uptycs

SEI Uses Uptycs and YARA Rules for Malware Detection and Forensic Investigations

> *"I would not want to do security anywhere without the level of visibility that Uptycs provides."*
>
> **Steve Shedlock**
> Incident Response Team Lead

Company
SEI

Champion
Steve Shedlock, Incident Response Team Lead

Computing Environment
13,000+ productivity endpoints, mostly Windows, some macOS and Linux

SEI Turns Cybersecurity Into a MSSP Business

SEI delivers technology and investment solutions that connect the financial services industry. With capabilities across investment processing, operations, and asset management, SEI works with corporations, financial institutions and professionals, and ultra-high-net-worth families to solve problems, manage change and help protect assets—for growth today and in the future. As of Sept. 30, 2022, SEI manages, advises, or administers approximately $1.2 trillion in assets.

In addition to serving its own internal needs for IT and security services, SEI provides services to support and secure the evolving cybersecurity and IT needs of today's regulated and fast-growing businesses. SEI Sphere, a managed security services provider (MSSP), delivers a comprehensive Managed Detection and Response program to help organizations strengthen their operational security and increase cyber maturity.

A 22-year employee of the company, Steve Shedlock currently leads the incident response team for SEI and the companies that subscribe to its MSSP program.

> *"SEI Sphere is unique; information security has become a revenue generator for our company rather than just a source of continual spend. But that also means my team has to be at the top of our game regarding cybersecurity."*
>
> **Steve Shedlock**
> Incident Response Team Lead

Challenges

- Deeper visibility than traditional endpoint detection and response (EDR) can provide
- Ability to write YARA rules to investigate threats on the endpoint
- Faster time to resolution of incidents

Uptycs Results

- Uptycs enables the infosec team to collect all the data it wants and conduct its own searches against that data
- Uptycs supports YARA to enable high-value indicator of compromise (IOC) searches
- Uptycs replaces a traditional forensic investigation tool with much more efficient data gathering and analysis

Looking for Threats on a Deeper Level

Shedlock's team is responsible for protecting endpoint devices. SEI alone has more than 13,000 endpoints—mostly Windows devices, but also macOS and Linux. This doesn't even count the devices that it oversees through SEI's MSSP services. With so many endpoints to protect, visibility into what is happening on them is critical.

SEI currently has CrowdStrike deployed for EDR, but Shedlock sought a complementary tool to get even more detail on endpoints so as to investigate incidents from a deeper perspective. "There are some things CrowdStrike can't do that we're interested in implementing. Specifically, we want to be able to run YARA rules on endpoints."

Uptycs Supports YARA Rules on Endpoints

By collecting events, feeding them to a SIEM, then analyzing them, you can identify malicious or anomalous activity to understand how intruders and malware operate on your network. Before learning about Uptycs, Shedlock's team initially considered using Sysmon to obtain detailed log information about process creations, network connections, and changes to file creation time. But Sysmon has too many drawbacks to use at scale.

"Uptycs solves a lot of the logistical issues that Sysmon has," says Shedlock. "Osquery [which turns an operating system into a relational database] was new to me, but I saw that it would deliver what I need to get, which is basically anything I want to write a rule against. We want to collect and store as much data as we possibly can, then use that to write better alerts. Uptycs lets us run YARA rules against process memory to detect threats in our environment."

> ***"We're always looking for high-value indicators, and YARA is one of the ways we can write rules that basically say, 'If you see this, throw an alert because we think this belongs to a certain malware family, like Emotet."***
>
> **Steve Shedlock**
> Incident Response Team Lead

YARA Helps Researchers Identify and Classify Malware Samples

YARA lets you create descriptions of malware families based on textual or binary patterns rather than on characteristics that change frequently, like IP address or domain name. Each description, or rule, consists of a set of strings and a Boolean expression.

"In running detections across our environment, I might discover that malware is communicating externally to a certain website or a set of IP addresses," explains Shedlock. "But those indicators are easy to change. A bad actor has hundreds of domains—maybe thousands of IP addresses—and they can easily change those indicators by messaging back to their malware. So that's a low-value IOC."

"YARA rules empower us to discover things of higher value. The key is to learn that a bad actor uses a certain pattern in their URLs or in creating their malware code. We might learn through our research or intel channels that every time a new piece of malware shows up, it always has defining characteristics," says Shedlock. "We can then focus on those characteristics that are extremely hard for a malware writer to change; it's part of their behavior and code development. Using YARA rules against that, the miscreant can change their DNS and IP address all they want. We'll still be able to track them any time."

Collective Defense Through Intel Communities Like FS-ISAC

Shedlock's team analyzes malware that targets SEI, then writes YARA rules to detect its behavior. It shares these rules with intel communities, including FS-ISAC. Anyone able to detect threats based on YARA rules can use what his team develops. The rules work across platforms—endpoints, servers, cloud—as well as on Windows, Linux, and macOS. With Uptycs, SEI can run YARA rules against particular processes and files for near real-time detections.

Uptycs API Routes Endpoint Data to SIEM

SEI wrote its own SIEM and ticketing system that lets it write alerts on anything it wants to. It plans to use the Uptycs API to send endpoint data to the SIEM. “Uptycs gives us so much information we never had before,” says Shedlock. “Now we’re thinking of all the cool stuff we can trigger with that we haven’t been able to do before.”

“Let’s say CrowdStrike alerts that something encoded in PowerShell ran on a particular system. This needs to be investigated. Uptycs can tell us all the DNS entries that were hit in the minutes before and after the PowerShell item ran. It reports all the processes that were created, as well as new registry entries that were created during that interval. We can configure the API to get all this information automatically when such an alert comes in, saving us considerable investigative time.”

Beyond CrowdStrike, Uptycs will also be used to complement SEI’s other security tools. “It’s going to show us where the gaps are,” says Shedlock. “It could be a firewall request that creates an alert. It could be data loss prevention [DLP]. If a user sends out a spreadsheet, what were they doing on their PC right before they did that? Uptycs data will help us quickly understand if an alert is legitimate or not.”

> *“Visibility is key. That’s where Uptycs fits in—to provide endpoint visibility that isn’t there otherwise. It’s a great complement to our other security tools.”*
>
> **Steve Shedlock**
> Incident Response Team Lead

Uptycs Reduces Investigation Timeframes from Hours to Minutes

“An investigation used to take us countless hours using forensics software. Now with our enhanced visibility, in five minutes we can see where something happened with 100 percent confidence,” Shedlock says.

Uptycs also reduces the skillsets required to conduct an investigation. “It takes a lot of forensic training prior to examining what transpired on a given hard drive. With Uptycs, it takes far less training to conduct queries and get the same information.”

Uptycs has replaced about 90% of the forensic software functions SEI once used. “We used EnCase Investigator as our main investigative tool for malware and incident response. We barely need it now since using Uptycs for endpoint visibility.”

“Uptycs has the ability to span multiple environments—from any endpoint to the cloud. This enables YARA rules to cover a wider threat landscape and provide even more value to SEI and its client organizations.

About Uptycs

Uptycs, the first unified CNAPP and XDR solution, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive enterprise-wide security posture.

Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today.
Be ready for what’s next.

Shift your cybersecurity up with Uptycs.

uptycs