramount

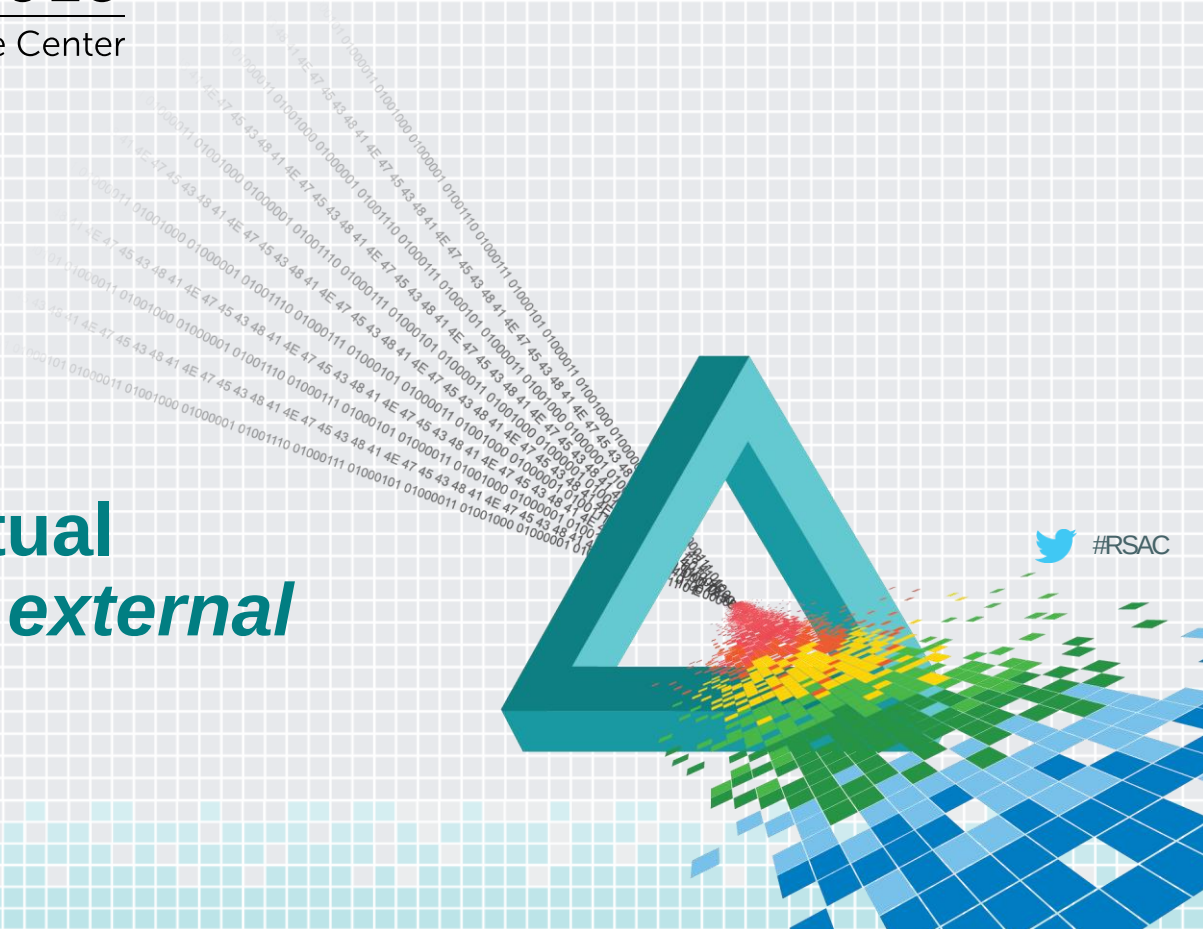
All Source Analysis Is Essential

- Relying on single sources of intelligence ("INT's") to detect malicious activity is a losing gambit;
- Review of network activity in context of employee HR records, work related travel/financial records, flight risk, etc
- Insider threats arise from a complex interplay of human factors;
  - Technical indicators such as data movement or privilege escalation are only a faint reflection of human motive, mood, or predilection for taking action against an employer;
- Network based indicators alone do not provide a fully contextualized picture of risk
- Employee decision to commit malicious act rarely rash act; often prepared over time

Data Volume Matters, Quality Matters More

- Automated analysis of large data volume is essential for behavioral anomaly detection.
- Typical profile of data required for a mature predictive, pro-active insider threat program:
  - Highly disparate sources and file types;
  - Extremely large data sets covering months or years of activity;
  - Often rapidly changing content
  - Combination of structured and unstructured data formats
- Key to identifying areas of highest risk is pattern analysis of all of the above making manual efforts nearly impossible.
- Data mining, pattern analysis, baseline analysis, deviation from typical patterns of employee behavior all demand automated tool suite
- Data sets must be carefully curated to ensure program is bringing in the right data to answer your standing intelligence requirements

Enriching contextual understanding of *external* adversaries



Current limitations…

- Current detection systems fail to leverage & capitalize on contextual information available in their networks
  - This very information may be critical to the performance and accuracy of these systems as the networks they are deployed in differ significantly with each other in terms of policy, the topological layout, the vulnerability landscape, the exploits observed, the traffic characteristics, etc.
  - Limited correlation

Defining Security Context

- Vulnerability Profile
  - Represents the space of all possible targets and ideally all methods of unauthorized access to those services
- Attack Surface
  - Represents the unique threats posed by attackers to the defenders of a particular network
- Usage Model
  - Helps defenders prioritize the importance of the services on the network & respective consumption of the same.
- Diversity amongst networks and the dynamic nature of the context can lead to changes in security context.

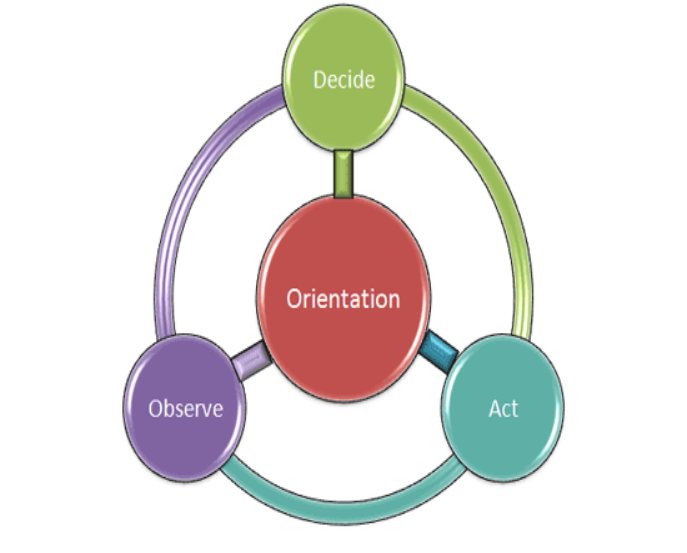
Context Aware Security Analytics

- Observe
  - Visibility into the network traffic and system activity
- Orient
  - Behavior analytics
- Behavior Modeling
  - Each user measured against individual norms and peer group norms
  - Characterized by a six dimensional feature vector constructed during session
    - Hour of login
    - Duration of session
    - Number of HTTP accesses
    - Number of File accesses
    - Number of e-mails sent
    - Removable device accessed (boolean)

Within your Opponents Decision Loop

Context Aware Security Analytics

- Decide
  - Transformation of data into actionable intelligence
- Act
  - Pre-empt incident
  - Reduce “dwell-time”
- Sixth Sense –
  - Initial stages can be art
  - Progress towards making it a science.



Structuring your defenses

- Automatic adaptation to the network context
  - To significantly improve the performance and accuracy of security systems
  - Explicit addition of context to events
    - Location
    - Role
    - Activity
    - Time
    - Operating environment
    - Workload
    - Type of network traffic
  - Takes into account
    - Vulnerability Profile
    - Attack surface
    - Usage Models
- Employ defenses based on context

Intelligence Gathering…Capturing new threats

- Network Aware Honeynet Configuration
  - Individual honeypots provide excellent visibility into threats that affect specific host and operation system configurations
  - However for large disparate networks – model fails to scale as decisions must be taken as to what systems need to be protected and what attacks need to be observed
  - Can lead to ad-hoc approaches to honeynet configurations – reducing strategic advantage.
- Propose:
  - Honeynets should be configured with individually consistent hosts and proportionally represent the surrounding network
  - Automated approach based on profiling the network & random sampling to generate honeynets with proportional representation hosts and network environment.
- Result:
  - Honeynets providing an accurate view of threats to the network and resistance to discovery.

Enhanced application level threat detection

- Continuous monitoring of available data streams
  - User activity
  - Electronic assets
  - Data resources
  - System logs
- Pattern matching – establishing normal behavior
  - Normalization of roles, user and corresponding activities.
  - Data access,
  - User behavior,
  - Computer activity,
  - Application activity,
  - Network activity.
  - Keystroke Dynamics.
- Anomaly Detection by Co-relation of disparate data sources to identify potential malicious behavior.
  - Pattern Matching against normalized behavior
  - Heuristics – Is behavior outside of normalized behavior

Conclusion

- Addition of contextual information enhances understanding of adversaries.
- Blending technical and non-technical data provides crucial context for identifying internally sourced threats
- Analytic models that compare deviations from previously baselined behavioral norms are more effective for insider threat detection scenarios.
- Network based indicators alone do not provide a fully contextualized picture of risk for internal threats.

Applying the Principles

- Know your operating environment
  - Develop activity & usage models
  - Create Inventory of consumable activity streams
  - Aggregation, Correlation and Alert models
- Insider Threat Detection:
  - Next week: identify stakeholders for technical and non-technical data across your organization, draft a program CONOP, identify data types for use in your program;
  - First 3 Months: Complete CONOP, initiate regular discussions with data owners, begin evaluations for “make/buy” decision on analytic tools
  - Within 6 months: initiate procurement for tool suite, obtain concurrence of data owners for program structure and CONOP; identify staff to support program.