SteelCentral NetProfiler Advanced Security Module

Cybersecurity attacks are becoming more sophisticated, more varied, and more frequent. In 2017, there was a 91% increase in DDoS attacks[1]; an 8,500% increase in cryptocurrency detections[2]; and a 600% growth in attacks launched from IOT-based devices[3]. Because of this uptick in activity, the average targeted malware compromise was present for 205 days before detection and then external parties, such as the FBI, discovered the issue 69% of the time[4].

Given the amount of time threats are present in networks, it's not surprising that 90% of security experts are not satisfied with the speed and capabilities they have in detecting incidents.[5] Clearly, a different approach is required – one that detects threats already in the network.

Unprecedented visibility

SteelCentral NetProfiler Advanced Security Module transforms network data into cyber intelligence, providing essential visibility and forensics for broad threat detection, investigation, and mitigation in today's hyper-connected digital world.

Using full-fidelity network flow analysis, which captures and stores all the data you need for forensic analysis, SteelCentral NetProfiler delivers the crucial insights and empirical evidence you need to detect and investigate threats that bypass typical prevention measures as well as those that originate inside the network.

The value of flow data is well recognized for network use cases, but less so for security. SteelCentral NetProfiler Advanced Security Module offers a wide range of detection capabilities, including:

- Data exfiltration – detects when large volumes of data are staged or move out of your network unexpectedly
- DDoS detection – quickly identifies a wide range of DDoS attacks and automatically triggers mitigations or black hole routes
- Blacklisted communications – alerts you when your system communicates with known malware, viruses, spyware, etc., so you can investigate and take action
- Security analytics – examines network traffic to identify threats that generate unusual traffic flows, such as unexpected new services, hosts, or

connections

- Incident forensics – provides full historical details so you get the complete scope of the attack; drill into the packets for even more details

Threat intelligence for situational awareness

Cyber threat intelligence is evidence-based information that identifies emerging threats and helps you mitigate your organization's exposure to them. SteelCentral NetProfiler Advanced Security Module shows you where threats may exist in your environment so you can swiftly act on them. It provides two types of threat intelligence, which are updated regularly:

- **Blacklists** detail known malicious or suspicious entities that should not be allowed access to your network. The NetProfiler Advanced Security Module correlates blacklisted items to your environment and alerts on positive matches so you can stop the communication. Event detail is available for further research on the threat. At any time, you can add new threats to your blacklist as you run across them in your security landscape.

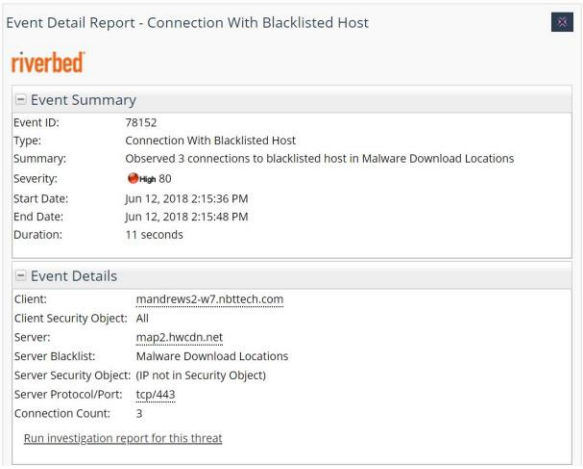

Figure 1. An example of an event detail report showing a connection to a blacklisted host with supporting info and links to investigative reports for the threat.

- **Threat feeds** are analyst-generated information about potential threats that may or may not mean your network has been compromised. Threat feeds can include topics like Shodan activity and cryptocurrency mining that could be legitimate traffic, but might also hide malicious activity. The alert provides you with resources to learn more and the links to investigate the potential vulnerability in your environment.

Figure 2. An example of a threat feed. You can read more about it, or explore your environment for signs of Electroneum on ports 3333, 5555, or 7777 in the past 1 hour, 1 day, or 1 week.

DDoS detection and mitigation

DDoS detection no longer needs to be a dedicated solution, so you need fewer vendors in the NOC/SOC. NetProfiler Advanced Security Module accurately identifies all types of DDoS attacks fast – in just 10 to 30 seconds – and acts immediately and surgically. Redirect traffic to an A10 TPS DDoS scrubber or Verisign cloud-scrubbing center so DDoS traffic is dropped while the rest of your network continues to operate normally.

Security Analytics

Worried that threats are slipping through the cracks? SteelCentral NetProfiler Advanced Security Module learns and understands the changing patterns of behavior in your network to combat both insider and external threats. It provides dynamic visibility into

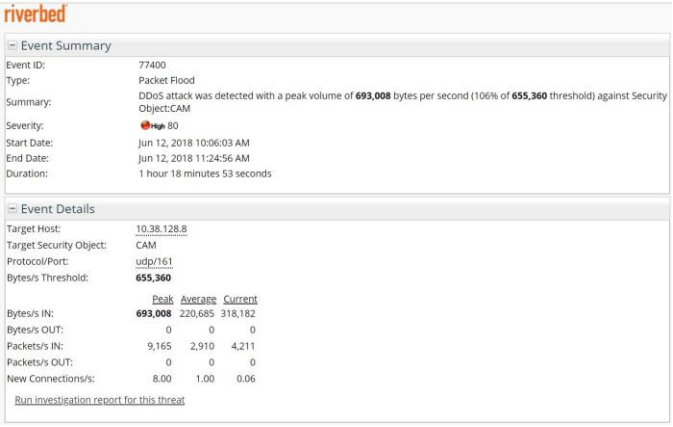

Figure 3. An example of a DDoS alert.

the applications and traffic flowing throughout your network.

Out of the box, the security analytics classifies threats into these broad categories:

- Suspicious connection – when two hosts that do not normally communicate with one another start communicating (for example, a maintenance department host connecting to a finance department host)
- Worm – a pattern of scanning among hosts, where systems previously scanned suddenly become scanners themselves. Identification of patient zero, infected hosts and means of propagation are reported
- New host – a host that has not been previously identified has sent enough traffic to be regarded as having joined the network
- New service – a host or an automatic host group is providing or using a service over a new port
- Host scan – a series of hosts on the monitored network being interrogated on the same port
- Port scan – a host or series of hosts on the monitored network being interrogated across a range of ports
- Bandwidth surge – a significant increase in traffic that conforms to the characteristics of a Denial of Service (DoS) or a Distributed Denial of Service (DDoS) attack

Threat hunting

Cyber threat hunting starts with the premise that bad actors have already breached your perimeter defenses and are operating inside your network. An analyst starts with a hypothesis about how an attacker might have breached your defenses, and then proactively and iteratively tries to find the evidence to support the hypothesis – the systems compromised, and the data accessed, etc. Along the way, the results of the investigation typically cause the analyst to pivot in other more fruitful directions.

Full fidelity flow data is critical for detecting and disrupting active attack activities. It provides both the breadth and depth of visibility you need to gain insight across the entire enterprise – the insight needed for cyber threat hunting. One-click access to packet data also supplements your flow data.

In addition, the Advanced Security Module provides rich security analytics and threat hunting workflows that improve your ability to uncover hidden and entrenched threats. They let you search the network for evidence and footholds and then pivot on promising leads to ultimately determine how the intruder is controlling compromised assets.

Professional Services

Your purchase of the SteelCentral NetProfiler Advanced Security Module includes configuration and deployment professional services that will be delivered by Riverbed Professional Services (RPS). These professional services are designed to help ensure that the initial configuration of the SteelCentral NetProfiler Advanced Security Module is based on Riverbed's best practices

and will deliver the security insights and business value described in this brochure. These services will include a review of your network architecture, desired security policy, and requirements. RPS will perform the applicable data analysis and configuration of your SteelCentral NetProfiler Advanced Security Module remotely in conjunction with your designated subject matter experts. RPS will help ensure you get maximum value out of your SteelCentral NetProfiler Advanced Security Module purchase through expert configuration based on best practice compliance.

Value delivered

The SteelCentral NetProfiler Advanced Security Module provides full visibility into the activities of threat actors with real-time and forensic capabilities to ensure even the most evasive attacker has no place to hide.

- **Proactive incident detection and response.** Analyze data from a range of sources across the enterprise, connecting the dots between various events to detect threats or security incidents in real time.
- **Reduce incident losses.** By detecting advanced persistent threats earlier, you can potentially limit the damage and the costs due to potential regulatory fines, bad publicity and the resulting loss of customers that inevitably comes along with a major breach.
- **Improve security forensics.** Provides insights into where an attack originated from, how a compromise happened, what resources were compromised, what data was lost, along with a timeline for the incident.
- **Reduce attack surfaces.** By supplementing your security defense posture with learned lessons, you shore up weaknesses and architectural shortcomings to ensure that similar incidents do not happen in the future.

To learn more about SteelCentral NetProfiler Advanced Security Module, click here.

[1] TechRepublic, Nov 2017
[2] Symantec, Internet Security Threat Report, 2018
[3] Gartner, Shift Cybersecurity Investment to Detection and Response, 2017
[4] Mandiant, Cyber Security in 2018
[5] RSA, Threat Detection Effectiveness Survey 2016

About Riverbed

Riverbed®, The Digital Performance Company™, enables organizations to maximize digital performance across every aspect of their business, allowing customers to rethink possible. Riverbed's unified and integrated Digital Performance Platform™ brings together a powerful combination of Digital Experience, Cloud Networking and Cloud Edge solutions that provides a modern IT architecture for the digital enterprise, delivering new levels of operational agility and dramatically accelerating business performance and outcomes. At more than $1 billion in annual revenue, Riverbed's 30,000+ customers include 98% of the *Fortune* 100 and 100% of the *Forbes* Global 100. Learn more at riverbed.com.