SteelCentral NetProfiler Advanced Security Module

Customer Presentation

riverbed
The Digital Performance Company

Agenda

1. Challenges & opportunities
2. SteelCentral solution
3. Why use full-fidelity flow
4. ASM overview
5. Summary

Challenges and Opportunities

Cyber Security Issues

Attacks more sophisticated and varied

91% increase in DDoS attacks

600% increase in IoT attacks[2]

8,500% increase in coinminer detections [3]

186% uptick in use of HTTPS domains for phishing attacks[4]

The average targeted malware compromise was present for 205 days before detection and 69% were discovered by external parties.[5]

[1] TechRepublic, Nov 2017
[2] Gartner, Shift Cybersecurity Investment to Detection and Response
[3,4] Symantec, Internet Security Threat Report2018
[5] Mandiant, Cyber Security in 2018

Cyber security

90% of security experts are not satisfied with the speed and capabilities they have in detecting incidents[1]

[1]RSA, Threat Detection Effectiveness Survey 2016

A Different Approach Required…

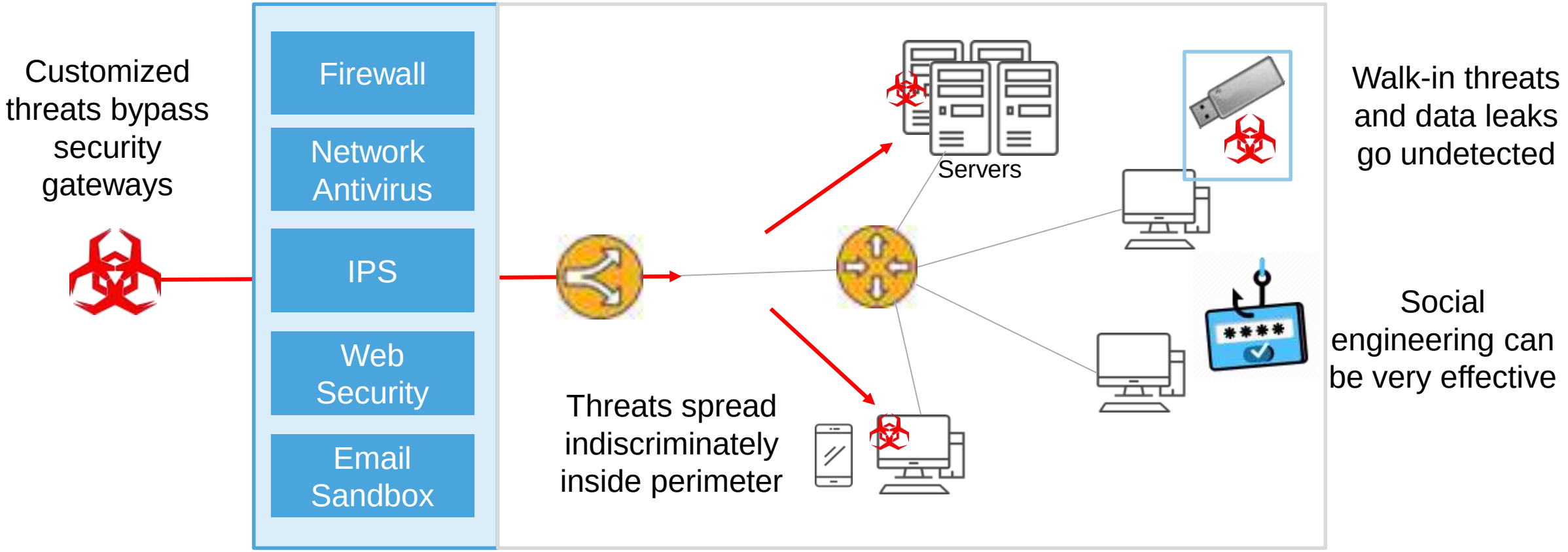
Gartner projects that by 2020

"60% of enterprise information security budgets will be allocated to rapid detection and response approaches — up from less than 20% in 2015."

Gartner, "Shift Cybersecurity Investment to Detection and Response," 3 May 2017

Preventative measures alone are not enough

Hackers are always busy trying to avoid detection



Balanced Approach using Detection & Rapid Response

Stop focusing efforts solely on prevention; balance investments across protection, detection and response.[1]

Prevent

Prevent breaches

Utilize automation and good hygiene to prevent compromises.

Detect

Detect targeted attacks

Utilize a combination of technical, procedural and human capabilities to detect when a compromise occurs.

Investigate

Determine scope of incident and impact on business

Separate normal user behavior from the malicious or compromised behavior.

Respond

Respond quickly to contain scope and impact

Mitigate events to contain the incident. Incorporate learnings into security process.

[1] "Shift Cybersecurity Investment to Detection and Response," Gartner, 3 May 2017

SteelCentral Overview

Digital Experience Management

Cloud Architect

NetOps/SecOps

App Dev/Owner

End User Services

Business & IT Execs

Integrated Digital Experience Management

End Users & Applications

Networks & Infrastructure

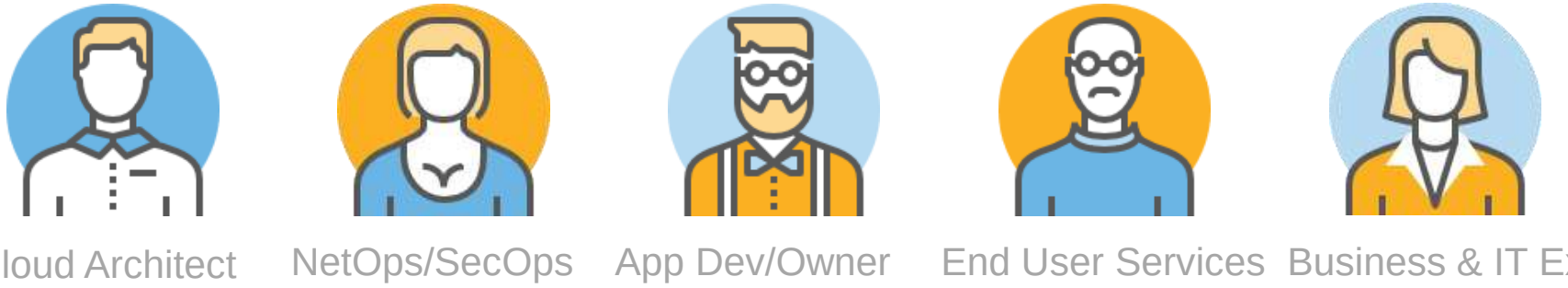
EU Devices

Applications

Networks

Infrastructure

Two core solutions



Cloud Architect | NetOps/SecOps | App Dev/Owner | End User Services | Business & IT Execs

Integrated Digital Experience Management

Broad

Depth of analysis

Deep

Unified APM	NPM & ITIM
Device-based EUEM	Network & security monitoring
Code-based APM / Network-based APM	Network forensics / Infrastructure monitoring

Broad

Depth of analysis

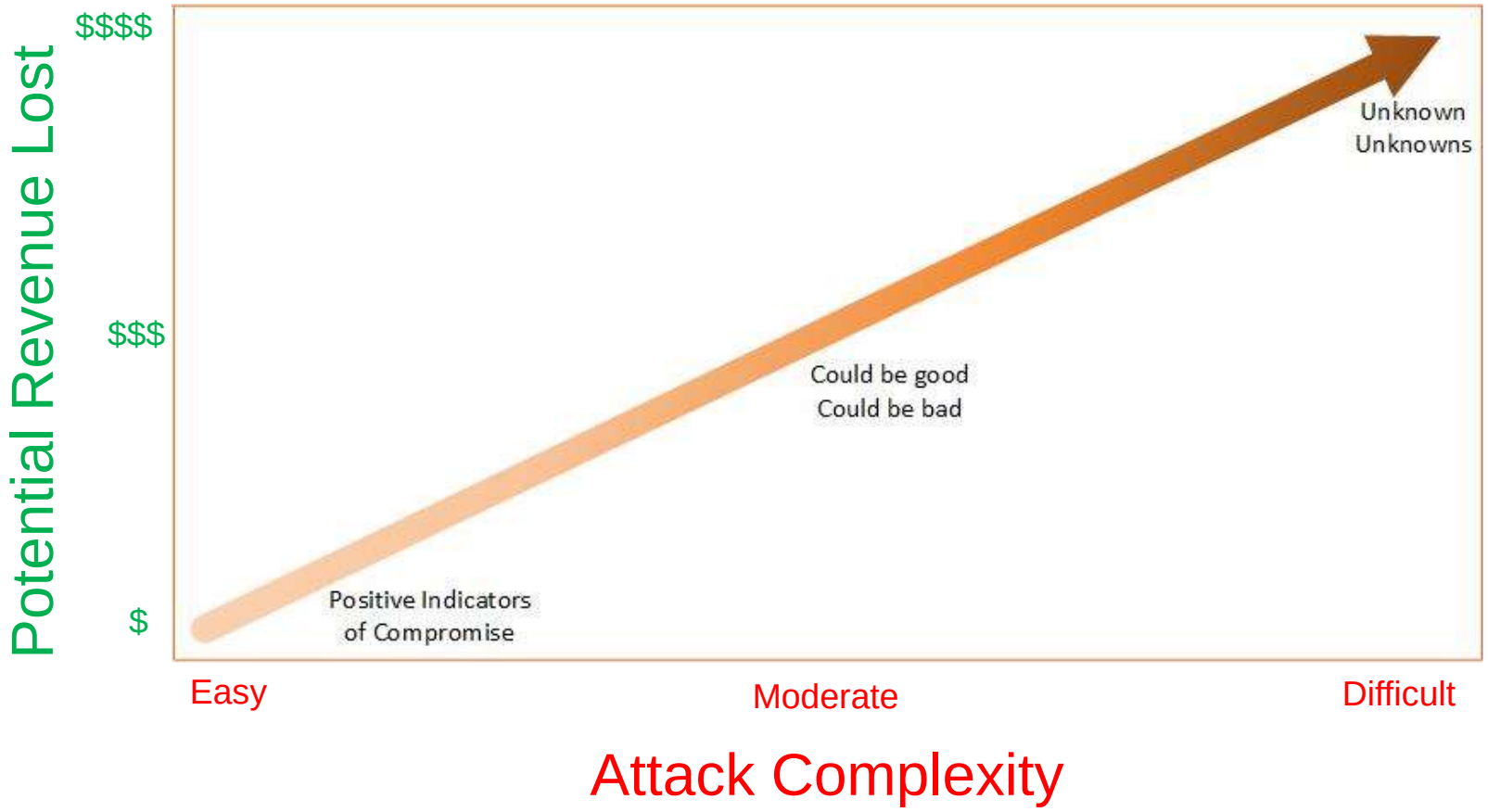
Deep

Advanced Security Module

Spectrum of Security Compromises

Types of attacks that can be discovered by ASM

- Positive Indicators of Compromise
  - Botnet C2
  - Fast DDoS
  - Malware
  - Recon / Brute Force
- Could be good, could be bad
  - NBA behaviors
  - Data movement
  - New services
  - Cryptocoin mining
- Unknown Unknowns
  - Advanced & Persistent attacks
  - Hunt, map & disable
  - Full Forensic Recall



You need full-fidelity Flow

Strike the Right Balance Between Data Fidelity and Retention

- Captures and retains *every flow*
  - Allows you to rapidly search, pivot, and filter down to the traffic of interest
  - Enables quick answers to difficult questions – even if it happened months ago
- Ubiquitous–broad coverage in security data sources
  - Broad visibility; can (SHOULD) be gathered from every network device
  - Cheaper; no special probes required
  - Scalable to store, retrieve, and index
- Supplement with packets for deep forensic analysis
- Hits key compliance checkboxes

Preserves full-fidelity flow data so you see every session in detail.

SteelCentral Advanced Security Module delivers…

THREAT INTEL

- Up-to-date intelligence for proactive and incident-reactive security

DDOS DEFENSE

- Quickly and easily detect & mitigate DDoS attacks

THREAT HUNTING

- Proactively seek out and disable threats that have penetrated your defenses

Why SteelCentral ASM

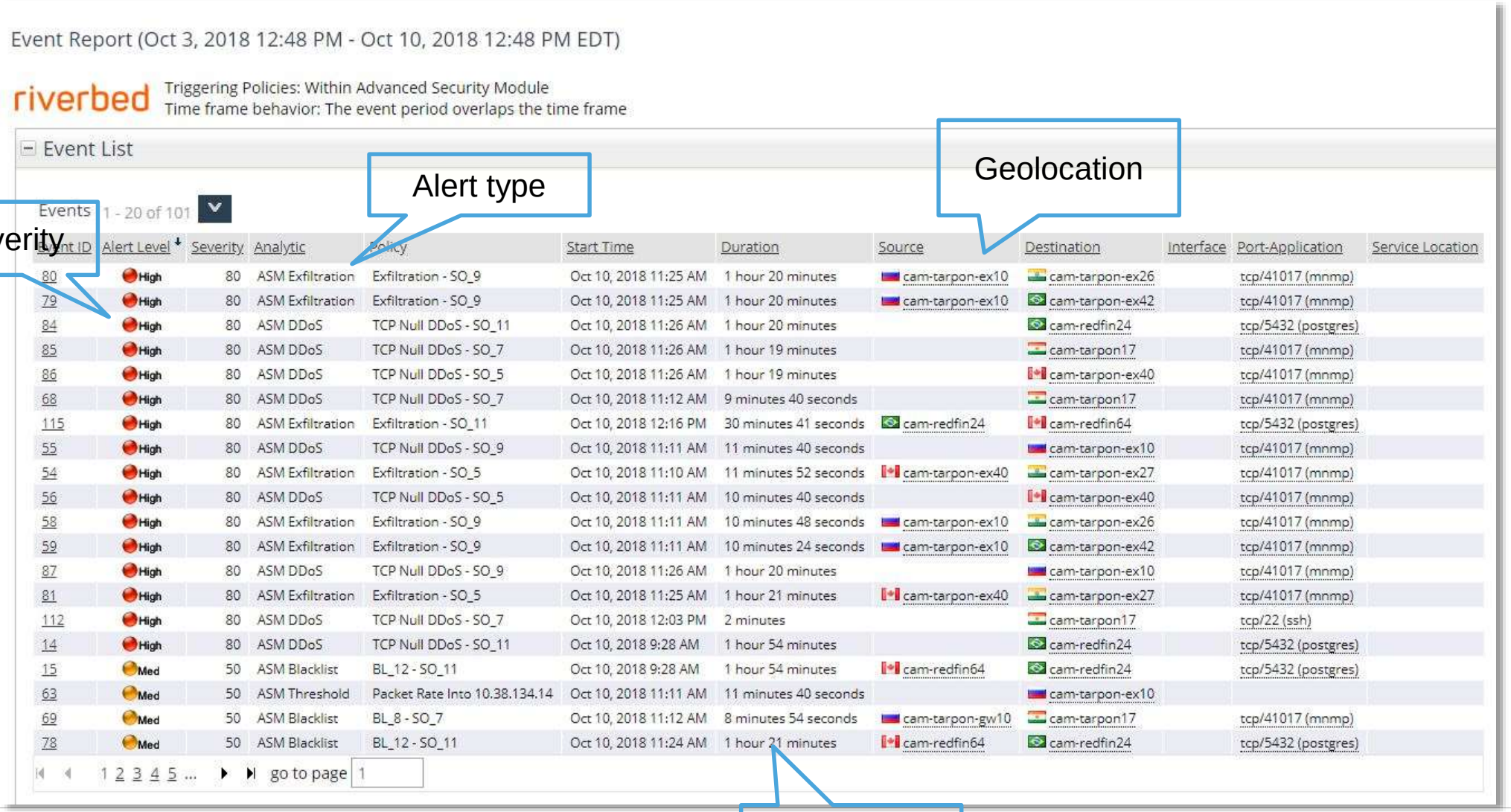
Benefits of security with visibility

Act with speed and confidence

Reduce / avoid financial and customer losses

Mitigate risks, avoid exposure

Event Detection



Event ID	Alert Level	Severity	Analytic	Policy	Start Time	Duration	Source	Destination	Interface	Port-Application	Service Location
80	High	80	ASM Exfiltration	Exfiltration - SO_9	Oct 10, 2018 11:25 AM	1 hour 20 minutes	cam-tarpon-ex10	cam-tarpon-ex26		tcp/41017 (mnmp)	
79	High	80	ASM Exfiltration	Exfiltration - SO_9	Oct 10, 2018 11:25 AM	1 hour 20 minutes	cam-tarpon-ex10	cam-tarpon-ex42		tcp/41017 (mnmp)	
84	High	80	ASM DDoS	TCP Null DDoS - SO_11	Oct 10, 2018 11:26 AM	1 hour 20 minutes		cam-redfin24		tcp/5432 (postgres)	
85	High	80	ASM DDoS	TCP Null DDoS - SO_7	Oct 10, 2018 11:26 AM	1 hour 19 minutes		cam-tarpon17		tcp/41017 (mnmp)	
86	High	80	ASM DDoS	TCP Null DDoS - SO_5	Oct 10, 2018 11:26 AM	1 hour 19 minutes		cam-tarpon-ex40		tcp/41017 (mnmp)	
68	High	80	ASM DDoS	TCP Null DDoS - SO_7	Oct 10, 2018 11:12 AM	9 minutes 40 seconds		cam-tarpon17		tcp/41017 (mnmp)	
115	High	80	ASM Exfiltration	Exfiltration - SO_11	Oct 10, 2018 12:16 PM	30 minutes 41 seconds	cam-redfin24	cam-redfin64		tcp/5432 (postgres)	
55	High	80	ASM DDoS	TCP Null DDoS - SO_9	Oct 10, 2018 11:11 AM	11 minutes 40 seconds		cam-tarpon-ex10		tcp/41017 (mnmp)	
54	High	80	ASM Exfiltration	Exfiltration - SO_5	Oct 10, 2018 11:10 AM	11 minutes 52 seconds	cam-tarpon-ex40	cam-tarpon-ex27		tcp/41017 (mnmp)	
56	High	80	ASM DDoS	TCP Null DDoS - SO_5	Oct 10, 2018 11:11 AM	10 minutes 40 seconds		cam-tarpon-ex40		tcp/41017 (mnmp)	
58	High	80	ASM Exfiltration	Exfiltration - SO_9	Oct 10, 2018 11:11 AM	10 minutes 48 seconds	cam-tarpon-ex10	cam-tarpon-ex26		tcp/41017 (mnmp)	
59	High	80	ASM Exfiltration	Exfiltration - SO_9	Oct 10, 2018 11:11 AM	10 minutes 24 seconds	cam-tarpon-ex10	cam-tarpon-ex42		tcp/41017 (mnmp)	
87	High	80	ASM DDoS	TCP Null DDoS - SO_9	Oct 10, 2018 11:26 AM	1 hour 20 minutes		cam-tarpon-ex10		tcp/41017 (mnmp)	
81	High	80	ASM Exfiltration	Exfiltration - SO_5	Oct 10, 2018 11:25 AM	1 hour 21 minutes	cam-tarpon-ex40	cam-tarpon-ex27		tcp/41017 (mnmp)	
112	High	80	ASM DDoS	TCP Null DDoS - SO_7	Oct 10, 2018 12:03 PM	2 minutes		cam-tarpon17		tcp/22 (ssh)	
14	High	80	ASM DDoS	TCP Null DDoS - SO_11	Oct 10, 2018 9:28 AM	1 hour 54 minutes		cam-redfin24		tcp/5432 (postgres)	
15	Med	50	ASM Blacklist	BL_12 - SO_11	Oct 10, 2018 9:28 AM	1 hour 54 minutes	cam-redfin64	cam-redfin24		tcp/5432 (postgres)	
63	Med	50	ASM Threshold	Packet Rate Into 10.38.134.14	Oct 10, 2018 11:11 AM	11 minutes 40 seconds		cam-tarpon-ex10			
69	Med	50	ASM Blacklist	BL_8 - SO_7	Oct 10, 2018 11:12 AM	8 minutes 54 seconds	cam-tarpon-gw10	cam-tarpon17		tcp/41017 (mnmp)	
78	Med	50	ASM Blacklist	BL_12 - SO_11	Oct 10, 2018 11:24 AM	1 hour 21 minutes	cam-redfin64	cam-redfin24		tcp/5432 (postgres)	

1 2 3 4 5 ... go to page 1

Threat Intelligence

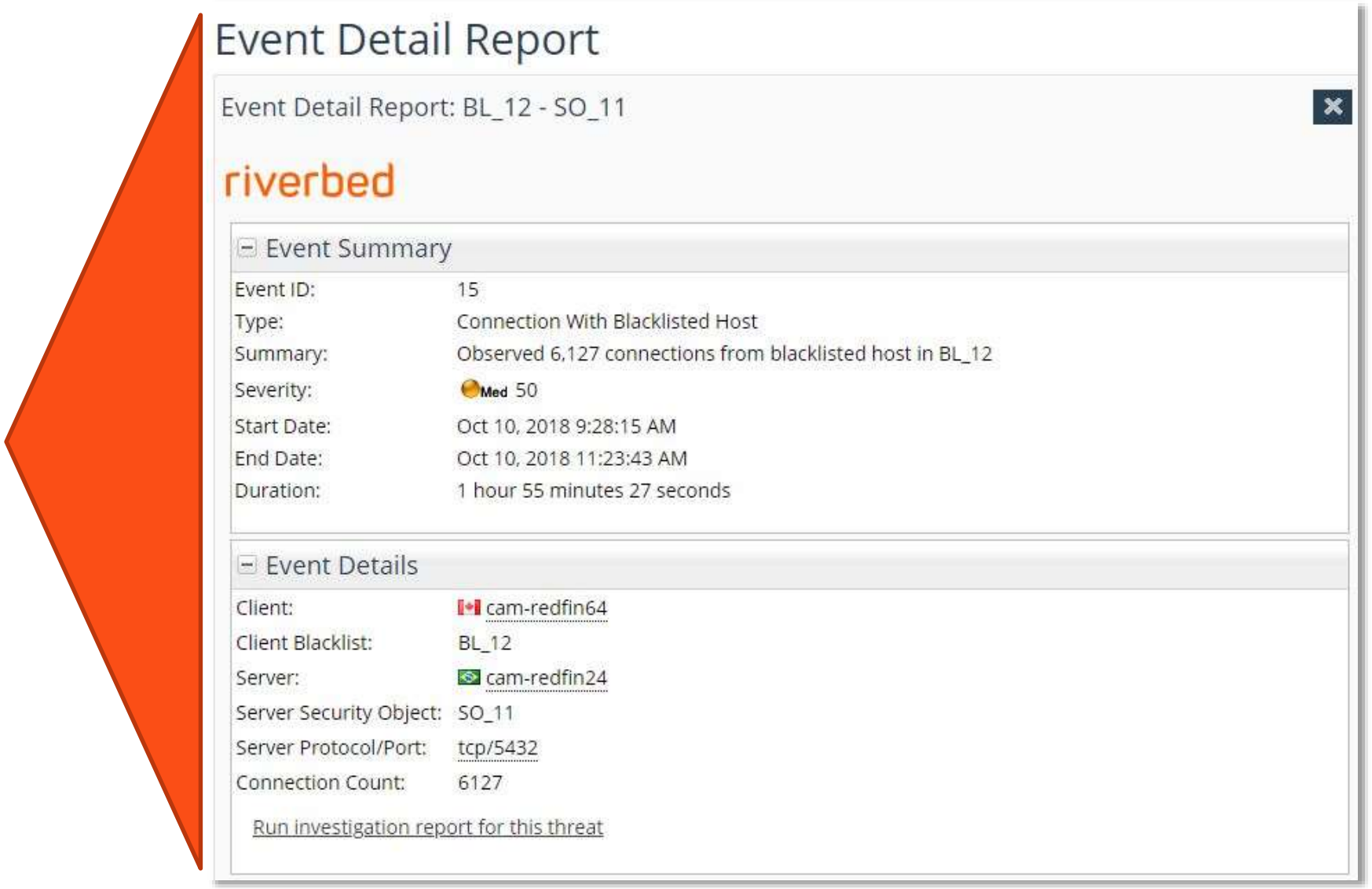
Pro-active as well as incident-reactive security feeds

- Automatically alerts on communication with known-bad addresses
  - Increases chances of detection for sophisticated malware and advanced persistent threats
  - Reduces time to detect botnet compromised machines and other threats

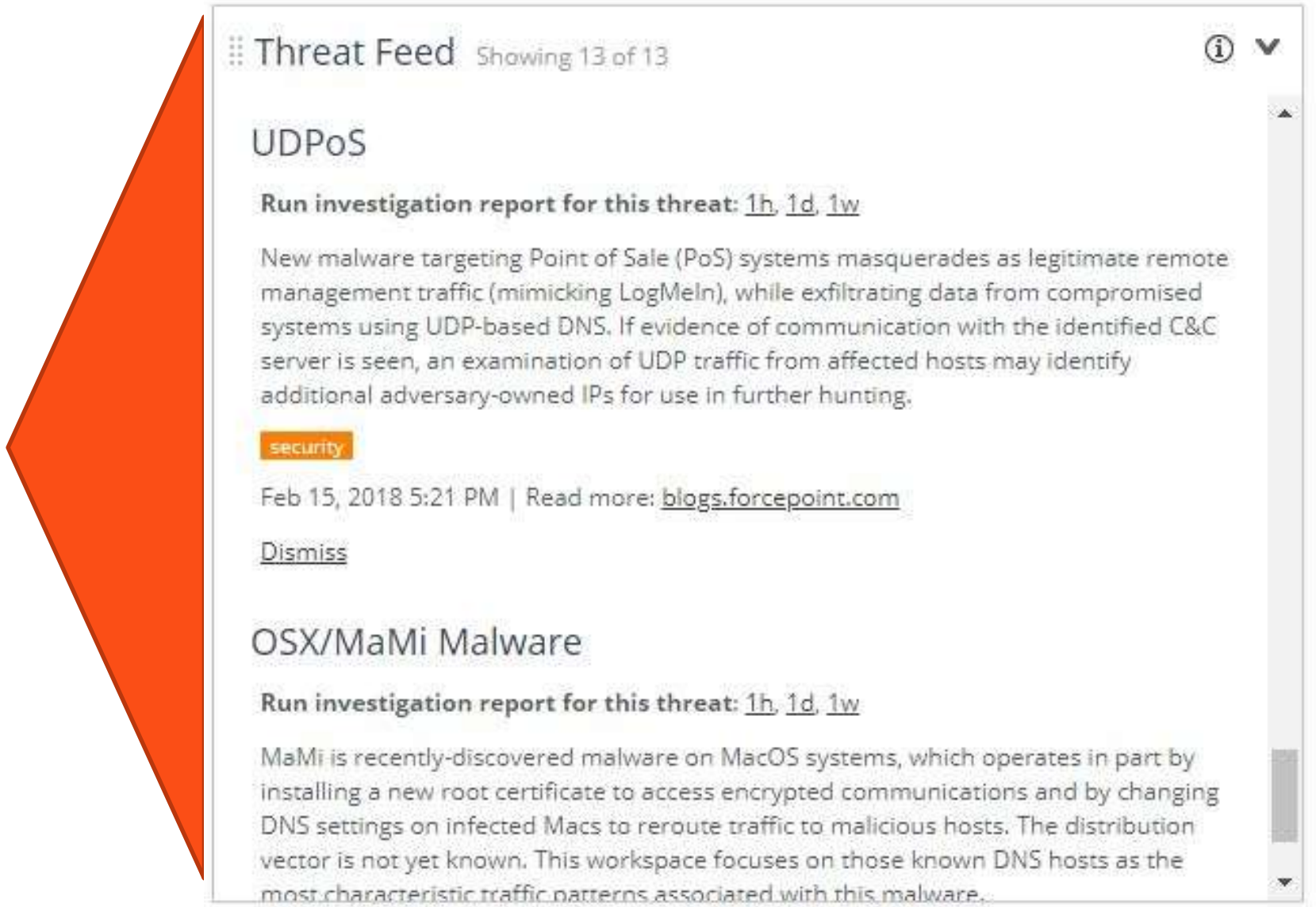
- Potential security-relevant events
  - Stay up to date with security-relevant news
  - Links to evaluate network
  - Additional readings (external)

- Automatically updated as new threats emerge

Blacklist example: Connections from blacklisted host



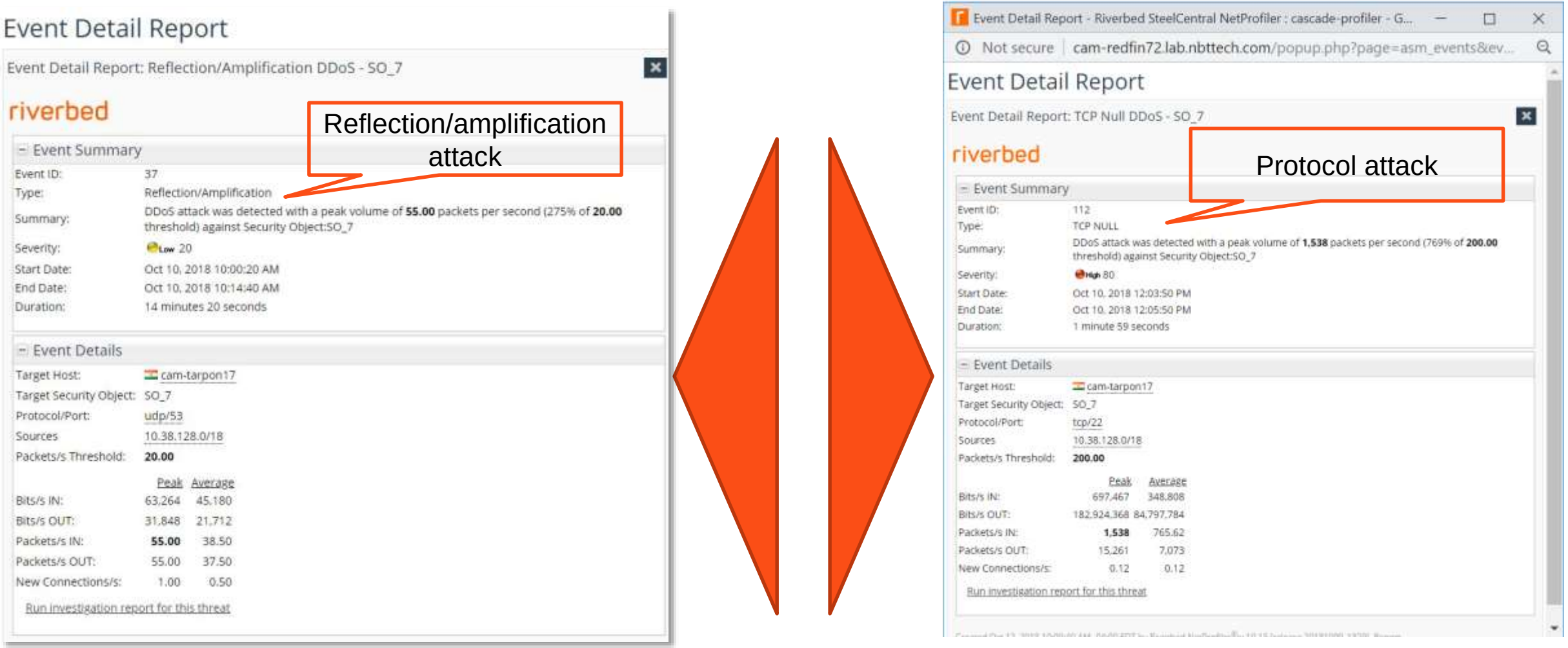
Threat Feed example: UDPoS



DDoS Detection & Mitigation

- Enables operators to detect and manage all types of DDoS attacks
  - Detect volumetric, protocol, application, amplification/reflection and multi-vector attacks
  - DDoS no longer needs to be a dedicated solution; Fewer vendors in the NSOC
- Reduces the impact of DDoS attacks on the organization
  - Fast detection –15 to 30 seconds – minimal interruption
  - Granular detection enables operator to make informed decisions
- Resolve through Mitigation
  - On-premise / data center scrubbers
  - Cloud scrubbers
  - Firewall/router ACLs

DDoS attack detection



Cyber Threat Hunting

No Evidence of Compromise ≠ Evidence of No Compromise

- Threat hunting is the art of proactively seeking out, tracking, and disabling persistent threats that have gained and retained access to the network
  - The average targeted malware compromise is present for ~205 days before detection[1]
- Full-fidelity threat hunting
  - Detect anomalies and suspicious behavior
  - Provide full forensic records to investigation post-compromise
  - Quickly assess scope of security incidents to reduce impact of negative publicity
  - (Pro)active threat hunting to reduce or avoid data theft or business interruption

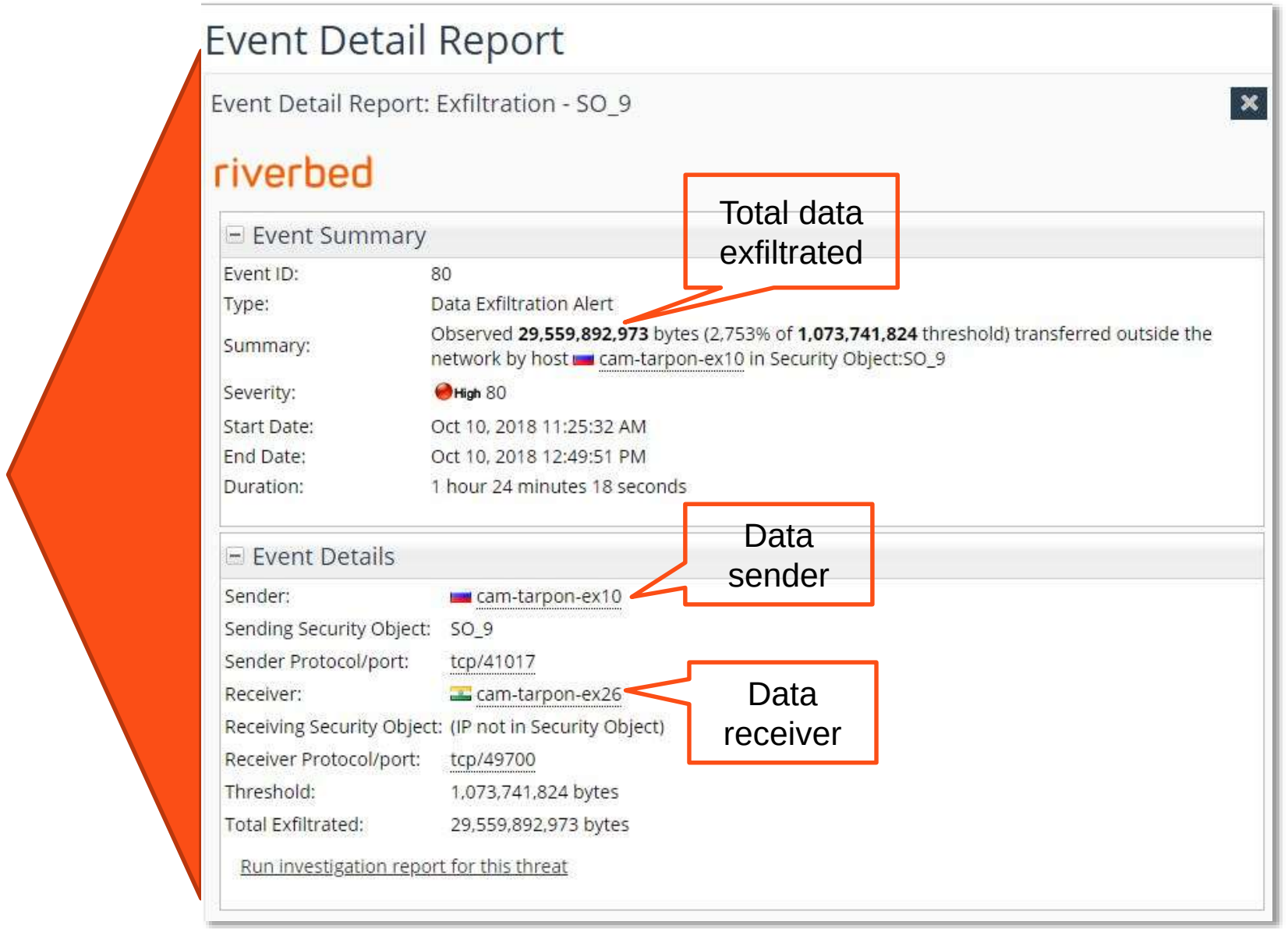
[1] Mandiant, Cyber Security in 2018

Behavior Anomaly Detection

Identify threats before sabotage or espionage impacts business

Behavior	What it is	How it is detected
Brute forcing	Attackers frequently try thousands of different username/password combinations to gain access to a host or a service	The compromised system initiates many connections to the same service on one or more hosts
Exfiltration	Data theft is a common objective used by hackers	The compromised system moves large volumes of data to an external destination
Scan/Recon	A common technique to find vulnerable hosts and services in the network	The compromised system initiates connections to many unique endpoints (server:port combinations)
New Service	Once a system is compromised, attackers frequently leave “back-doors” through which they can re-enter	Once the attacker reconnects to the back-door on a previously compromised system, the new service is spotted
New Client	Attackers frequently gain access through stolen credentials, and connect to services from unusual locations	A never before seen IP address connects to a known service end point

Data exfiltration

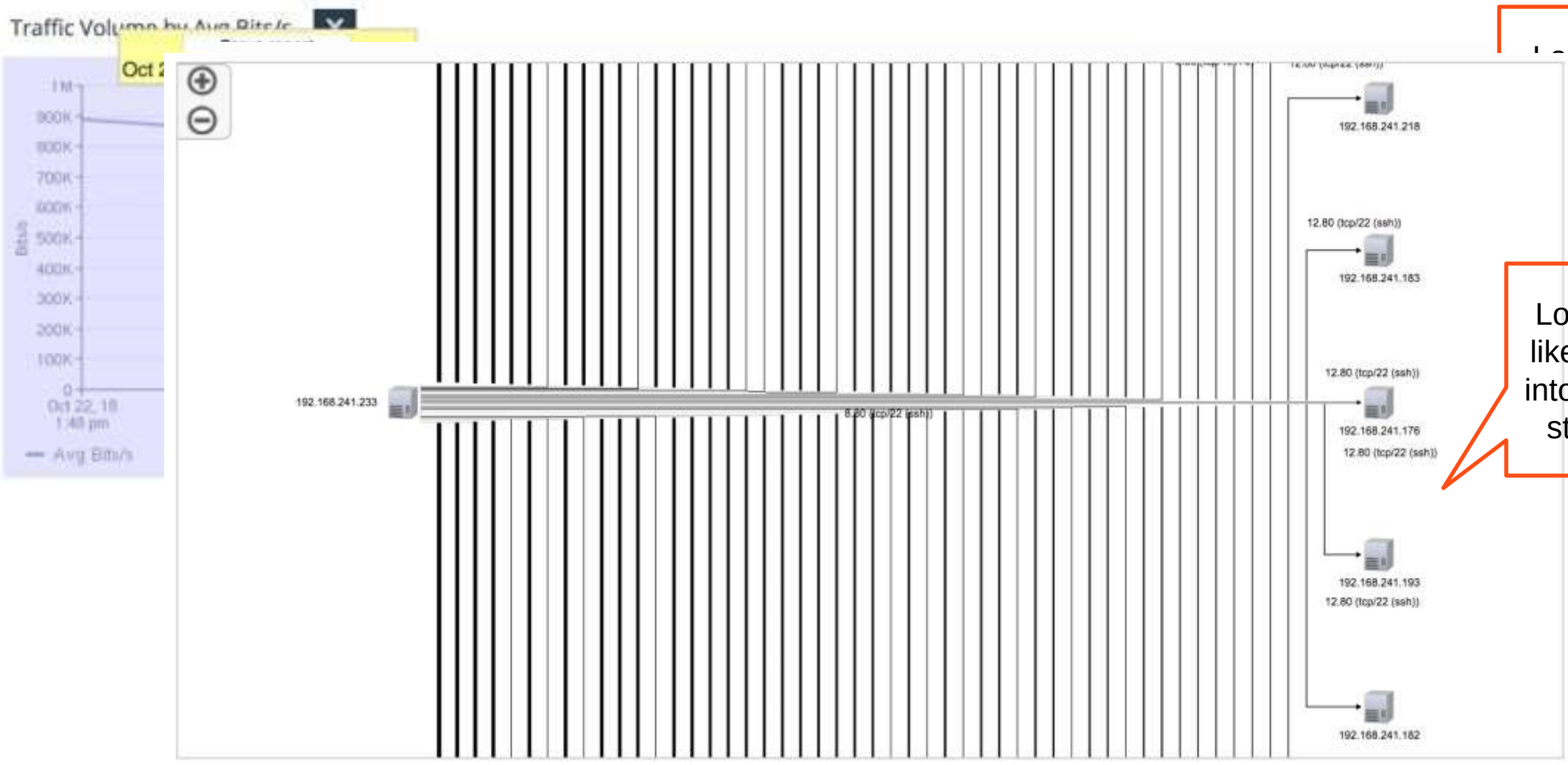


Pivoting and Drilldown

Hunting for threats already on your network

- “Pivoting” is a technique used by operators to continually change the focal point of an investigation
- Powerful techniques to drill down on only the traffic that matters
- Using network traffic to map out the full extent of the hacker in your network

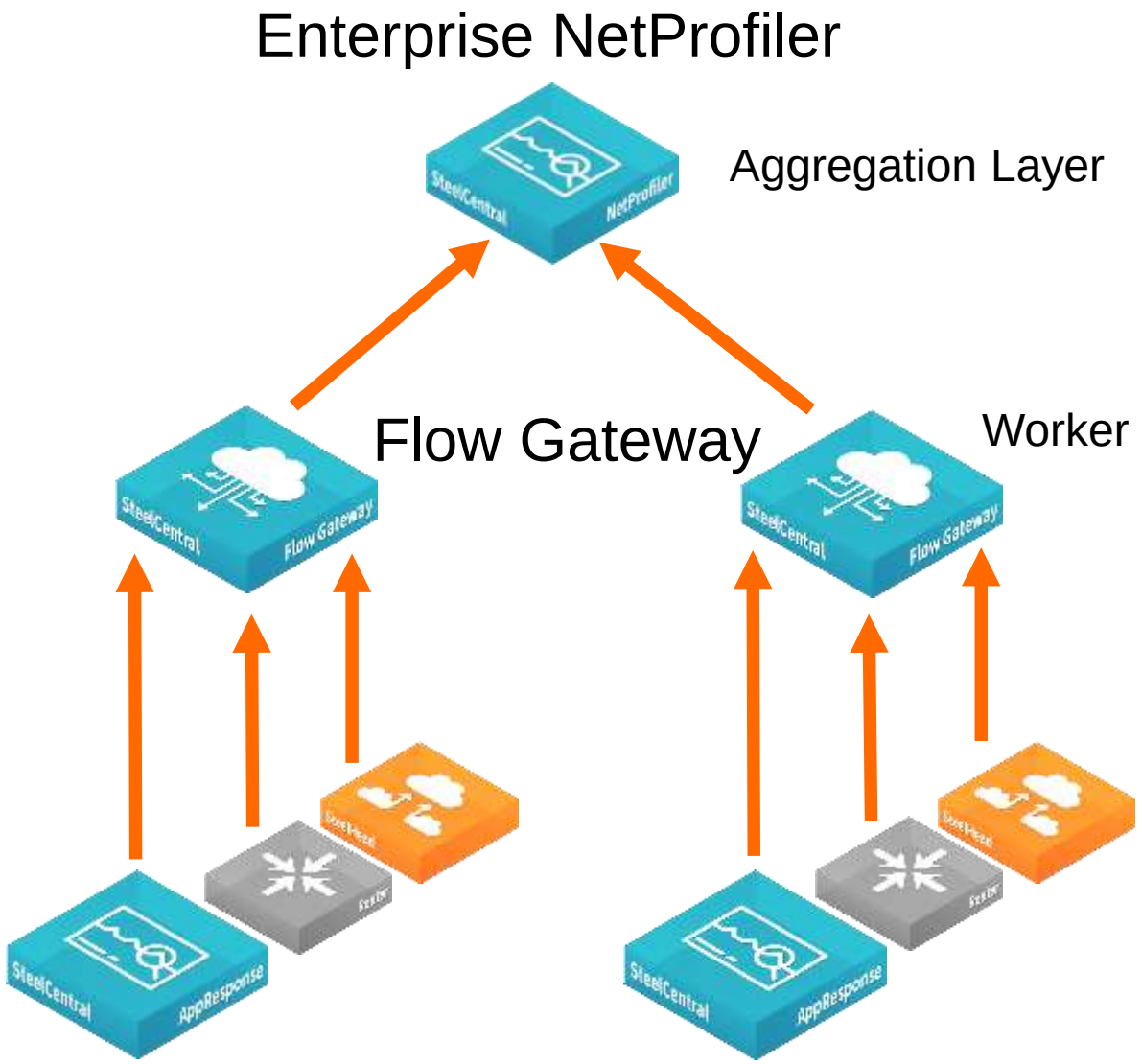
Threat hunting workflow



Deployment Overview

Deployment Overview

- ASM is an optional software module for SteelCentral Enterprise NetProfiler
- ASM has two high-level components
  - "Worker" runs on Flow Gateways
    - Enables near real-time security analysis on flow-based detection
    - Performs most of the heavy analysis
    - AppResponse / NetShark must be directed to Flow Gateway for security analysis to occur on those flows
  - "Aggregation Layer" runs on DB module of Enterprise NetProfiler
    - Talks to each Worker to aggregate individual analysis for end-to-end view
    - Organizes and presents data and workflows



Summary

Network and security monitoring in one solution for today's consolidating NetOps/SecOps tools budget

Finds the advanced persistent threats that perimeter tools miss

Builds on existing SteelCentral NetProfiler flow monitoring investment

Thank You

Splunk, Log Data and overcoming objections

Binoculars vs Radar

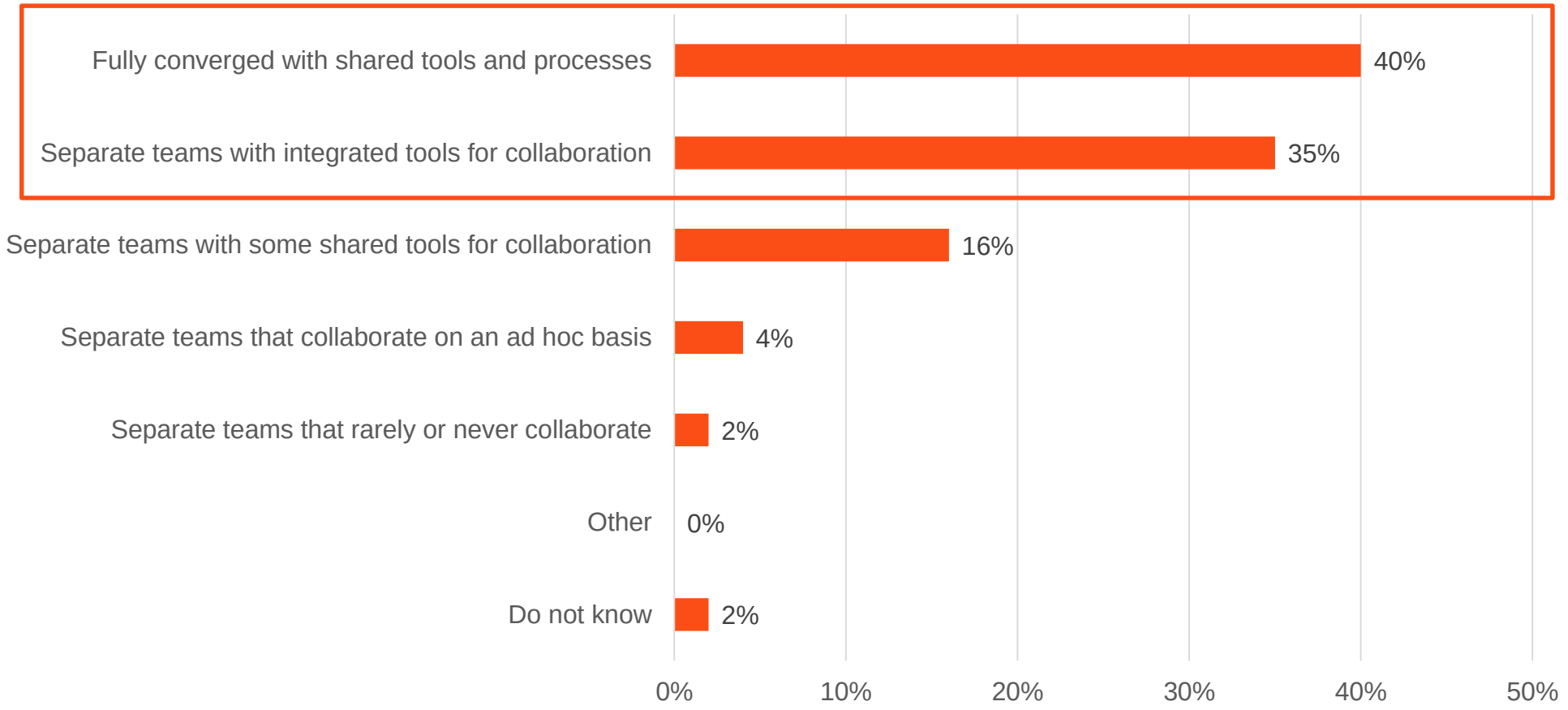
- Log data is self-reported
  - If the system is compromised, it's not necessarily going to tell you
  - A good hacker will immediately shut off logs
  - Sometimes log data will fail
- You need multiple points of telemetry
  - Logs, flow, packets provide full story
  - Situational awareness

Threat Intel identified threats

Know about attacks sooner

Behavior	What it is
Malware Command and Control	C2 servers for known control of malware; if a system in your network communicates with a known botnet C2 server, it is probable the system is under hacker control.
Credential Drop Sites	Locations where stolen credentials get dropped; if communication with a known drop-site is detected, it is likely an attacker is uploading stolen credentials from your network to a server controlled by them.
Spyware Reporting Sites	Locations where spyware sends espionage data; it is likely that the sending system has been infected by spyware and needs scrubbing or re-imaging.
Scanners	Repeat visits from the same scanner should raise suspicion: hunt for similar patterns from unknown addresses, and keep close watch on the data gathering the adversary is engaging in.
Brute Forcers	Brute forcers are systems that try many username/password combinations for services such as SSH, Telnet, and RDP to gain remote access to systems or infrastructure. They typically try thousands of common default passwords to gain access.
Fake Anti-Virus	Communication with fake anti-virus hosts should be taken seriously, as users are frequently tricked into installing malware that masquerades as virus protection software.
Sinkhole DNS	Sinkhole or blackhole DNS server serves incorrect IP addresses for certain name queries, allowing the attacker to subvert traffic. This is subverts websites and tricks users into give up credentials to the actual site.
Malware Download Locations	Servers known to host malware for download: if you observe communication with a known malware download location, the host is actively being infected with spyware or a rootkit.

NetOps & SecOps teams and tools are converging



EMA, Network Management Megatrends, 2018