



Security Intelligence in the real world

# Wotif Group – About Us

- Operates a family of leading global online travel brands
- Accommodation in 69 countries around the world
- 25,500 accommodation properties available for bookings
- **One** in every **ten** room nights in Australia was booked through the Wotif Group of brands in the last financial year
- Employs more than 500 people in 19 countries on five continents



- **Leader in online accommodation** in Australia and New Zealand
- Ranked number one visited online travel agency by Hitwise
- Great rates and a broad range of accommodation and flights
- Fast, easy-to-use, **secure** travel website
- 24/7 customer service centre based in Brisbane
- **Trusted** Australian brand
- Receives almost 260,000 bookings per month



# What makes us unique?

- Web Shop Front
- Online Partners
- Growth through acquisitions
- Small amount of externally hosted services/cloud based services
- Many “Custom” developed applications
  
- Evolving security measures
  - AntiVirus;
  - WAFs,
  - IDS/IPS
  - ...



# Maintain our Trust

- Fast, easy-to-use, **secure** travel website
- **Trusted** Australian brand

So what threats are there?

Threat Landscape is constantly changing

# Is this really public enemy #1?













wotif.com



travel.com.au  
ONE DESTINATION. ENDLESS POSSIBILITIES.

live every  
lastminute.com.au

ASIWEB  
DIRECT

LateStays.com  
LAST-MINUTE HOTEL BOOKINGS

Arnold  
Award-Winning Technology Provider

# Summary

- External Threats
  - Script kiddies
  - Botnets
  - Price Comparison crawlers
  
- Internal Threats
  - DOSing ourselves
  - Transient staff and devices
  - Human Error, data breaches
  - Malware
  - Marketing Campaigns – (EDMs; 11 minute deals)



# Other Challenges

- Growing complexity
  - applications
  - infrastructure



- Compliance requirements



# Simplicity





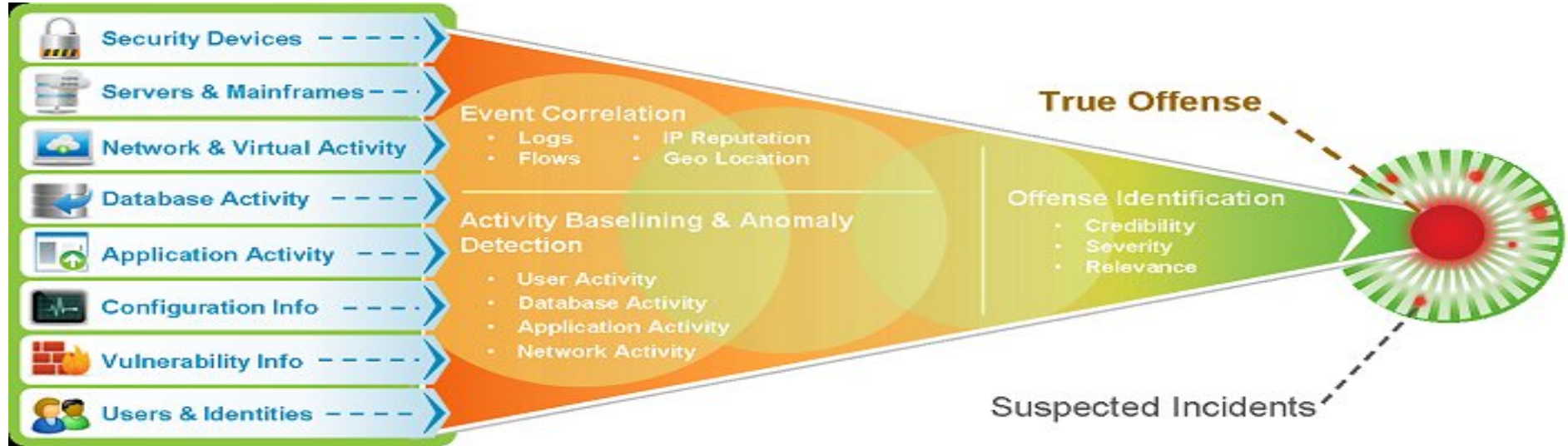


# What we wanted

- Proactive on security
- Leverage existing infrastructure
- Noise filter
- Meaningful Data
- Real-time and Historical views
- Scheduled/batch Reporting
- Vulnerability and Risk based prioritisation



# We need a SIEM!





**Next-Generation SIEM: Security Intelligence**

Category  
Credibility  
Severity

Asset  
Discovery  
Active VA  
Passive VA

Statistical  
Correlation  
Rules-Based  
Correlation

Attacker  
Profile  
IP Location  
External  
Threats

User Logs

Network  
Behavior  
Application  
Behavior  
Identity  
History



**Offense**



**First-Generation SIEM: Rules & Correlation**

# Which SIEM is right for us?



# Which SIEM is right for us?

splunk™ >

 Radar

 ArcSight™

**McAfee**®  
Proven Security™

Tier-3  **HUNTSMAN**®  
Intelligent Security. We invented it.

# Selection Process

- Minimal set selection criteria?
- Short list 3
- Get technical presentations from those 3
- Take 1 for a test drive

# tldr; Criteria

proactive security  
Easy to use  
Correlated Application Logs  
Network flows  
packet capture  
Anomaly detection  
Accessible  
compliance reporting  
Vulnerability Assessment  
Investigation  
data retention  
scalable architecture  
distributed network  
monitoring  
Flexible Device Support

alerts  
Dashboards  
Australian based Support  
user/role privilege separation  
self-service custom log formats  
log sources  
3rd party feeds  
update frequency reports  
custom rules and custom data  
white list; black lists; grey lists  
performant querying  
real-time rule evaluation  
advanced persistent threat detection  
Real-Time analysis



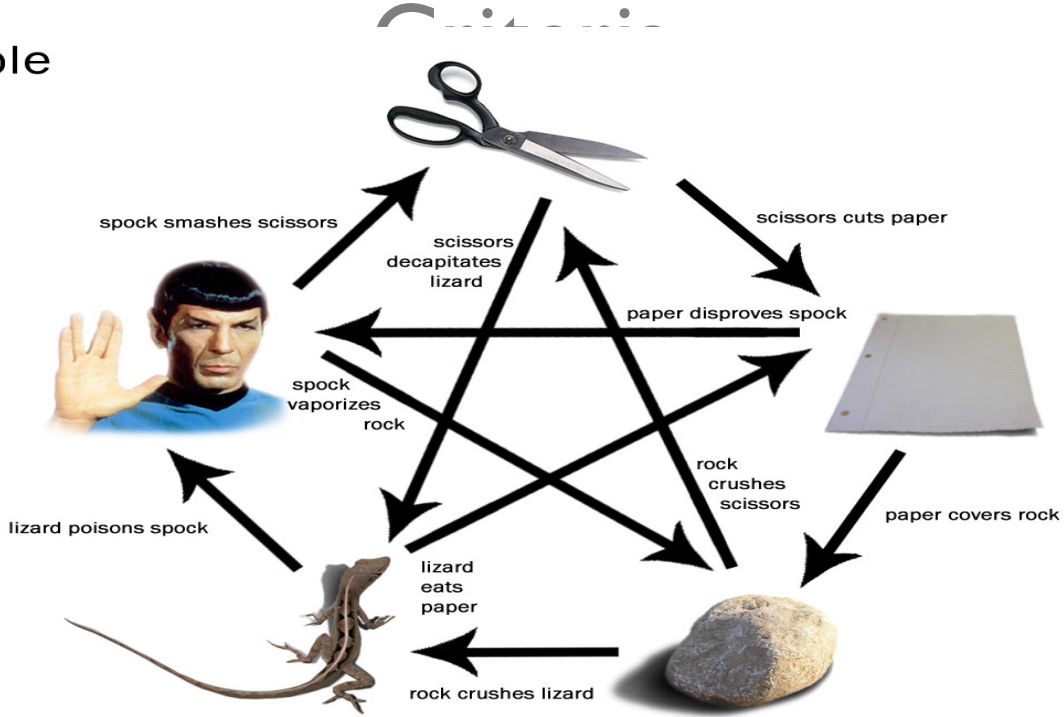
**THERE CAN BE ONLY ONE!**

memegenerator.net

# Discussions



# Its Simple





# The Test Drive

- Pick one



# Sizing and Deployment Options



# Input Sources

- Routers
- Firewalls
- Load Balancers
- OS
- Chasis
- Virtualization
- IPS
- Authentication Services
- “Our Custom Log Sources”
  - Critical that we can define and modify these ourselves

# Event Logs aren't as easy as you think

- Event Logs would be easy?
  - source system syslog versions,
  - single syslog forwarders
  - poor filtering options in source systems
  - custom log formats, lots of options

# Iterative Deployment/Tuning

- Sit back and watch
  - Assisted in resolution of a live back-office issue
- High number of Alerts, initially
  - Time to Configure
    - Network Hierarchy
    - Network zones and hosts
    - Trusted VA Scanners
    - Internal Monitoring hosts
  - Remote Networks
    - Partner subnets/hosts

# Dashboards

Show Dashboard: **Threat and Security Monitoring** | New Dashboard | Rename Dashboard | Delete Dashboard | Add Item... | Next Refresh: 00:00:35

### Default-IDS / IPS-All: Top Alarm Signatures (Event Count)

Reset Zoom | May 23 04:38 - May 23 10:45

Legend:

- SQL\_SSRP\_Stammer\_Worm
- SensorStatistics\_Cumulative
- SensorStatistics
- HTTP\_Netscape\_Method\_Overflow
- DNS\_Bind\_OPT\_DoS
- Remainder

[View in Log Activity](#)

### Top Systems Attacked (Event Count)

Reset Zoom | May 23 04:38 - May 23 10:45

Legend:

- 10.25.200.182
- 54.252.131.124
- 202.125.108.229
- 202.125.108.227
- 202.125.108.230
- Remainder

[View in Log Activity](#)

### Top Systems Sourcing Attacks (Event Count)

Reset Zoom | May 23 04:38 - May 23 10:45

### My Offenses

No results were returned for this item.

### Most Severe Offenses

Offense Name	Magnitude
Multiple Exploit/Malware Types Targeting a Single Source preceded by Botnet Successful Inbound Connection from a Known Botnet C&DC	[Progress bar]
Exploit/Malware Events Across Multiple Targets containing Nachl_Ping_Sweep	[Progress bar]
ICMP_Unreachable_Storm preceded by DNS_RDATA_String_BO	[Progress bar]
Communication to a known Bot Command and Control preceded by Possible Local Worm Detected preceded by Excessive Firewall Denies Across Multiple Hosts From A Local Host preceded by Local TCP Scanner Detected preceded by Local IM Scanner	[Progress bar]
Generic Computer Account Added	[Progress bar]

### Most Recent Offenses

Offense Name	Magnitude
Communication to a known Bot Command and Control preceded by Local P2P Client Connected to more than 100 Servers preceded by Connection to a remote proxy or anonymization service (Outbound) preceded by Local TCP Scanner Detected preceded by Local UDP Scanner Detected preceded by Local Web Scanner Detected	[Progress bar]
IRC Connections preceded by Communication to a known Bot Command and Control preceded by Connection to a remote proxy or anonymization service (Outbound) preceded by Possible Tunneling preceded by Local UDP Scanner Detected preceded by Local TCP Scanner Detected preceded by Local Web Scanner Detected	[Progress bar]
Local P2P Client Connected to more than 100 Servers preceded by Possible Local Worm Detected preceded by Connection to a remote proxy or anonymization service (Outbound) preceded by Local UDP Scanner Detected preceded by Local TCP Scanner Detected preceded by Policy: Remote Clear Text Application Usage	[Progress bar]
Communication to a known Bot Command and Control preceded by IRC Connections preceded by Connection to a remote proxy or anonymization service (Outbound) preceded by Exploit/Malware Events Across Multiple Targets preceded by Possible Tunneling preceded by Local TCP Scanner Detected preceded by Local Web Scanner Detected	[Progress bar]
Communication to a known Bot Command and Control	[Progress bar]

### Top Services Denied through Firewalls (Event Count)

Reset Zoom | May 23 04:38 - May 23 10:45

### Flow Bias (Total Bytes)

Reset Zoom | May 23 04:38 - May 23 10:45

Legend:

- Mostly Out
- Mostly In
- Near Same
- In Only
- Other
- Out Only

[View in Network Activity](#)

### Top Category Types

Category	Offenses
Potential Botnet Connection	287
Information	242
Firewall Permit	241
Web	191
Unknown	75

### Top Sources

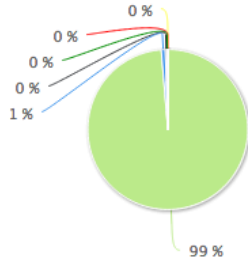
Source	Offenses
[Redacted]	14
[Redacted]	10
[Redacted]	7
[Redacted]	6
[Redacted]	5

### Top Local Destinations

Destination	Offenses
[Redacted]	39
www.wotif.com_vip	12
images.wotif.com_vs	10
www.asiawebdirect.com_vs	10
static.wgcdn.com_vs	10

# Log Activity

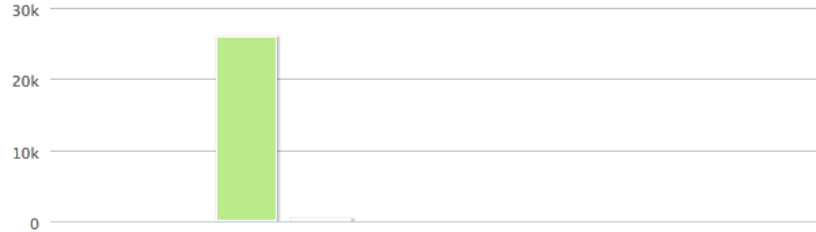
Top 10 appApplicationName (custom) Results By Count



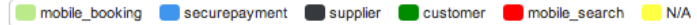
Legend



Top 10 appApplicationName (custom) Results By Count



Legend



(Hide Charts)

appApplicationName (custom)	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Category (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)	Username (Unique Count)
mobile_booking	HTTP 200 - OK	[REDACTED]	68,973	2013-06-10 14:27:51	System Status	Multiple (2)	0	N/A
securepayment	Multiple (3)	[REDACTED]	250	2013-06-11 10:04:03	System Status	Multiple (13)	0	Multiple (3)
supplier	Multiple (3)	[REDACTED]	95	2013-06-11 11:01:07	System Status	Multiple (2)	0	Multiple (6)
customer	Multiple (2)	[REDACTED]	37	2013-06-11 09:44:33	System Status	Multiple (7)	0	Multiple (2)
mobile_search	Multiple (2)	[REDACTED]	21	2013-06-11 00:38:57	System Status	Multiple (2)	0	N/A
N/A	Multiple (2)	[REDACTED]	3	2013-06-11 00:39:25	Multiple (2)	Multiple (3)	0	N/A

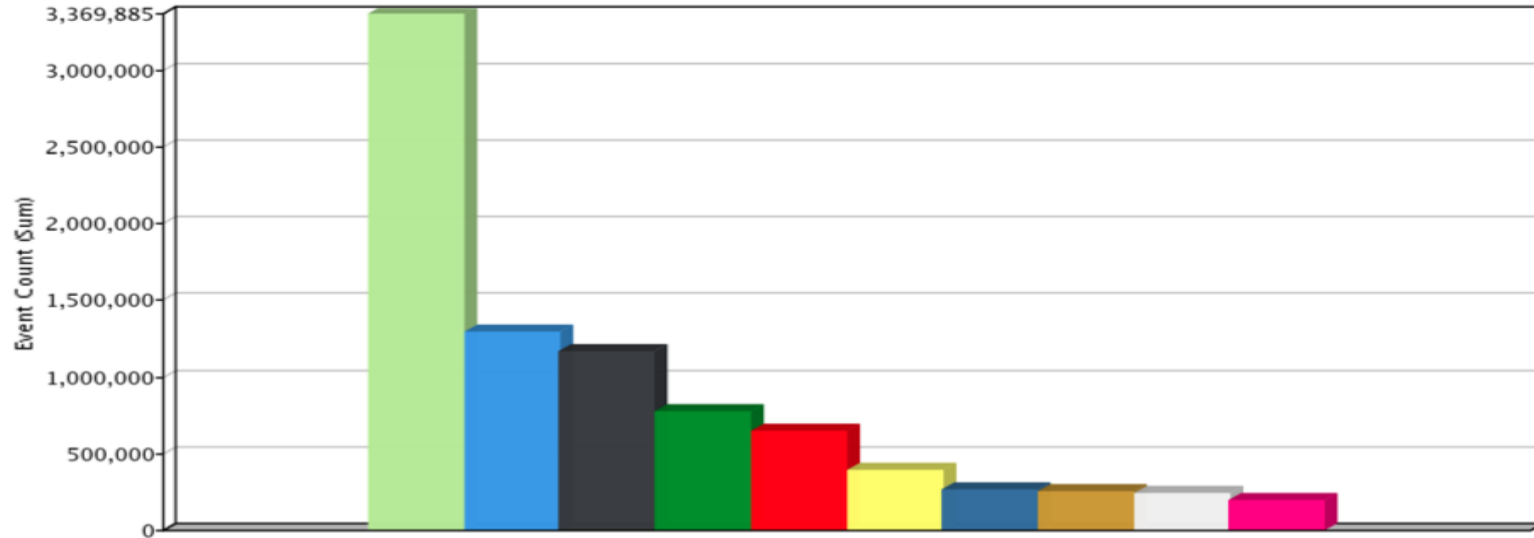
# Reports

## Weekly Firewall Deny Activity

Generated: May 20, 2013 1:00 AM EST



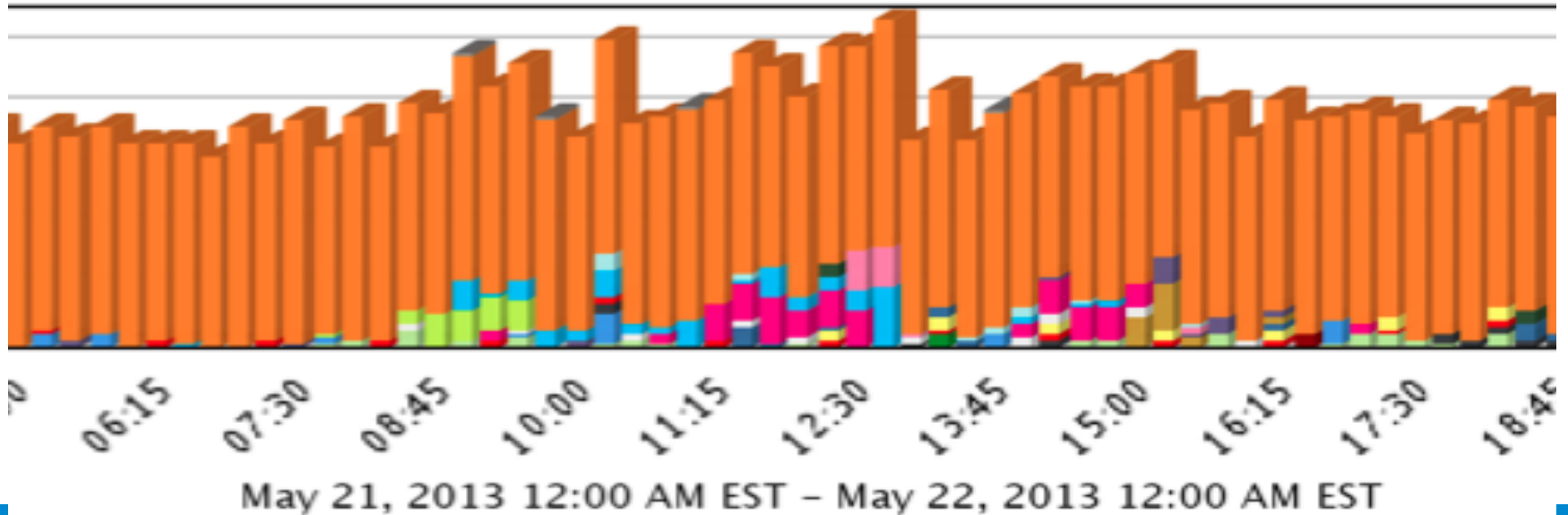
Firewall Deny by Source IP  
Firewall Deny by SRC IP





# Reports

## Authentication Failed by UserName Top Authentication Failures by User



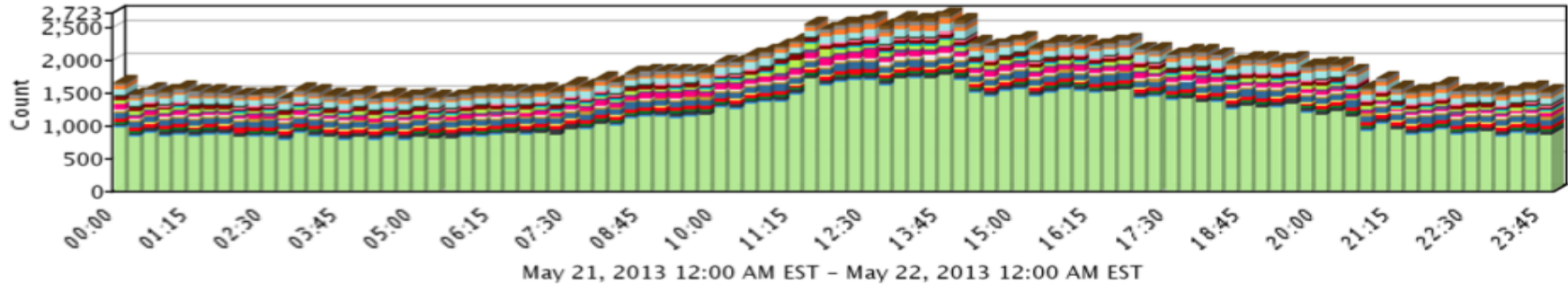
# Reports

## Daily User Authentication Activity

Generated: May 22, 2013 3:39 AM EST

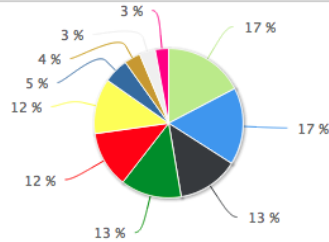


Authentication Successful by UserName  
Top Authentications by User



# Reports – Top Traffic Sources

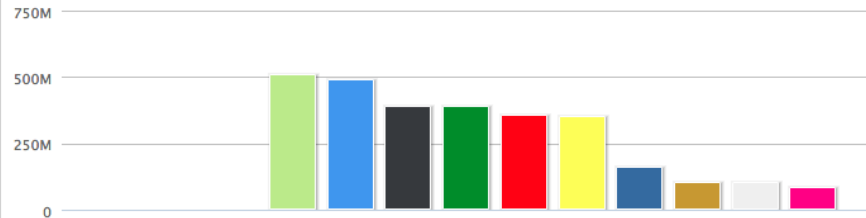
Top 10 Remote Network:Source IP Results By Total Bytes (Sum)



Legend

ChannelMessage StarMinder 132.204.84.48 ChannelMessage StarMinder 9.28.110.15 ChannelMessage StarDedicated 60.84.95.88

Top 10 Remote Network:Source IP Results By Total Bytes (Sum)



Legend

ChannelMessage StarMinder 132.204.84.48 ChannelMessage StarMinder 9.28.110.15 ChannelMessage StarDedicated 60.84.95.88



# Lessons Learned

- You can get quick wins and immediate benefits
- Configuration takes time
  - Network Hierarchy
  - Building Blocks
  - Log Sources
  - Remote Networks
  - Reference Sets
  - Asset Profiles
  - Vulnerability Scans
- Regularly review and tune you configuration to deliver the benefits.

# Lessons Learned 2

- Tuning rules to get the right amount of Offences
  - don't let them pile up, we had thousands per day in the beginning
  - Aim for 5, or <10 per day.
  - What Data Sources do you need, what are you willing to pay for?
  - What black lists do you want to import to assist
  - Developers use IRC (potential Botnet command and control)
- Anomaly Detection
  - basic rules; thresholds; time-series variation based (holt-winters) on a single metric
- Searching
  - Can take longer than you expect, time-series databases are different.
  - Reports need to be tailored

# Lessons Learned 3

- Interpreting results
  - Takes a mix of skills and domain knowledge for your events.
- Reference Sets
  - Very useful for defining sets of data, such as IP addresses.
  - Reference Sets are making it easier to name and defined data and share conditions across different searches
- Name lookups associated with an offence or a host
  - are sampled
- IP and Port pairs represent our internal applications
  - Standard ports, like 80 can't be overridden.
  - Matching that ip and port combination = wotif.com:80 requires two conditions
- Bugs happen

# Future Plans

- GI-Prod Team Training
  - Tending to building blocks and rules
  - Art of triage
- Rolling dashboards out for our dev/test teams
- Feed data out of QRadar for other systems/analysis
  - Improve our Fraud Risk Assessments
  - Try other anomaly detection algorithms
- Integrate more devices
- Better events sent from Applications.
- Auto provisioned assets
  - Dynamic scaling needs to fit in with Network Hierarchies etc.

# Questions?

