GBprotect

Personalized Approach • Better Security

Real World SIEM

ISSA Portland Symposium on SIEM

October 22, 2015

Speaker Bios

- **Todd Reder** is a Solutions Engineer with GBprotect. Over the past nine years, Todd has progressed from handling escalations as an operator, conducting client security reviews as an analyst, and on to his current role which includes platform management, client turn up, and consulting engagements. His SIEM experience includes management and day to day operations of ArcSight, LogRhythm, Splunk, QRadar, LogLogic, and enVision. Todd is a Splunk Certified Architect and LogRhythm LCSE.

- **Andrew Riley** is VP of Security Solutions at GBprotect with responsibility for Sales Engineering, Professional Services, and Product Development. Mr. Riley has close to 25 years of IT experience and has held a focus on information security since the late 1990's. Andrew holds CISSP, C|CISO, and HCISPP certifications and is a former Portland ISSA Chapter president.

Company Overview

Highly focused managed security service provider
delivering next-generation security management services

Security Operations

•

Strategic Consulting

•

Application Security

"GBprotect consistently provides a superior level of service compared to traditional MSSPs. Their intimacy with our network and operations is incredibly valuable."
-- Information Security Director, Financial Institution

- Flexible high-touch specialty managed security services
- US-based global service provider
- Manage security events for over 20,000 devices in 18 countries
- 12 year history of growth and profitability
- Industry leading customer retention
- Focused exclusively on information security services

GBprotect
Personalized Approach • Better Security

GBprotect SIEM Context

- Core platform is ArcSight ESM and Logger (Partner since 2002)
- Providing full management for client deployments of:
  - QRadar
  - LogRhythm
  - LogLogic

SIEM Made Simple?

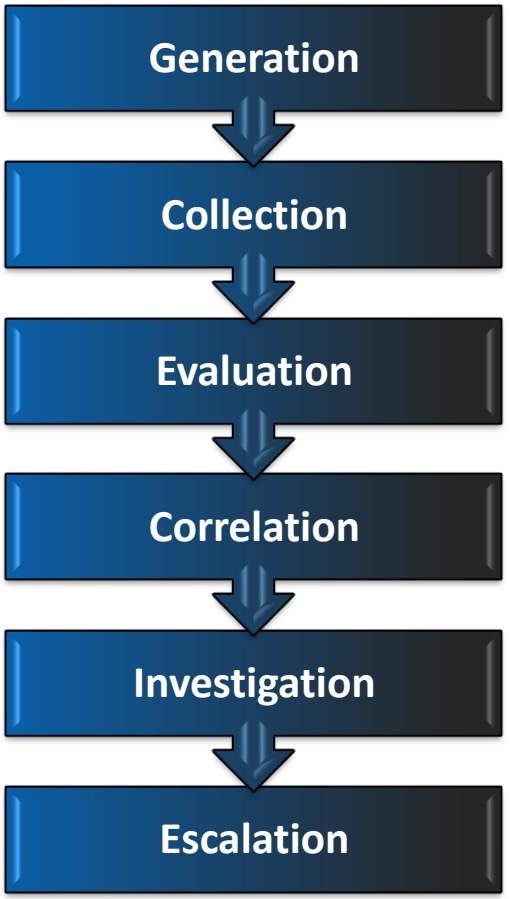
- SIEM technology is powerful and evolving
- Most people are cooking with a partial recipe
- To get from concept to business value…Here are some of the missing pages

Identifying Purpose

- What are we trying to accomplish with the SIEM?'
  - Compliance? Security? Business Insight?
- By knowing our purpose we can start defining the specific use cases that will help us meet those goals.
- Defining use cases should be a team sport.
- What's built in?
- Other sources
  - vendor forums, update and vulnerability notifications, industry sites, and conferences.
- Who are the consumers of SIEM alerts and reports?

6 Security Event Management Elements

- Focus:
  - Perform event evaluation & escalation
    - Not all events are evaluated
    - Need to capture, normalize and highlight meaningful or potentially suspect events
- Goal:
  - Produce actionable events that can be escalated & reported on
  - Understand the differences between “Traffic & Audit” Events
  - Define “Actionable” event criteria to meet the objectives of your business



Event Generation

- Select Event Sources that support use cases
- Create a source inventory
- Log source supported by SIEM vendor?
- Log generation options:
  - general log level that is applied globally, individual log settings per rule, or a hierarchy based policy system?
- Log format options: static or customizable?
- Log output options: Syslog? API? File?
- Log configuration options:
  - manual configuration
  - automated via scripting or policy management?

Event Collection

- Two main types
  - Agent
  - Agentless
- Agent Resource considerations
- Parsing, filters, and aggregation
- Processing limits
- Communication protocols
- Documentation is key

Event Evaluation

- Source Acceptance.
- Network and Asset Model
- Use case resources, rules, lists, reports, dashboards, etc.,
  - Try to build resources with efficiency, simplicity, and reusability in mind.
  - Test event streams
    - Live data
    - Generated data

Event Correlation

- Manual likely precedes automatic
  - Capture analyst input
- Time Based
- Frequency Based
- Use Case Specific
  - Host AV detection followed by firewall threat detection involving the same host

Event Investigation

- SIEM is a starting point
  - Normalization only covers PART of the story
- Source console investigation
- Third party intelligence
  - SANS
  - URLQuery.net
  - Virus Total

Event Escalation

- Single source for escalation information
- Provide detail, avoid information overload
- Ticketing
  - Tracks current incidents
  - Historical reference

Tips

- **SIEMs fail in all kinds of ways from logs not parsing correctly to memory exhaustion and database halts.**
  - **Schedule reviews of source configuration, collection, and monitoring resources.**
  - **Validate sources are reporting and agents are running, a SIEM can only function when it's receiving logs.**
  - **Reviewing log volume fluctuation and database usage over time can protect the platform against license violation and capacity issues.**
  - **Agents that are caching, report generation times, and SSL certificate expiration.**

Key Takeaways

- **Understand what you want out of the SIEM**
- **Know the devices that support that functionality**
- **Understand log collection techniques**
- **Build resources with a clear purpose**
- **Monitor the platform to avoid interruption.**