TECH TALKS: SUPPORTING THE REMOTE WORKFORCE

Monitoring for Insider Threats in Turbulent Times
PANELISTS TODAY

Host: Brad Six
Technical Product Evangelist

Guest Speaker: Mark Brooks
VP Customer Solutions

- Enter comments anytime via Q&A Window at the bottom
- All Tech Talk recordings are here - https://www.graylog.org/tech-talks/s1
THE INSIDER THREAT

Tough to talk about, but must be addressed

Challenges

● Frequent changes
● Insider knowledge
● Systems outside AD/LDAP
● When privileged users leave
● Hackers know account termination is an issue

Intentional Behavior Risks

● Privilege escalation
● Creating new accounts
● Shared accounts
● Data exfiltration
● Fraud
TRACKING A BEAR

Tools, tools the wonderful fruit

Consolidation of all (relevant) log sources & alerts

Build complex queries in minutes, get results in milliseconds and share workflows with teammates

Create unique data visualizations using enriched data

Quickly and easily pivot from alerts to root cause analysis
CENTRALIZED COLLECTION & PROCESSING

1. Collection
   - Windows
   - Linux
   - Unix
   - JSON, CSV, TXT
   - Commercial Apps
   - Custom Apps
   - Firewalls
   - Switches
   - Routers
   - Network
   - DBMS
   - Storage Mgmt
   - Change Mgmt Systems

2. Enrichment

3. Analysis, Action & Storage
   - SIEM
   - SOAR
   - Service/Help desk
   - App PerfMon
   - UEBA
   - Network PerfMon
   - IDS/IPS
MONITORING USER BEHAVIOR

MONITOR THE ADMINISTRATORS ACTIVITY

Event Logs Cleared by User

Scheduled Tasks by User

Top 10 EventID's By User

Domain Policy Changed by User

Users Added to Admin Groups

Domain Groups Created by User
MONITORING USER BEHAVIOR

FIND OUT WHERE THE ACCOUNT WAS LOCKED OUT
MONITORING USER BEHAVIOR

Alert on suspicious activity

- Geolocation, Time of Day, Frequency
- The unusual has become usual and the usual, unusual
- Balance alert rules granularity with quantity
HIGHLIGHTING RISK

Leveraging Dynamic Lists

Integrates Alert Parameters and Lookup Tables

Define a Filter with Parameters.
When the event definition is being checked, these parameters are replaced with the result of a configured Look up table.

Endless Possibilities
Compliance
Policy Violations
Behavior Validation
Positive AND Negative Conditions
Any Normalized Field
Per Field Correlation
Perform correlation on logs while aggregating on a specific field. This allows unique field alerting (i.e. User Name)

Cross Event Source Correlation
Monitor for a pattern of logs across multiple log sources, so you can see the login happening right after the IDS log from the same IP address

Look for the Negative Event
Monitor for logs not there. When your web server shuts down you want to see it start back up, what if it doesn’t?

Complex Correlation
Feed your correlation alerts, back into the alert feed to be built upon for another alert. Detect the brute force attack, and alert if someone creates a user right after.
QUESTIONS?
● TechTalks@graylog.com

FOLLOW US
● Twitter: @graylog2
● Linkedin: Graylog
● Reddit: /r/graylog/
BUT WAIT, THERE’S MORE!

14 May - Collaborating To Improve Availability, Root Cause Analysis
21 May - Threat Hunting Techniques For Today’s Biggest Threats

SPECIAL PRICING ON 10GB & 20GB PACKAGES WITH JUMP START SERVICES