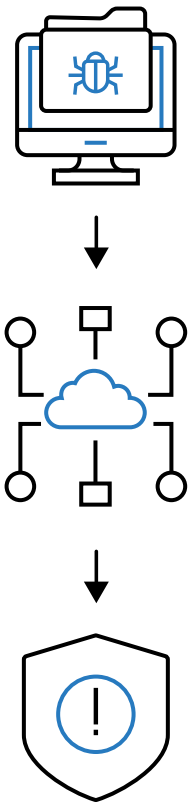
SMARTMonitor

Cyber assurance that gives you peace of mind.

Ransomware Protection: a user scenario

While preparing for a meeting, Eric visits a client website. Unknown to him, their website has been hacked. He absently clicks through some annoying popups that say something about "untrusted Flash" and "Java content". It just seems like unimportant techno-jargon to him.

He finishes up for the day and goes home.



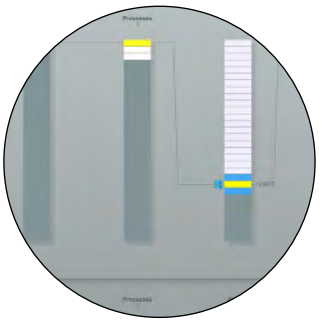
Once Eric's machine was idle for a while, the ransomware payload downloaded from the exploit kit and started doing its damage: encrypting files on Eric's machine and all attached network shares.

SMARTMonitor is able to detect this attack and prevent a wide scale catastrophic ransomware event.

ActiveAgents are continuously collecting Windows log data from all the machines.

This data is sent to the cloud based knowledge repository where SMARTMonitor compares it to the baseline for Eric's machine.

Through entity tracking, the Knowledge Repository determines that this ransomware process is a new addition to Eric's machine and flags it as an alert, indicating the need for human review.

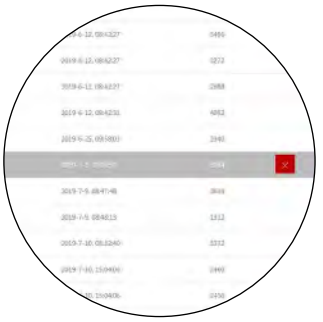


Is this new activity a threat?

Julie, the head of I.T. security sees the alert in the SMARTMonitor web user interface. In a few minutes she can determine that:

- Eric's machine is running software that has not been seen before on the network.
- This new program was started from Adobe Flash, suggesting a web compromise.
- The program connected to internal file servers, suggesting an attack.

Julie immediately escalates the incident and starts remediation right away.

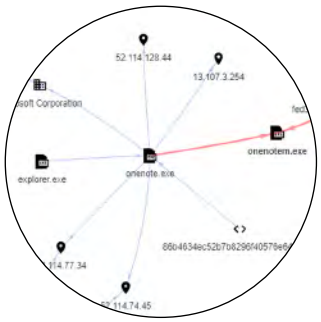


Neutralizing the threat

With the SMARTMonitor response module, she immediately:

- Tasks the Windows firewall on Eric's machine to block outgoing traffic (except to the SMARTMonitor cloud).
- Creates a detection rule that will fire an alert if that program hash (unique identifier) is found anywhere on the network.
- Attaches a response policy to the rule to immediately kill the process before any harm can be done.*

** Upcoming feature*



Assessing the damage

SMARTMonitor also allows Julie to assess the impact of this attack on the rest of the network and inform further action.

Using the SMARTMonitor entity graph explorer, she can drill down into the logs and discovers:

- Eric's computer was running outdated Adobe Flash software.
- This outdated software is also running on a few other machines.
- However, the other vulnerable machines did not report any deviations from their baseline and did not have the hash for the ransomware found on Eric's machine.

SMARTMonitor Cyber Assurance

Julie now has confidence that she understands the full scope of the incident.

With this assurance, she can start the recovery process, making a mental note to patch the vulnerable software once this incident is resolved.

Find out how SMARTSentinel can protect your network

www.cyberdefencecorp.com

info@cyberdefencecorp.com

613-701-2854

Cyber Defence Corporation