September 2016
Commissioned by Recorded Future

Recorded Future for SOC Teams Lab Test

Real-Time Threat Intelligence Security and Productivity Evaluation

Executive Summary

› **One SOC analyst experienced a 10x gain in productivity after Recorded Future real-time threat intelligence was integrated with a SIEM in this lab test.**

› Effective monitoring of firewall logs enables organizations to detect relevant threats that could otherwise be missed. However, creating actionable security events from these high-volume/low-context log sources is a time-consuming challenge, especially when firewalls usually account for 50% or more of daily log volume.

› To address the above challenge, we conducted a lab test, to enrich firewall events in a SIEM with Recorded Future's real-time threat intelligence. Matching what one analyst was able to do ***with*** the Recorded Future enriched report would require ten analysts working on the same report ***without*** Recorded Future — a 10x gain in analyst productivity:

  » ***Without*** Recorded Future, one SOC analyst (in a controlled environment) required over ten hours to review one hour of firewall logs. To keep up with the constant flow of incoming logs required ten analysts — not practical for any organization.

  » ***With*** Recorded Future real-time threat intelligence, one SOC analyst (in a controlled environment) reviewed the same one hour of firewall logs in four minutes (versus ten hours previously), which translates to the 10x gain in analyst productivity. Additionally, in this lab test, a Dridex C2 IP was identified as the highest-rated risk in the report.

› To make the test more realistic we also enriched the same report with over 40 free OSINT feeds but ended up with very few matches (less than 2%) and no meaningful context, which did not significantly change our findings with Recorded Future.

› Integrating Recorded Future into an organization's detection framework enables that organization, no matter how large, to effectively and efficiently monitor high-volume/low-context data sources.

The Challenge

There's always a clue, always a thread that wasn't pulled. A connection to an IP on an unusual port, the one time that noisy signature actually mattered, the cluster of enumeration commands executed on a server …

Codis Technologies has supported countless forensic investigations; while each investigation is unique we cannot think of one where we did not have that "if-only" moment. Usually the reason a compromise was not identified on day zero will fall under one of these categories:

› Gaps in logging and/or detection logic

› High-volume/low-context log events were not effectively monitored

› Low-fidelity event was prematurely dismissed

› A security event was prioritized too low and not analyzed

While each of these categories presents its own set of challenges, for this report we would like to focus on the challenge of monitoring of high-volume/low-context log sources.

Most organizations will utilize high-volume/low-context data sources, such as firewall logs, during a forensic investigation. However, security events generated from these log sources are usually rated as low-priority events in a SIEM, and for good reason. These types of log sources have a poor effort-reward ratio and produce too many events for a typical security operations center to triage in a timely manner. Research performed by Codis Technologies has found the following in regard to the monitoring of firewall logs:

› During business hours a typical device will contact 25 to 35 unique external IP addresses during any given hour window[1].

› On average, when triaging a security event sourced from firewall logs, Codis Technologies has found that a seasoned analyst will take three minutes to determine whether to dismiss the event or to continue with the investigation.

› Pre-processing firewall logs by excluding port 80 and 443 traffic reduced the overall event count though events still lacked sufficient context to effectively prioritize the events.

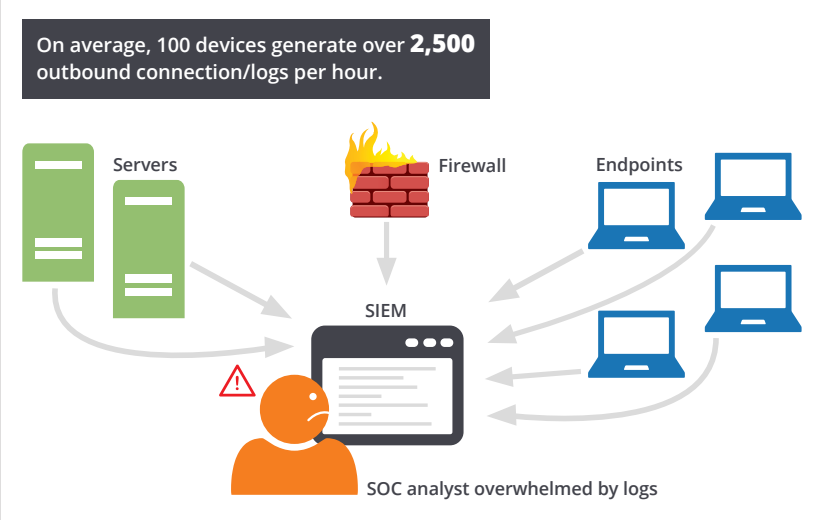

Figure: SOC analysts typically are overwhelmed by the volume of logs pouring into their SIEM.

Given that a typical device will contact 25 to 35 unique external IP addresses during any given hour window, a typical organization with only 100 devices could generate over 2,500 outbound connections per hour.

The numbers above do not take into account any pre-processing/filtering that may be done to the logs (e.g., geoIP, odd ports, bad IP lists, etc.) to reduce the number of events. Unfortunately, as we discovered, even pre-processing/filtering high-volume/low-context log sources still resulted in a high number of events, which lacked the context required to prioritize them effectively. In some cases pre-processing of the logs actually resulted in an increase of false negatives.

Given this data, it's easy to see why so many organizations choose to rank security events generated from high-volume/low-context data sources as low priorities and only focus on them during a forensic investigation.

[1] These numbers were derived from the study of one week of firewall logs of a 15,000-seat organization.

The OSINT Factor

Integrating Recorded Future into an organization's detection framework enables that organization, no matter how large, to effectively and efficiently monitor high-volume/low-context data sources.

Using Recorded Future, we were able to enrich firewall events with:

- Current risk indicators
- Malware attribution
- Related observables
- Risk scores

The context provided, via automation, by Recorded Future goes well beyond a typical threat intelligence feed. As you'll see in the following section, the context provided by Recorded Future not only increases an organization's ability to generate meaningful security events but also acts as a force multiplier. The Recorded Future enriched data set allows analysts to reach critical decision points faster which in turn allows the analyst to analyze more events; all without sacrificing the quality of analysis.

The Results

Test Environment

For our testing we created a controlled environment consisting of four PCs, a firewall, and a SIEM solution. One of the four PCs was infected with malware (see figure below).

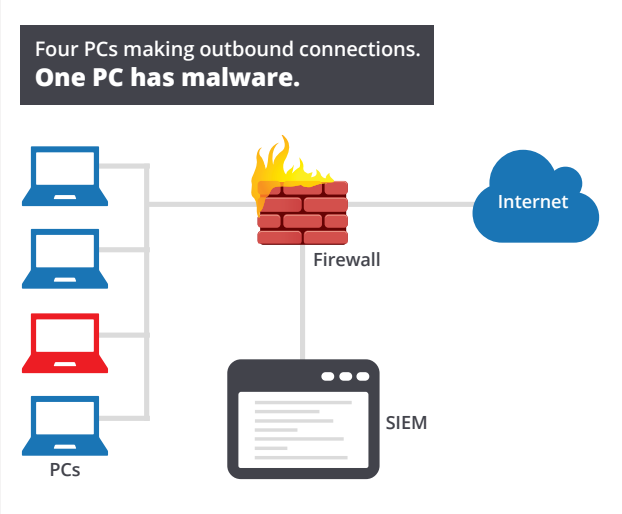

Figure: Lab test environment.

Using our SIEM solution, two reports were generated which showed all outbound connections for the past 60 minutes from the firewall logs. Recorded Future was used to enrich one report and the other was not. The report contained 210 unique IPs.

The Task

› One SOC analyst (in a controlled environment)

› 210 unique IPs to be triaged

› 60 minutes time limit

Results

	Without Recorded Future	With Recorded Future
IPs checked	20	210
Average triage time per IP	180 seconds (Triaged only 20 IPs in 60 minutes. Ran out of time after 60 minutes of triage.)	1.2 seconds (All 210 IPs triaged in four minutes. See explanation of the approach in the next section.)
Actions	No malware found.	Dridex infection discovered in 12 seconds — the IP with the highest risk score was investigated first.
Conclusion	One analyst would require 10.5 hours to manually review the 210 IPs. While most organizations would not be reviewing every IP that shows up in their firewall logs, this exercise shows how the monitoring and review of high-volume/low-context data sources is not practical for any organization. Also, this report was run against 40 OSINT feeds, but only two IPs from the 210 were flagged, which did not provide the analyst any significant time savings in this controlled environment.	One analyst could triage 210 events in under four minutes as opposed to the 10.5 hours required to investigate them manually. In other words, if all events have to be processed within the hour (since the next hour would bring in a new set of events), an analyst using Recorded Future could process one hour's worth of events in four minutes with 56 minutes to spare. Without Recorded Future, 10 analysts would be required to process the same report within the one-hour timeframe with no guarantee the Dridex event would be triaged properly — resulting in a 10x gain in analyst productivity, even if one assumes that the analyst using Recorded Future takes the full hour and not the actual time of four minutes.

An Explanation of the Approach Using Recorded Future

Recorded Future's threat intelligence integration with the SIEM helped the analyst triage all 210 IPs in under four minutes. Recorded Future provides risk scores (see figure below) which allowed the analyst to quickly prioritize which IPs to ignore and which ones to investigate further. Here is the approach:

› 11 IPs prioritized with a Recorded Future risk score greater than five were triaged using Recorded Future IP Cards, which provide immediate context on malicious indicators associated with an IP address.

› Five IPs with a Recorded Future risk score of five were quickly assessed.

› 89 IPs with a Recorded Future risk score of zero were discarded due to the low threat.

› 105 IPs without a Recorded Future risk score were discarded since investigation of these IPs was unlikely to lead anywhere.

Using Recorded Future's risk scores as a force multiplier of high-volume/low-context data sources can be considered in scope. These are impressive numbers.

In the real world, a report that shows all outbound connections for the past hour would most likely never exist, at least one that is expected to be reviewed by a SOC analyst. Most organizations are not reviewing firewall logs on an hourly basis, aside from perhaps a "top 10" report or comparing against various OSINT feeds, and it is easy to see why.

Even when we checked the IPs in the report against over 40 OSINT feeds there were only two matches and those lacked any meaningful context. A key point here is that while OSINT did flag two of the 210 IPs there was no analysis performed or risk assigned to the other 208 IPs in the report.

However, with the context and risk scoring provided by Recorded Future, organizations can begin efficiently and effectively monitoring data sources that were previously untouchable, prioritize events by risk, and increase their chances of detecting a compromise in its early stages with existing resources.

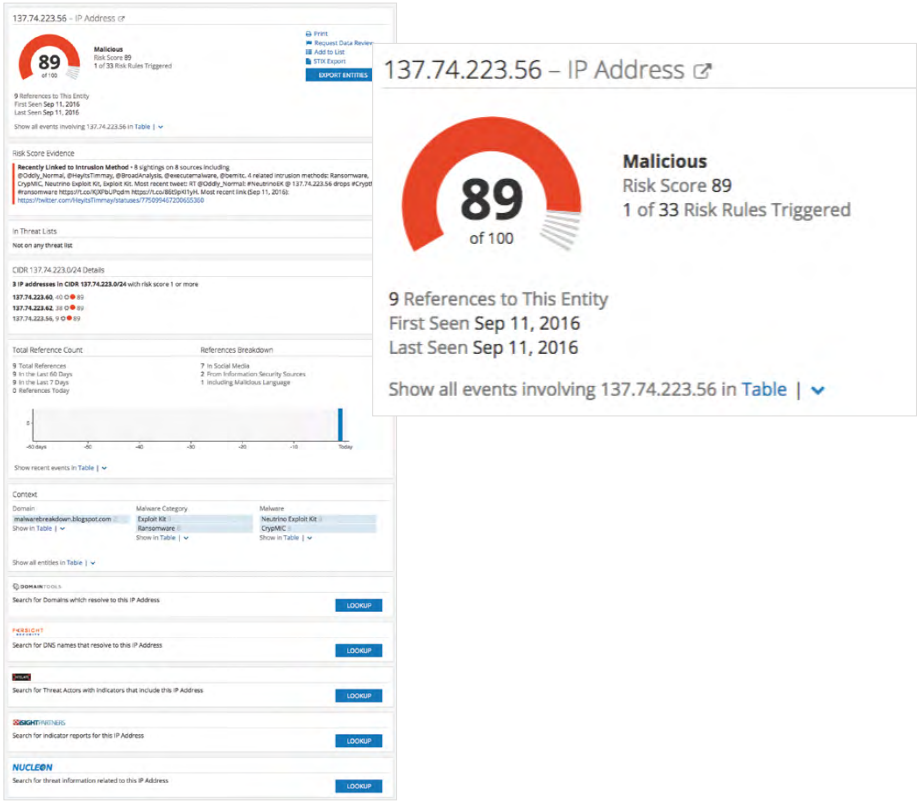

Figure: Recorded Future IP risk score displayed on an Intel Card enables more effective prioritization. The Intel Card provides immediate context on the maliciousness of an IP address. This information is automatically available in the SIEM.

Conclusion

Recorded Future provided the analyst a 10x gain in productivity (in this controlled environment). With Recorded Future, following the approach described above, one analyst could triage 210 events in under four minutes as opposed to the 10.5 hours required to investigate them manually. In other words, if all events have to be processed within the hour (since the next hour would bring in a new set of events), an analyst using Recorded Future could process one hour's worth of events in four minutes with 56 minutes to spare. Without Recorded Future, 10 analysts would be required to process the same report within the one-hour timeframe with no guarantee the Dridex event would be triaged properly — hence the 10x gain in analyst productivity, even if one assumes that the analyst using Recorded Future takes the full hour as opposed to four minutes. Using Recorded Future's risk scores as a force multiplier of high-volume/low-context data sources can be considered in scope.

In the real world, a report that shows all outbound connections for the past hour would most likely never exist, at least one that is expected to be reviewed by a SOC analyst. Most organizations are not reviewing firewall logs on an hourly basis.

When checking the IPs in the report against over 40 OSINT feeds there were only two matches and those lacked any meaningful context. While OSINT did flag two of the 210 IPs there was no analysis performed or risk assigned to the other 208 IPs in the report.

With the context and risk scoring provided by Recorded Future, organizations can begin efficiently and effectively monitoring data sources that were previously untouchable, prioritize events by risk, and increase their chances of detecting a compromise in its early stages with existing resources.

ABOUT CODISTECH

Founded in 2011, Codis Technologies is an information security consulting firm which specializes in developing innovative incident detection, incident recognition, and process automation solutions. Working collaboratively with an organization's analysts, Codis excels at identifying incident detection opportunities and developing custom tailored solutions to ensure incidents are detected and recognized on day zero.

ABOUT RECORDED FUTURE

Recorded Future's mission is to empower customers with real-time threat intelligence to defend their organizations against threats at the speed and scale of the internet. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world, and over 17,000 IT security professionals use Recorded Future everyday. Request a demo at www.recordedfuture.com.

To learn more, please contact Recorded Future at info@recordedfuture.com.

DISCLAIMER:

This disclaimer governs the use of this report. By using this report, you accept this disclaimer in full.

The report contains information about threat intelligence and productivity evaluation. The information is not advice, and should not be treated as such. Any decision to purchase Recorded Future, or any other service, should be based exclusively on your own evaluation of your business needs.

You must not rely on the information in the report as an alternative or substitute to legal, business, IT or cybersecurity advice from an appropriately qualified profession. This research contained in this report was performed under a variety of conditions, and actual results may vary. Prospective users should evaluate all services based on their own systems to understand the implications of this report.

Recorded Future accepts no legal responsibility whatsoever and no warranties, express or implied, are given by us. To the maximum extent permissible by law, Recorded Future excludes all representations, warranties, undertakings and guarantees, and makes no representation, warranty, or guarantee that the information in the report is correct, accurate, complete or non-misleading.

By using this report, you agree that any use of information is wholly at your own risk, and you accept all risks and responsibility for any losses, damages, or any other adverse consequences that may have resulted from your use of the data. Recorded Future is not responsible for, and you agree Recorded Future will not be liable to you in respect of any business losses, including without limitation loss of or damage to profits, revenue, use, commercial opportunities, goodwill, or any other special, indirect or consequential loss or damage.

If a section of this disclaimer is determined by any court or other competent authority to be unlawful and/or unenforceable, the other sections of this disclaimer continue in effect. All trademarks used in the document are owned by their respective owners, and may only be used in strict accordance to their relevant terms.

This disclaimer will be governed by and construed in accordance with Massachusetts law, and any disputes relating to this disclaimer will be subject to the exclusive jurisdiction of the courts of Massachusetts.

This disclaimer was created in part with SEQ Legal.