Ransomware Readiness Assessment for Manufacturing
At a Glance

Ransomware has emerged as a pervasive threat to manufacturing operations. We have seen plant downtime due to ransomware. Targeted attacks always took down multiple plants at once, so the attacker could extort a high ransom payment.

Manufacturing is one of the most targeted industries, and attacks succeeded even when virus protection software and firewalls were in place, such as those recommended in the IEC 62443 standards. Once installed, organizations must pay attention to their antivirus software and firewall update notices so that they know when there is new ransomware being created.

There is no silver bullet that can provide complete protection. However, to mitigate the risks, manufacturing organizations should work with industry security experts to create effective cybersecurity plans to mitigate the risks. These plans should include a Ransomware Readiness Assessment, which can save manufacturing organizations time and money if they get hit by ransomware.

Palo Alto Networks Unit 42 Ransomware Readiness Assessment

Standards like IEC 62443 were developed a while ago and lag behind current events. With this said, standards should reflect today's threat environment even though it's not easy to update them often due to the complexity of the process.

Unit 42 is an elite team of skilled security professionals, and they can help you create an intelligence-driven, response-ready organization. The Unit 42 Threat Intelligence team provides threat research that enables security teams to understand adversary intent and attribution while enhancing protections offered by our products and services to stop advanced attacks like ransomware.

With the rise of ransomware attacks, manufacturers are being forced to rethink their overall security strategy and need a plan to proactively prepare for and rapidly respond to mitigate the risks.

Ransomware is constantly evolving. Are you? This is why the industry needs a Ransomware Readiness Assessment. The program is built on Unit 42's expertise in threat intelligence research and incident response and applies everything they've observed and learned to continuously evolve best practices over the last decade.

This assessment and advisory service is focused on your ability to prevent, detect, respond to, and recover from a ransomware attack. The goal of the assessment is to assist your security team in identifying gaps in your ransomware prevention, response programs, and supporting procedures. We will assist the security team in identifying actionable recommendations to enhance training, tool sets, and the capabilities to prevent, detect, respond, and recover from a ransomware attack. This engagement will help you empower the organization to understand threats and drive better security outcomes.

The Ransomware Readiness Assessment is set up in tiers to provide an easily consumable roadmap to ransomware resiliency—each tier adding more strategic services and deliverables to drive more strategic outcomes.

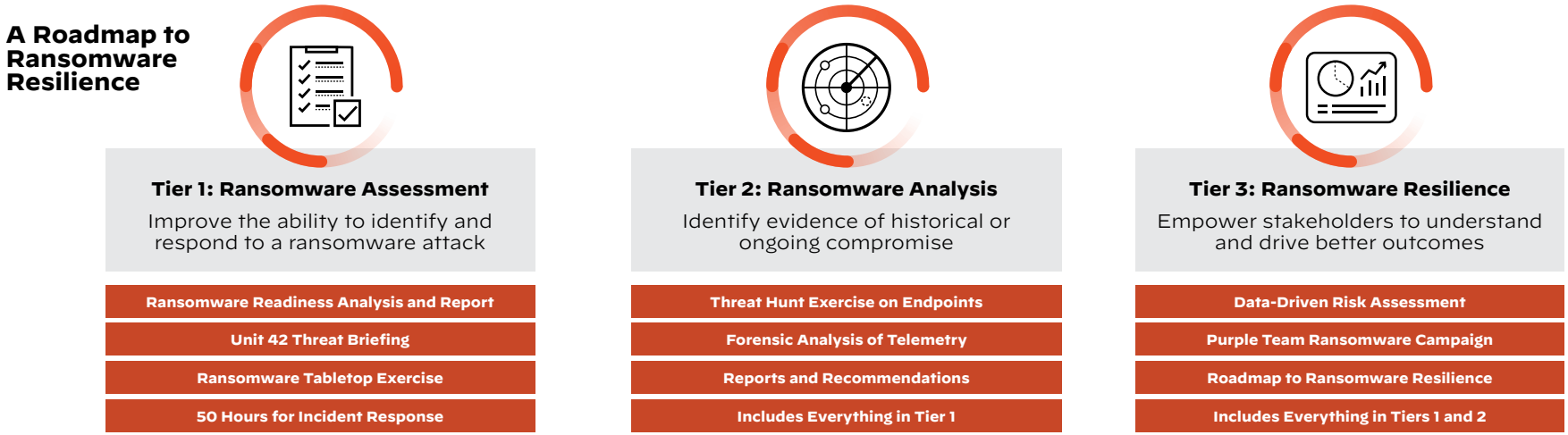


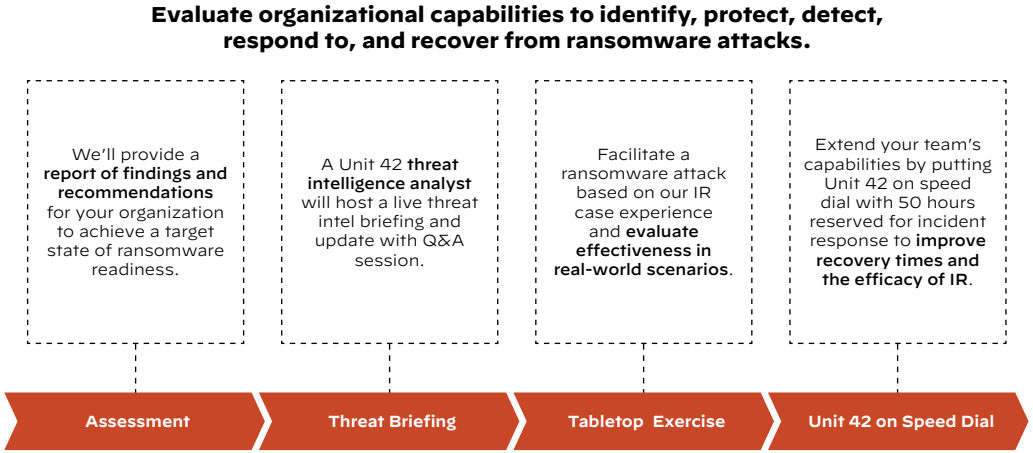
Figure 1: Unit 42 Ransomware Readiness Assessment Tiers

Ransomware Readiness Assessment for Manufacturing
At a Glance

Tier 1: Ransomware Assessment

Tier 1 is an assessment of your security team's ability to respond and recover from a ransomware attack. The Ransomware Readiness Assessment includes a full examination of your incident response plan, capabilities, and technologies. Our team of industry security consultants will highlight gaps and identify areas for improvement to help bolster your readiness and strengthen your overall cyber defense capabilities. We offer:

- A best-practices ransomware response playbook
- Prioritized recommendations for program enhancements and technical recommendations for prevention, detection, response, and recovery measures
- Recommendations enhancing the existing capabilities and capacity of your security team



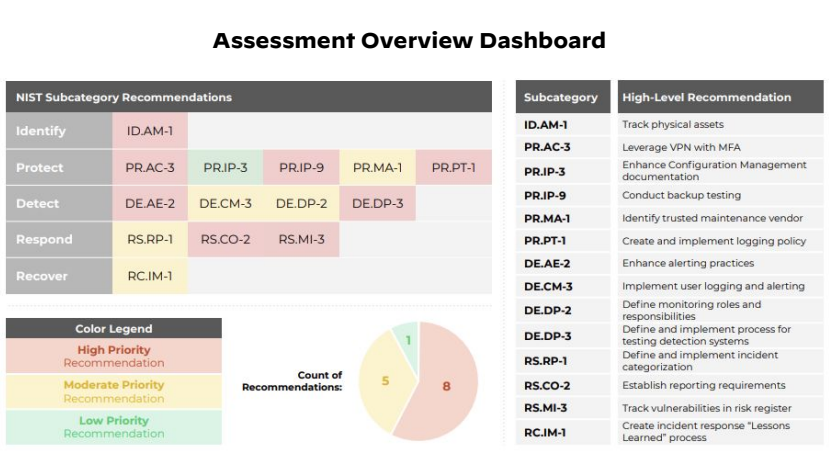


Figure 2: Unit 42 Ransomware Readiness Assessment Tier 1 (left); Assessment Overview Dashboard (right)

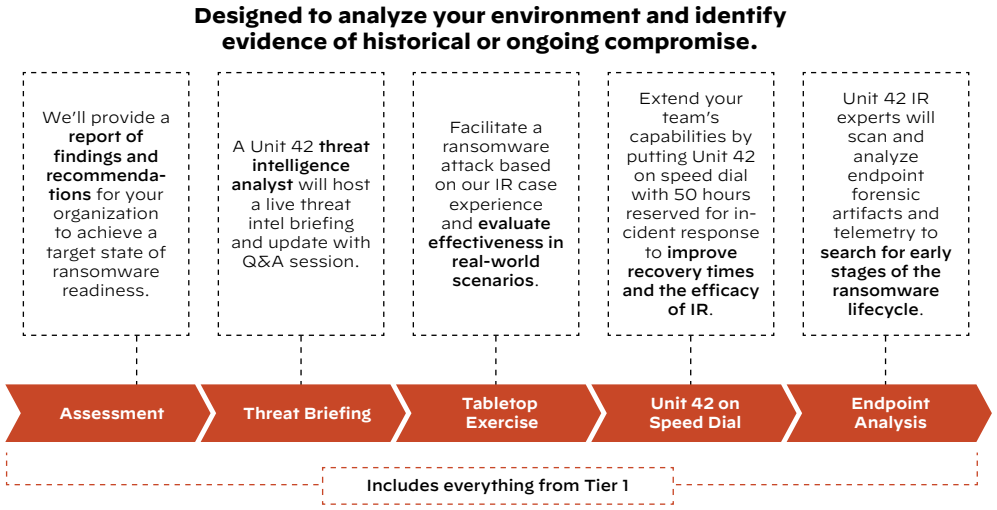
Ransomware Readiness Assessment for Manufacturing
At a Glance

Tier 2: Ransomware Analysis

Tier 2 takes your assessment to the next level with a detailed ransomware threat hunting exercise in your environment. The ransomware analysis is designed to identify evidence of historical or ongoing compromise. Unit 42 IR experts will analyze endpoint forensic artifacts and telemetry to search for the early stages of the ransomware lifecycle.

We hunt for indicators of compromise (IoCs) related to sophisticated ransomware threat actors, including unauthorized access, use of PowerShell post-exploitation frameworks, and precursor malware that often leads to the installation of ransomware, such as:

- Unauthorized access to the environment
- Malicious software and malware persistence
- Lateral movement and remote execution
- Credential theft
- Data exfiltration or sabotage
- Profile external attack surface for threats
- Vulnerabilities exploitable by ransomware actors



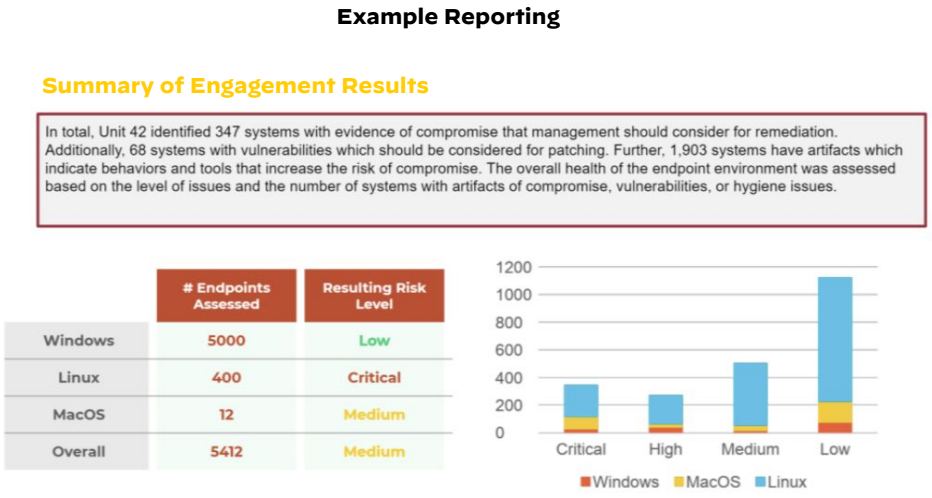


Figure 3: Unit 42 Ransomware Readiness Assessment Tier 2 (left); example reporting (right)

Ransomware Readiness Assessment for Manufacturing
At a Glance

Tier 3: Ransomware Resilience

Tier 3, the last and final tier of the program, is designed to empower key stakeholders to understand organizational risks related to the ransomware threat, like factory floor downtime and business continuity, to drive better security outcomes. From the start, the Unit 42 offensive security team at Palo Alto Networks targets your environment following predefined rules of engagement with a custom-designed campaign of advanced TTPs used in real-world ransomware attacks.

Purple Team Exercises will attempt to enumerate gaps in defenses and ensure that you can protect your organization from current threats. Unit 42 will work with your security team to complete the following objectives:

- Create and establish a baseline for the environment.
- Optimize defenses to prevent malware.
- Create a shorter response time for a security incident.
- Detect and respond to anomalous events and common offensive tactics and techniques.
- In conjunction with your security teams, we will verify configurations, review tool output, and test the fidelity of the rules, indicators, and/or events that generate security events.

An executive report detailing the approach, methodology, findings, and recommendations will be delivered when the exercises are completed.

Conclusion

As ransomware escalates, Unit 42 is available to advise you on the latest risks, assess your readiness, and help you recover when the worst occurs. The Unit 42 Security Consulting team serves as a trusted partner with state-of-the-art cyber risk expertise and incident response capabilities, helping you to focus on your business before, during, and after a breach.

Learn more about Unit 42 services:

Service Description Ransomware Readiness Assessment

About Unit 42

Contact Us

If you think you may have been breached, please email unit42-investigations@paloaltonetworks.com or call 1-866-4-UNIT42 to get in touch with the Unit 42 Incident Response team. If you'd like to learn more about how the Unit 42 Security Consulting team can help your organization defend against and respond to severe cyberthreats, please fill out this form.

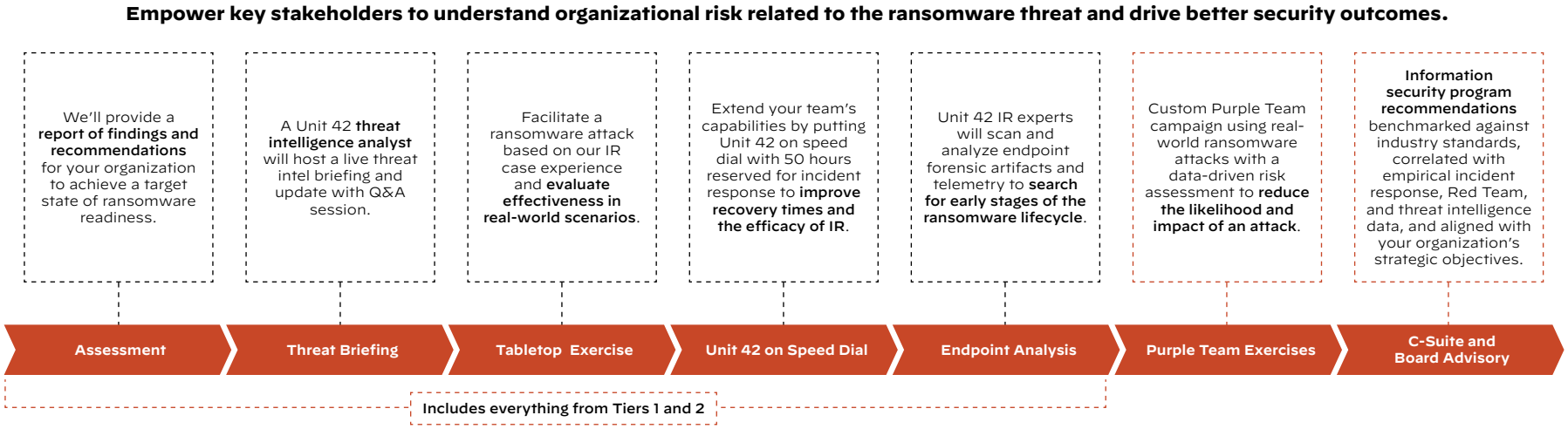


Figure 4: Unit 42 Ransomware Readiness Assessment Tier 3